DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

# Trabajo Práctico

**Traceroute**

Teoría de las Comunicaciones


| Integrante | LU | Correo electrónico |
|---|---|---|
| Gonzalo Ariel Meyoyan | 514/20 | gonzalo@meyoyan.com |
| Alexandra Abbate | 710/19 | alexandra-abbate@hotmail.com |
| Cielo Serena Roccella | 122/21 | cielorocella@gmail.com |
| Florencia Rosenzuaig | 118/21 | f.rosenzuaig@gmail.com |






**Facultad de Ciencias Exactas y Naturales**
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

# 1. Introducción

El protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) permite la comunicación efectiva y envío de información entre computadoras. El protocolo ICMP (Internet Control Message Protocol) le da soporte al protocolo TCP/IP. Éste se encarga de diagnosticar errores en la comunicación; principalmente informa si la información llego al destino correcto en el tiempo esperado.

En este informe explicaremos como, gracias a ICMP, es posible reconstruir el traceroute de una conexión, es decir, la ruta por la que viajaron los paquetes desde un host hasta cierto destino. En particular, nos enfocaremos en identificar saltos interoceánicos en estas rutas.

El análisis lo realizaremos sobre los resultados obtenidos de ejecutar traceroutes a distintas universidades: Universidad Charles Darwin, Universidad Politécnica de San Petersburgo Pedro el Grande, Universidad de Münster y Universidad de Hong Kong. Para ello utilizaremos una extensión del script de **Python** provisto por la cátedra, aplicando las librerías **Folium** y **Seaborn** para la creación de visualizaciones. Nuestro objetivo en este TP fue recopilar información detallada con el fin de poder responder satisfactoriamente a las preguntas que guiaron nuestra experimentación, planteadas más adelante.

A continuación, exhibiremos nuestros experimentos y conclusiones.

# 2. Métodos y condiciones de los experimentos

## 2.1. Script utilizado

Implementamos una herramienta de traceroute que, dada una IP destino, devuelve las IPs recorridas hasta llegar al mismo. Además devuelve el RTT (Round Trip Time) de cada IP, es decir, cuánto tarda en llegar la respuesta de cada IP.

Para ello, mandaremos desde la IP origen paquetes al destino incrementando el TTL (Time to live). A medida que el paquete se desplaza a través de la red, el valor del TTL disminuye en cada salto. Una vez que el TTL llega a cero, el router actual descarta el paquete y envía un mensaje ICMP de "Tiempo Excedido"de vuelta a la computadora de origen. En particular, el mensaje de error contiene la IP del router donde se produjo el error. De esta forma, incrementando el TTL de a uno, podemos enterarnos de las direcciones IP recorridas, y permitiéndonos aproximadamente reconstruir el trayecto.

Sin embargo, debido a que las rutas no son estáticas, existe la posibilidad de que los paquetes sigan caminos distintos a medida que incrementamos el TTL. Por lo tanto, es imposible saber con absoluta certeza que la ruta obtenida sea totalmente precisa.

En particular en este código, incrementamos el TTL desde 1 hasta 25. Para cada TTL, enviamos 30 paquetes, y recopilamos todos los RTTs de las IPs que contestaron. A partir de estos datos, nos quedamos con aquella IP que más contestó y calculamos el RTT promedio.

Ya teniendo los RTTs de cada IP, es sencillo calcular el tiempo de Hop (tiempo entre salto) entre dos IPs: Dadas dos IPs A y B, su tiempo de salto es B.rtt - A.rtt.

## 2.2. Nuestra hipótesis

Si en el traceroute un salto entre IPs tiene un RTT comparativamente alto, entonces es indicativo de que es un salto interoceánico.

# 3. Experimentación

Ejecutamos nuestro traceroute, utilizando como destino las direcciones IP de múltiples universidades alrededor del mundo. A continuación, detallamos información de cada una de ellas.

#### 3.0.0.1 Universidad Charles Darwin

- IP: 138.80.162.69
- Ubicación: Sydney, Australia
- Página web: `https://www.cdu.edu.au`

#### 3.0.0.2 Universidad Politécnica de San Petersburgo Pedro el Grande

- IP: 178.154.244.120
- Ubicación: San Petersburgo, Rusia
- Página web: `https://english.spbstu.ru`

#### 3.0.0.3 Universidad de Münster

- IP: 128.176.6.250
- Ubicación: Münster, Alemania
- Página web: `https://www.uni-muenster.de/en/`

#### 3.0.0.4 Universidad de Hong Kong

- IP: 147.8.2.58
- Ubicación: Hong Kong
- Página web: `https://www.hku.hk`

## 3.1. Resultados de los experimentos

Durante el análisis de los resultados obtenidos, observamos que en algunos casos el RTT para un TTL $n$ es mayor que para el TTL $n+1$. Esto implica que existen hops con un delta de tiempo negativo con respecto a sus RTTs.

Esta situación puede ser atribuida a cambios en la ruta de la red, congestión de paquetes que se resolvió antes del siguiente salto, o a una combinación de ambos factores.

En estos casos particulares, decidimos no representar los valores negativos de RTTs en nuestros gráficos. Sin embargo, creemos que estos deltas negativos proporcionan información relevante al entendimiento de la ruta, por lo que optamos por representar su RTT como 0 en lugar de simplemente ignorarlos. Así, podemos fácilmente deducir durante que segmentos de la ruta se produjo un cambio o congestión.

### 3.1.1. Identificación de saltos interoceánicos

#### 3.1.1.1 Universidad Charles Darwin

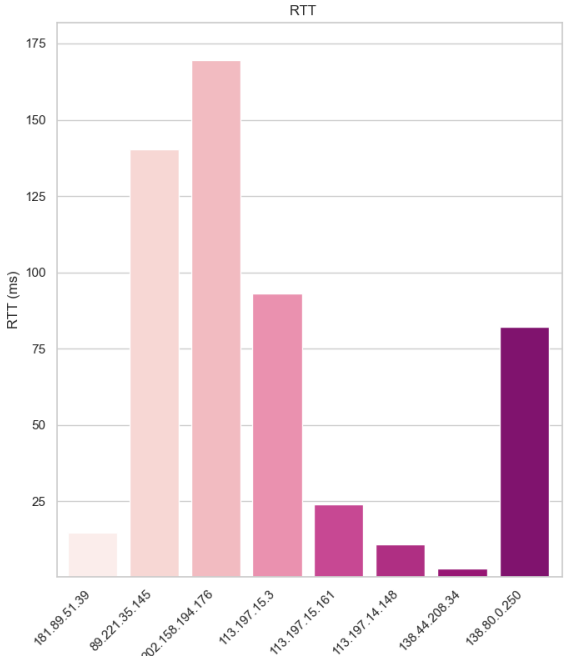



Figura 1.1: RTT promedio hacia la Universidad Charles Darwin

En la Figura 1, observando el RTT promedio para cada hop, vemos que hay 4 IPs cuyos tiempos de respuesta llaman la atención: 89.221.35.145, 202.158.194.176, 113.197.15.3 y 138.80.0.250. En particular 89.221.35.145 y 202.158.194.176 poseen RTTs extremadamente altos en comparación, los cuales sospechamos pueden tratarse de saltos interoceánicos.

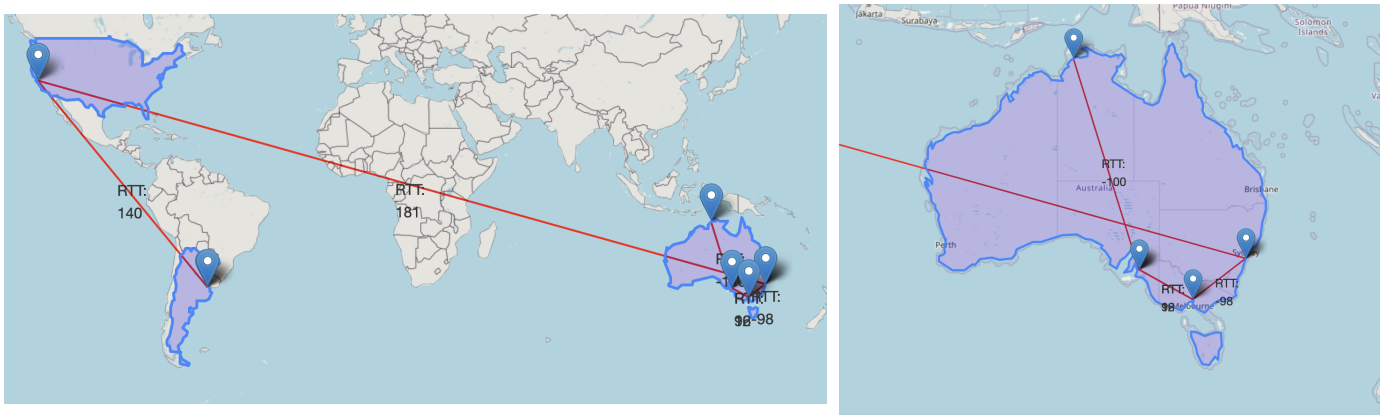



Figura 1.2: Ruta hacia la Universidad Charles Darwin

Visualizando la ruta resultante presentada en la figura 1.2, observamos que identificamos correctamente como saltos interoceánicos aquellos asociados a las IPs 89.221.35.145 y 202.158.194.176, los cuales consisten en saltos AR→US y US→AU respectivamente.

Por otro lado, los restantes dos saltos con un RTT anómalo (202.158.194.176 → 113.197.15.3) y (138.44.208.34 → 138.80.0.250) no representan saltos interoceánicos ni tampoco, para nuestra sorpresa, saltos de gran longitud. El primero consiste en un salto dentro de la ciudad de Melbourne(AU) mientras que el segundo, de un salto desde la ciudad de Adelaide(AU) hacia Darwin(AU).

#### 3.1.1.2 Universidad de Münster

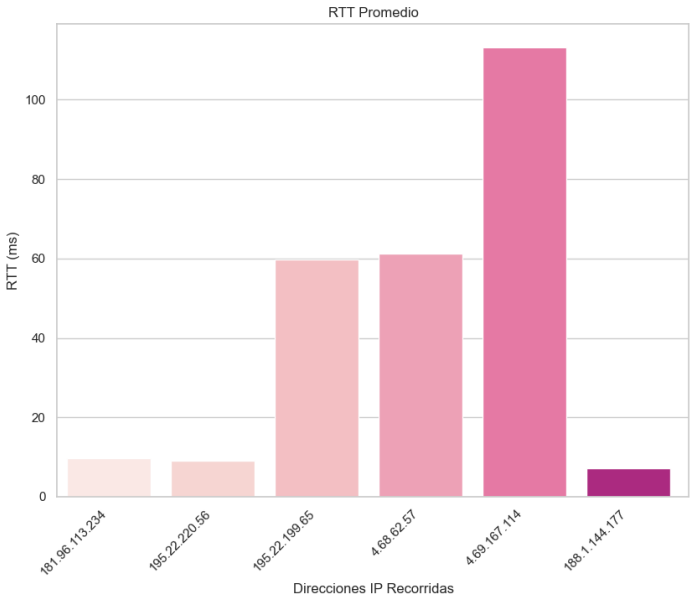



Figura 2.1: RTT promedio de la ruta hacia la Universidad de Münster

Analizando la figura 2.1, notamos que la IP con RTT más alto es 4.69.167.114 y, al igual que en el caso de Australia, existen dos saltos más con un RTT más elevado al promedio, pero aun asi alejadas del outlier principal. Hipotetizamos entonces que el salto hacia la IP 4.69.167.114 es probablemente un salto interoceánico, pero no podemos realizar con certeza afirmación alguna sobre los otros dos outliers.

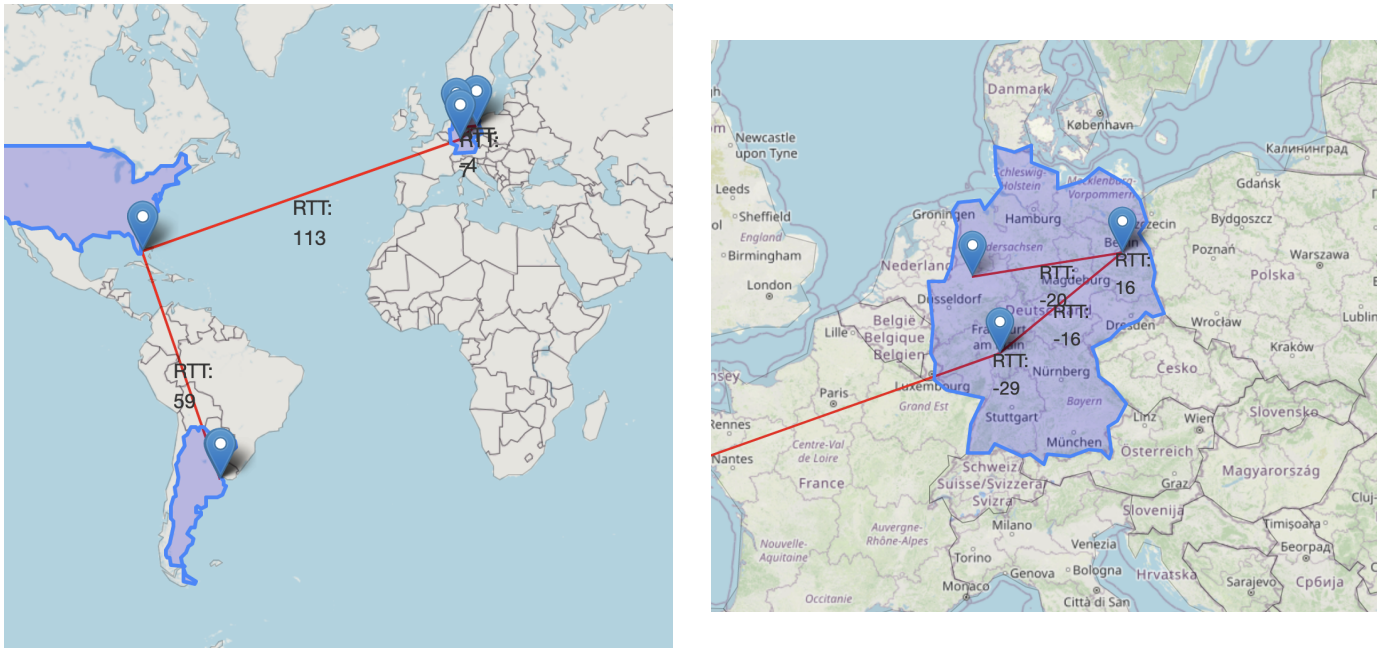



Figura 2.2: Ruta hacia la Universidad de Münster

Observando la figura 2.2, vemos que deducimos correctamente que el salto hacia la IP 4.69.167.114 (US → GER) consiste en un salto interoceánico basándonos en su alto tiempo de respuesta.

Además, notamos que uno de los dos outliers ya mencionados (195.22.220.56 → 195.22.199.65) consiste también en un salto interoceánico (AR → US), mientras que por otro lado el salto (195.22.199.65 → 4.68.62.57) representa solo un salto dentro de Miami(US) a pesar de su elevado RTT.

#### 3.1.1.3 Universidad Politécnica de San Petersburgo Pedro el Grande

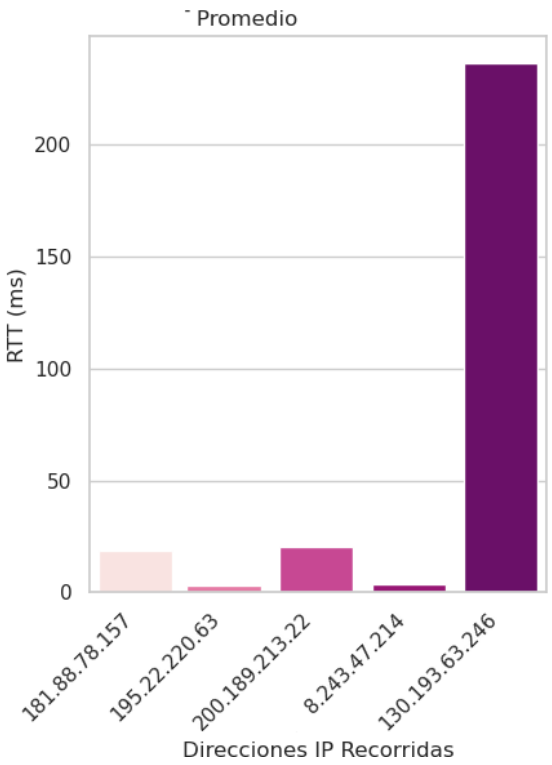



Figura 3.1: RTT promedio de la ruta hacia la Universidad de San Petersburgo

La figura 3.1 muestra claramente que uno de los routers intermedios (130.193.63.246) se destaca por su elevado tiempo de respuesta (RTT). Debido a esto, sospechamos que el salto (8.243.47.214 → 130.193.63.246) se trata de un salto interoceánico.

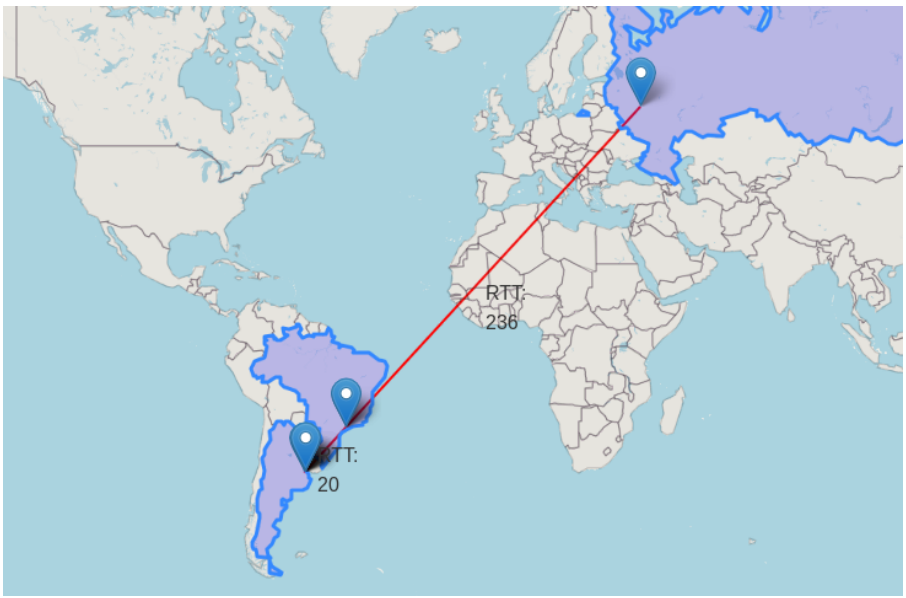



Figura 3.2: Ruta hacia la Universidad de San Petersburgo

Analizando la figura 3.2, podemos confirmar nuestra afirmación anterior y verificar claramente que el salto (8.243.47.214 → 130.193.63.246) consiste en un salto interoceánico entre Brasil (8.243.47.214) y Rusia (130.193.63.246).

#### 3.1.1.4 Universidad de Hong Kong

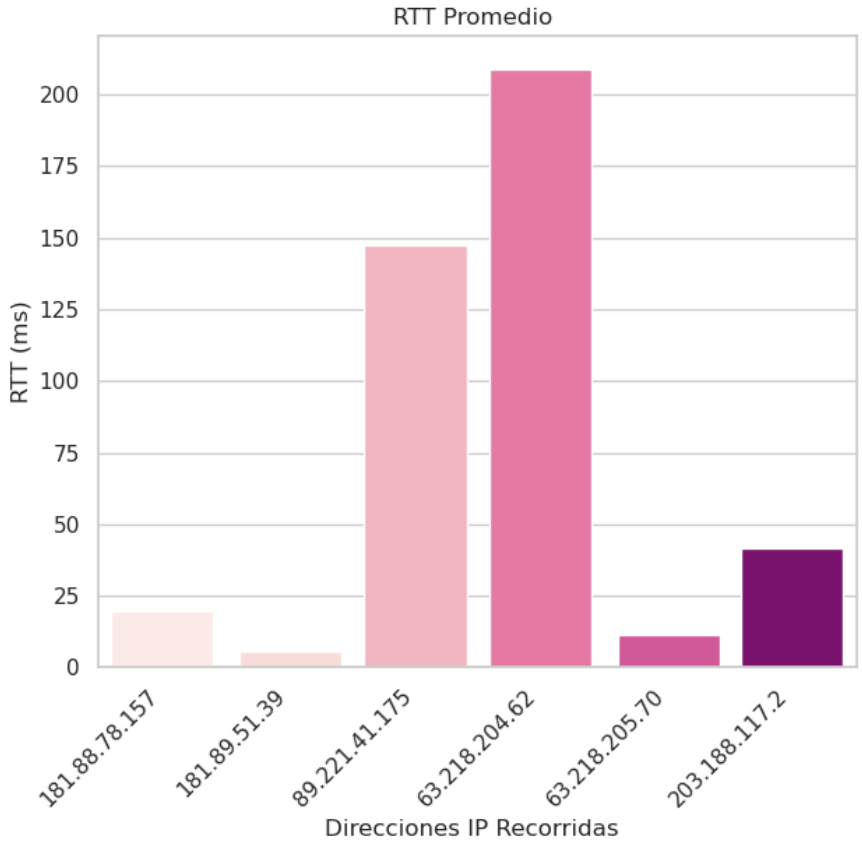



Figura 4.1: RTT promedio de cada hop en la ruta hacia la Universidad de Hong Kong

Observando la figura 4.1, notamos que los mayores tiempos de respuesta ocurren en los saltos (181.89.51.39 → 89.221.41.175) y (89.221.41.175 → 63.218.204.62), por lo que sospechamos que ambos consisten en saltos interoceánicos.

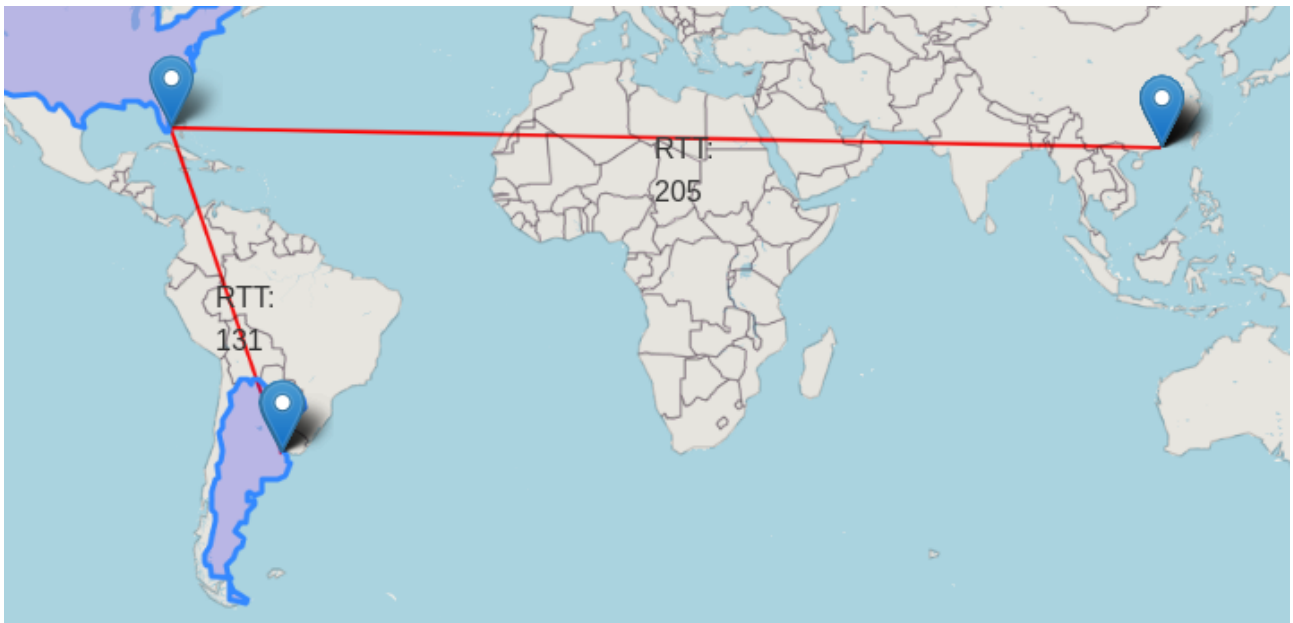
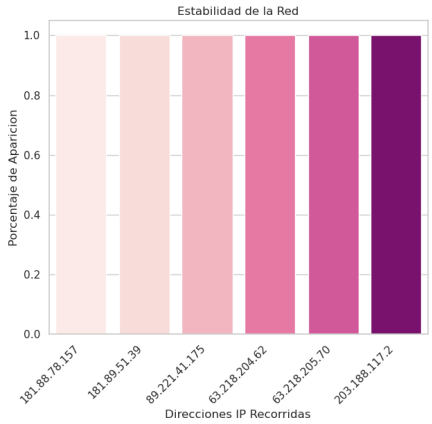



Figura 4.2: Ruta hacia la Universidad de Hong Kong

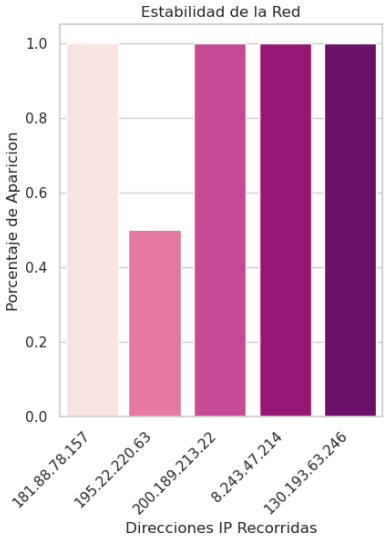
Efectivamente, la figura 4.2 corrobora que el salto (181.89.51.39 → 63.218.204.62) va de Argentina a Estados Unidos, y el salto (89.221.41.175 → 63.218.204.62) va de Estados Unidos a Hong Kong, siendo ambos interoceánicos. Cabe destacar que el gráfico del mapa es levemente erróneo, pues el salto presentado de Florida a Hong Kong pase probablemente a través del océano pacifico, y no a través de Europa.

### 3.2. Estabilidad de las rutas

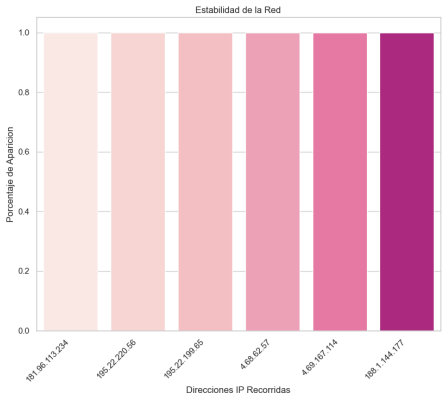
Para cada destino, nos preguntamos si para cada TTL siempre se llegaba a la misma IP. Para ello, en nuestra experimentaciones guardamos todas las IPs visitadas en cada TTL. Los resultados son los siguientes:



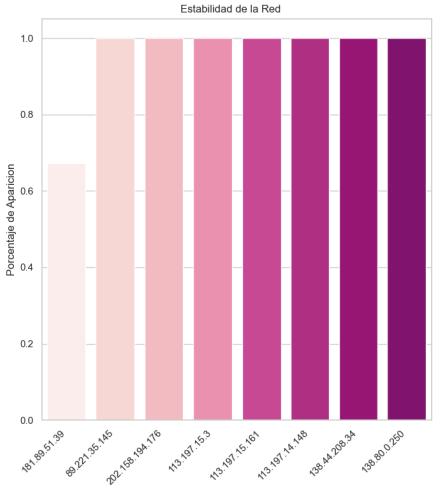

(a) Estabilidad hacia la Universidad de Honk Kong




(b) Estabilidad hacia la Universidad de San Petersburgo




(c) Estabilidad hacia la Universidad de Münster




(d) Estabilidad hacia la Universidad Charles Darwin

Figura 5: Estabilidad de las Rutas

Como podemos ver en la figura 5 las cuatro redes parecen ser estables, dado que el porcentaje de aparición de la IP más común de cada hop es máxima. Es decir, casi no hay varianza en las IPs de cada ruta.

Estos resultados nos parecieron extraños, ya que sabemos que la ruta es dinámica pero aun así observamos una escasa diversidad en las IPs visitadas. Llegamos a la conclusión de que la ruta seguramente esté variando en aquellos TTL que no responden.

### 3.3. TTLs sin respuesta

Durante cada una de las experimentaciones, notamos que ciertos TTLs nunca tenían respuesta. Por ejemplo, en el caso de la Universidad de San Petersburgo, de los 19 TTLs que enviamos, solo recibimos respuesta de 8. Es probable que esto se deba a que los routers no están configurados para responder paquetes ICMP, o a una perdida de paquetes causada por, entre múltiples otras causas, congestión de red.

### 3.4. Detección de ISPs

Una ISP (Internet Service Provider) es una organización que se encarga de proveer internet. Durante nuestra experimentación, notamos que todas nuestras rutas siempre pasaban por ciertas IPs parecidas las cuales sospechábamos que pertenecían a nuestro ISP. Luego, pudimos corroborar que le pertenecen a Telecom. Cuando corrimos el código desde Colegiales, la IP empezaba con 195.22.199, y cuando corrimos desde Vicente Lopez, la IP empezaba con 195.22.220. Otra ISP que pudimos detectar es aquella que empieza con 89.221, por la cual pasamos para ir a Hong Kong y a Australia. Ésta IP también le pertenece a Telecom y está ubicada en Estados Unidos.

## 4. Conclusiones

En primer lugar, notamos que identificar saltos interoceánicos mediante el análisis de tiempos de respuesta altos no es una táctica infalible. Si bien suele funcionar, observamos muchos casos borde donde nos era difícil afirmar con certeza si el salto consistía o no en uno interoceánico. La variación en los RTT en algunos saltos pueden deberse a causas como congestión de la red, lo que hace mas difícil separar los saltos interoceánicos de los saltos a routers congestionados. Concluimos que deberíamos utilizar heurísticas mas complejas para distinguir tales saltos, como por ejemplo una implementación basada en el método de detección de outliers detallado por Cimbala.

Por otro lado, nuestro análisis de la estabilidad de cada trace muestra una estabilidad inesperada en las rutas que toma el trace a lo largo de múltiples iteraciones. Esto contrasta con nuestra expectativa inicial, donde esperábamos observar alguna inestabilidad, sea mínima o a gran escala, en alguno de nuestros experimentos.