DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

# TP2: Rutas en internet

Teoría de las Comunicaciones
Segundo Cuatrimestre de 2021


| Integrante | LU | Correo electrónico |
|---|---|---|
| Christian Nahuel Rivera | 184/15 | christiannahuelrivera@gmail.com |
| Guido Rodriguez Celma | 374/19 | guido.rc98@gmail.com |
| Miguel Rodriguez | 57/19 | mmiguerodriguez@gmail.com |






**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
https://exactas.uba.ar

# Índice

# 1. Introducción

En el presente trabajo nos propondremos analizar las rutas que siguen los paquetes del protocolo TCP/IP cuando el origen y el destino están en continentes distintos. Para esto nos valdremos del *Internet Control Message Protocol*, el cual provee los mensajes `Echo Request` y `Echo Reply` que sirven para probar la conexión entre dos dispositivos a partir de sus direcciones IP.

Los paquetes `ICMP` poseen un campo `TTL` (Time To Live) cuyo valor es decrementado por cada dispositivo que lo recibe y provoca que, al llegar a 0, el dispositivo descarte el paquete y envíe un mensaje de tipo `Time Exceeded` a la IP origen del mismo. A partir de esta funcionalidad deriva el algoritmo que usaremos para descubrir los dispositivos intermedios, entre el origen y el destino, por los que pasan los paquetes. Este algoritmo sigue los siguientes pasos:

1. Sea h la IP del host destino y variable ttl = 1.
2. Enviar un paquete `ICMP` de tipo `Echo Request` al host h cuyo campo `TTL` en el header IP sea igual a ttl.
3. Si se recibe una respuesta ICMP de tipo `Time Exceeded`, anotar la IP origen de dicho paquete. En otro caso, marcar como desconocido (*) el salto.
4. Incrementar ttl.
5. Repetir desde el paso 2 hasta obtener una respuesta ICMP de tipo Echo Reply por parte de h.

El código desarrollado para implementar este algoritmo se encuentra en el archivo `traceroute.ipynb`. En el mismo para cada TTL se envían paquetes de tipo `Echo Request`, midiendo el tiempo desde el instante antes de enviarlo hasta que se obtiene su respuesta u ocurre el timeout. Este tiempo es el *tiempo de viaje* del paquete a un destino y nos referiremos a él como `RTT` por ser la abreviatura de Round-Trip Time.

Este proceso se repite n veces con n el número de ráfagas seleccionado, en cada iteración se guarda en un diccionario la IP que contestó ("*" si no se obtuvo respuesta) junto a el número de veces que lo hizo y la suma de los RTTs para cada IP. Luego se obtiene la IP que más veces respondió para esta iteración, se calcula su RTT promedio y se agrega la tupla (IP, RTT) a la lista que se devolverá como resultado, donde la $i$-esima posicion corresponde a haber corrido el algoritmo para $TTL = i + 1$. Una vez que se obtiene una respuesta de tipo `Echo Reply` (significando que se llegó a destino) o que se superó el límite de TTL permitido, termina el algoritmo.

# 2. Análisis de rutas

En esta sección vamos a probar la herramienta desarrollada anteriormente para analizar rutas que realizan los paquetes de datos al conectarse a sitios web de universidades en diferentes continentes. Estas rutas pueden atravesar más de un continente, y esos caminos pasar por enlaces que cruzan océanos.

Para realizar el calculo de RTTs entre saltos que usaremos en la experimentación desarrollamos la función `RTTEntreSaltos` que toma como parámetro la lista resultado de la función `traceroute` explicada anteriormente y calcula, para cada posición $i$ de la lista de resultados, la diferencia de RTTs con la posición $j$, con $i > j$. Si la diferencia es negativa se hace el mismo calculo aumentando el $j$ hasta conseguir una diferencia positiva o alcanzar el final de la lista.

Para todos los experimentos el algoritmo de `traceroute` fue ejecutado con los siguientes valores para sus parámetros:

- Máximo TTL: 30.
- Numero de Ráfagas: 30.
- Timeout: 0.8s.

## 2.1. Universidad de Kobe

En este experimento elegimos analizar la ruta hacia el sitio web de la Universidad de Kobe (www.shoin.ac.jp), ubicada en la bahía de Osaka en Japón central. Las muestras de paquetes fueron tomadas un día viernes alrededor de las 14hs (GMT-3).

| **TTL** | **Host más común** | **TTL** | **Host más común** |
|---|---|---|---|
| 0 | 192.168.0.1 | 9 | 129.250.4.143 |
| 1 | 10.32.128.1 | 10 | 129.250.3.22 |
| 2 | 10.242.2.145 | 11 | 203.105.73.106 |
| 3 | 192.168.64.66 | 12 | * |
| 4 | 185.70.203.38 | 13 | * |
| 5 | * | 14 | * |
| 6 | 149.3.181.65 | 15 | * |
| 7 | 129.250.2.12 | 16 | 49.212.73.215 |
| 8 | 129.250.6.177 | - | - |

Cuadro 1: Host más común por TTL hacia la Universidad de Kobe

Observamos que la ruta toma 16 saltos hasta llegar a destino. De estos 16 hay 5 valores de `TTL` para los cuales no se obtuvo respuesta, aproximadamente un 32 %. A continuación presentamos los RTTs obtenidos entre saltos, notar que seleccionamos aquellos para los cuales la diferencia de RTT es positiva.

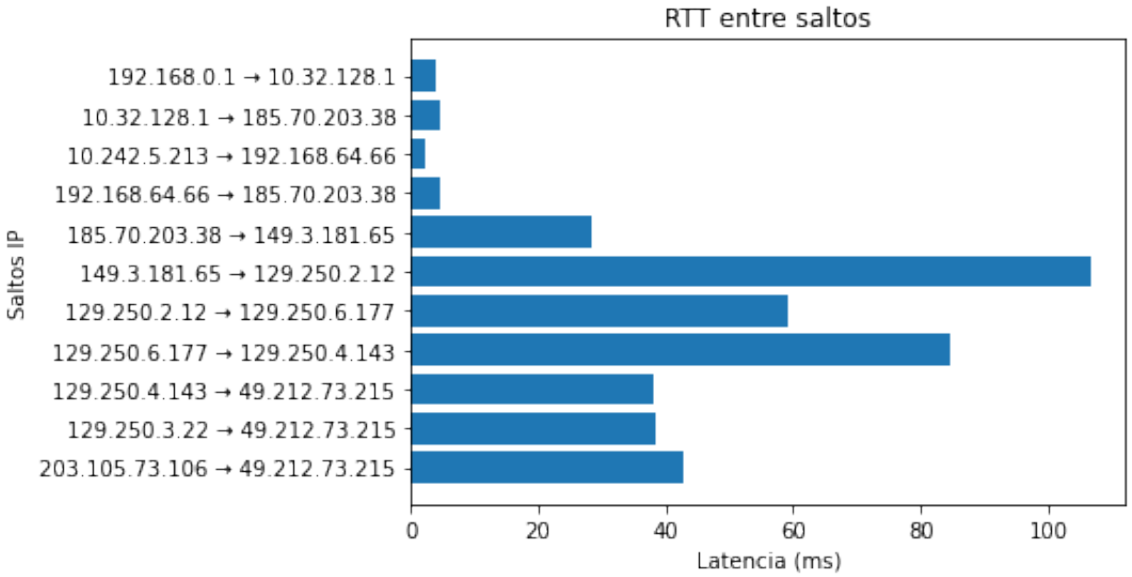


Figura 1: RTTs entre saltos con ruta hacia Japón

A partir de los Round Trip Times calculados, podemos conjeturar que los saltos interoceánicos se dan entre:

- `149.3.181.65` ⟶ `129.250.2.12`
- `129.250.2.12` ⟶ `129.250.6.177`
- `129.250.6.177` ⟶ `129.250.4.143`

Esta hipótesis se debe a que la diferencia de RTTs entre estas direcciones es notoriamente mayor que entre las demás. Utilizando una herramienta de geolocalización IP [5], encontramos que las mismas tienen las siguientes ubicaciones geográficas:

- `149.3.181.65`: San Pablo, Brasil
- `129.250.2.12`: Nueva York, EEUU
- `129.250.6.177`: Seattle, EEUU
- `129.250.4.143`: Tokio, Japón

Observamos que las direcciones IP `129.250.2.12`, `129.250.6.177` y `129.250.4.143` pertenecen a la empresa de telecomunicaciones japonesa "Nippon Telegraph & Telephone Corporation" [1]. En particular esta empresa es dueña del cable submarino *Pacific Crossing 1* [2], que une las ciudades de Seattle y Tokio.

Además la dirección IP `149.3.181.65` también es de una empresa de telecomunicaciones, en este caso "Telecom Italia Sparkle" [3]. Esta empresa es un backbone nivel 1 y dueña del cable submarino *Seabras-1* [4], que conecta directamente San Pablo con Nueva York.

Notamos que los saltos de mayor RTT se corresponden con los interoceánicos, aquel entre San Pablo y Nueva York y Seattle y Tokio. El otro salto destacado es el que conecta las costas Este y Oeste de EEUU que si bien no es interoceánico recorre una gran cantidad de kilómetros. A continuación presentamos un mapa cuyos puntos numerados representan el recorrido en orden de los paquetes ICMP:

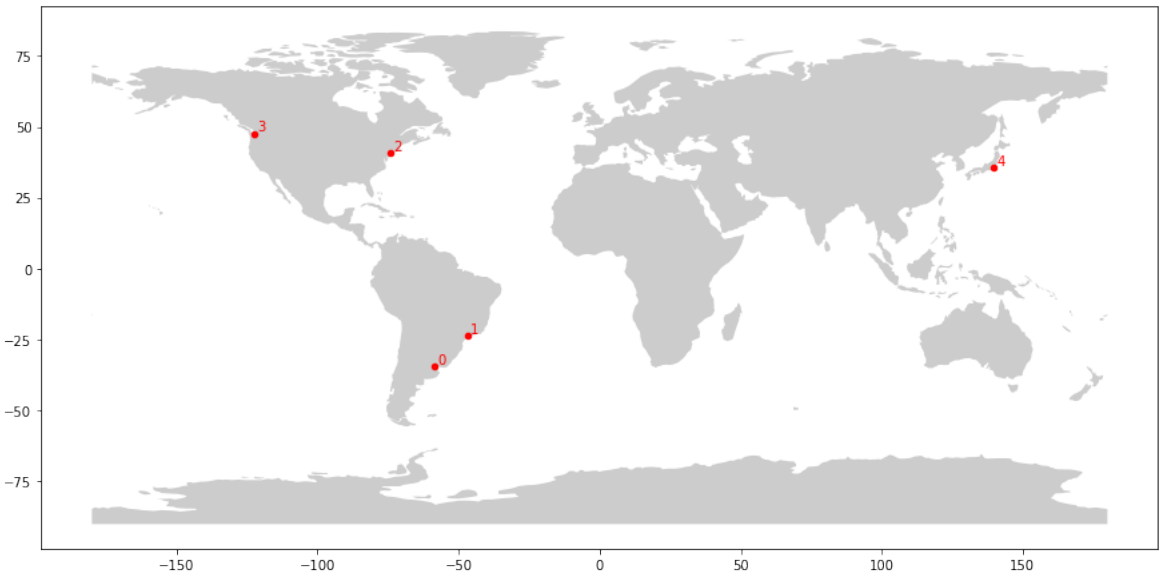


Figura 2: Recorrido ICMP hacia la Universidad de Kobe

Teniendo en cuenta la trama global de cables submarinos, vemos que el recorrido obtenido es uno válido. Otro posible recorrido hubiera sido ir de Buenos Aires a Chile, de Chile directamente a la costa oeste de EE.UU y finalmente a Japón.

## 2.2. Universidad de Madrid

Para este experimento, vamos a analizar el recorrido de los paquetes hasta llegar al servidor donde se encuentra el sitio de la Universidad Autónoma de Madrid (www.uam.es) ubicado en Madrid, España. Las muestras fueron tomadas un día sábado a las 12:30hs (GMT-3).

| TTL | Host más común | TTL | Host más común |
|---|---|---|---|
| 0 | 172.23.48.1 | 10 | 109.105.102.98 |
| 1 | 192.168.0.1 | 11 | * |
| 2 | * | 12 | * |
| 3 | * | 13 | * |
| 4 | * | 14 | 62.40.98.72 |
| 5 | * | 15 | 83.97.88.130 |
| 6 | 181.96.113.234 | 16 | 130.206.216.2 |
| 7 | 195.22.220.56 | 17 | 193.145.14.13 |
| 8 | 195.22.209.198 | 18 | * |
| 9 | 195.66.225.24 | 19 | 150.244.214.237 |

Cuadro 2: Host más común por TTL hacia la Universidad de Madrid

Podemos observar en el cuadro 2 que de los 20 TTL que se utilizaron para llegar a destino, para 8 saltos no se encontró respuesta, aproximadamente el 40 %. El largo de la ruta en términos de los saltos que responden correctamente es de 12. En el siguiente gráfico podemos ver el RTT entre saltos:

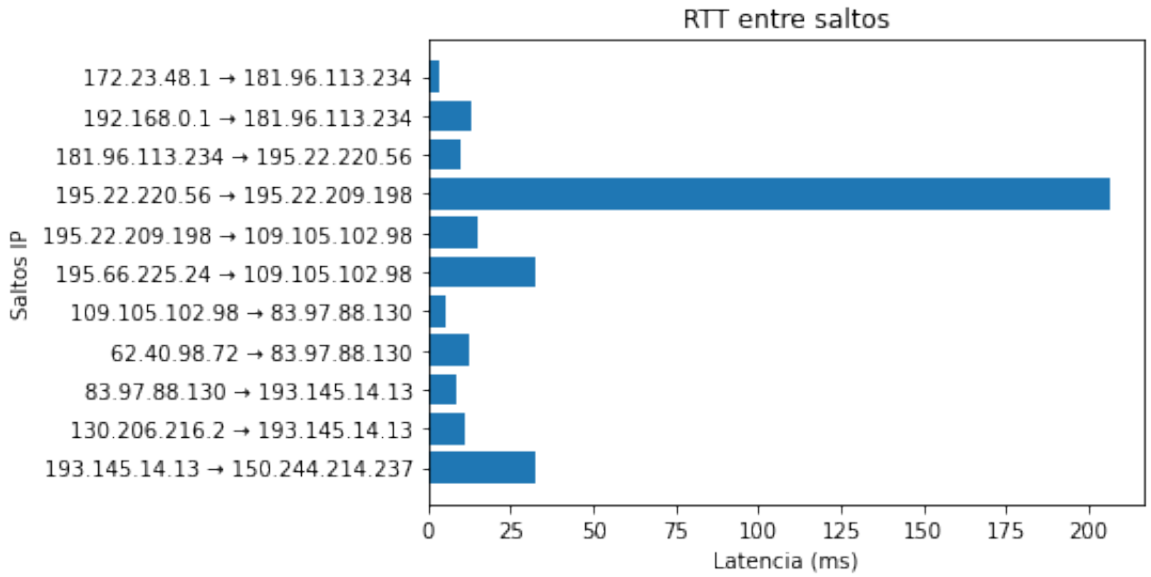


Figura 3: RTTs entre saltos hacia la Universidad de Madrid

Podemos observar en la figura 3 que la mayoría de los saltos no tienen una gran latencia, por lo que pueden significar saltos entre ciudades o países cercanos. Además, podemos ver que entre las direcciones IP 195.22.220.56 y 195.22.209.198 hay una latencia promedio de mas de 200 milisegundos, esto es un indicador de que la conexión entre esas dos direcciones es a través de un enlace interoceánico.

Haciendo un análisis mas en profundidad la dirección IP 195.22.220.56 pertenece a una compañía de telecomunicaciones global llamada “Telecom Italia Sparkle” [3], al igual que

vimos en el caso anterior con la Universidad de Kobe. Esta empresa tiene en Buenos Aires su "TI Sparkle Seabone Buenos Aires POP" que es uno de los que provee a los ISPs para establecer comunicaciones a nivel global. En este caso es probable que la dirección IP 195.22.220.56 esté conectada directamente con 195.22.209.198 a través de un cable interoceánico manejado por esta empresa. En la siguiente figura podemos observar el recorrido de los paquetes hasta llegar a destino:

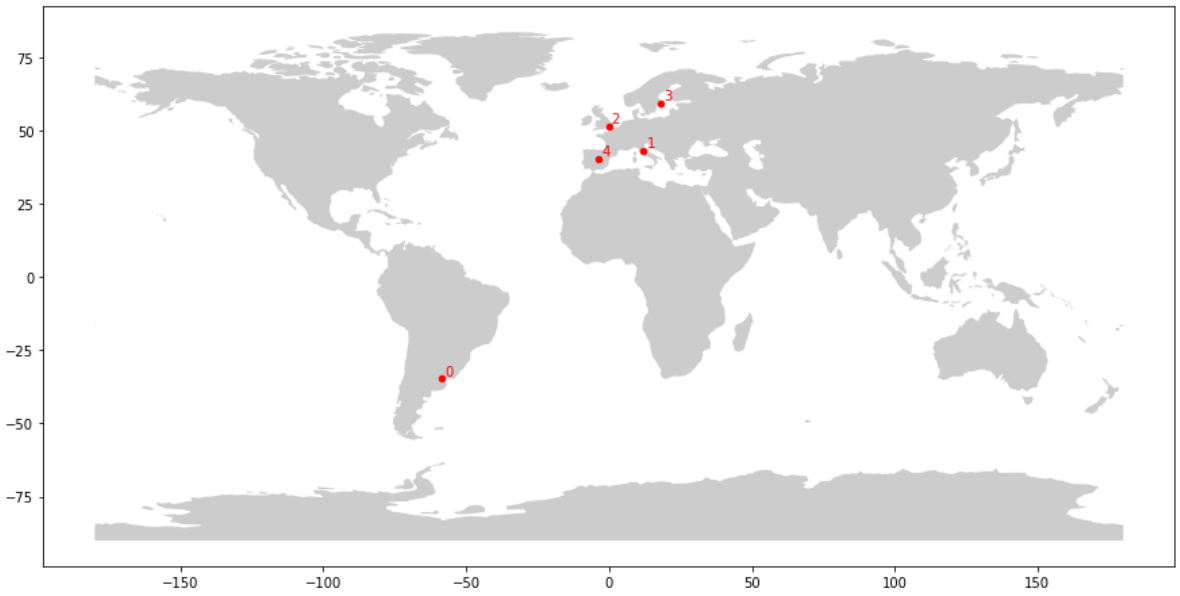


Figura 4: Recorrido ICMP hacia la Universidad de Madrid

Podemos ver que el paquete sigue el camino de Buenos Aires a Italia a través del backbone mencionado anteriormente. Después de llegar a Italia ocurre un comportamiento anómalo con el recorrido del paquete ya que no se utiliza una ruta que vaya directamente a Madrid sino que se salta a Reino Unido, para luego ir a Suecia y finalmente llegar al servidor en Madrid, España.

Este comportamiento no es algo esperado ya que creemos que debería haber una conexión directa entre Italia y España, pero por alguna razón se están utilizando rutas hacia otros países para llegar al destino. Aunque estos saltos no implican una latencia mucho mayor, creemos que si pudiésemos obtener un salto desde Italia a España la conexión al sitio web seria más performante que la actual.

## 2.3. Instituto Indio de Tecnología de Delhi

Para este experimento buscamos una universidad en la India. Probamos con varias de las principales universidades y con muchas de ellas nos sorprendimos encontrando que no tenían completamente activado el protocolo ICMP ya que los servidores donde tienen sus páginas hosteadas o no responden al mensaje de `ping` o no terminan de responder `Echo Reply`. Al margen de ello encontramos un Instituto con el que sí pudimos hacer nuestras pruebas y

es el Tecnológico de Delhi (www.iitd.ac.in) ubicado en Hauz Khas, New Delhi, India. Las muestras se hicieron un día viernes a las 15:30hs (GMT-3).

| TTL | Host más común | TTL | Host más común |
|---|---|---|---|
| 0 | 192.168.1.1 | 14 | 216.6.87.43 |
| 1 | 190.210.239.253 | 15 | 216.6.57.5 |
| 2 | 190.210.118.118 | 16 | 209.58.124.6 |
| 3 | 190.210.118.158 | 17 | * |
| 4 | 200.51.235.61 | 18 | 14.140.210.22 |
| 5 | 200.51.240.61 | 19 | * |
| 6 | 213.140.39.116 | 20 | * |
| 7 | 176.52.255.29 | 21 | * |
| 8 | 94.142.97.65 | 22 | 103.27.9.24 |
| 9 | 94.142.119.188 | 23 | 103.27.9.24 |
| 10 | 66.110.72.30 | 24 | 103.27.9.24 |
| 11 | 63.243.152.61 | 25 | - |
| 12 | 66.198.154.177 | 26 | - |
| 13 | 63.243.137.133 | 30 | - |

Cuadro 3: Host más común por TTL hacia el Institulo tecnológico de Delhi

De los datos mostrados en el cuadro 3 se pueden destacar algunos hechos relevantes. Hasta el salto número 22 únicamente 4 hosts no respondieron siguiendo el protocolo ICMP. En este caso tenemos un comportamiento extraño en que la IP del sitio web responde `Timeout` 2 veces antes de responder `Echo Reply`. A continuación analizaremos los RTT entre los saltos:

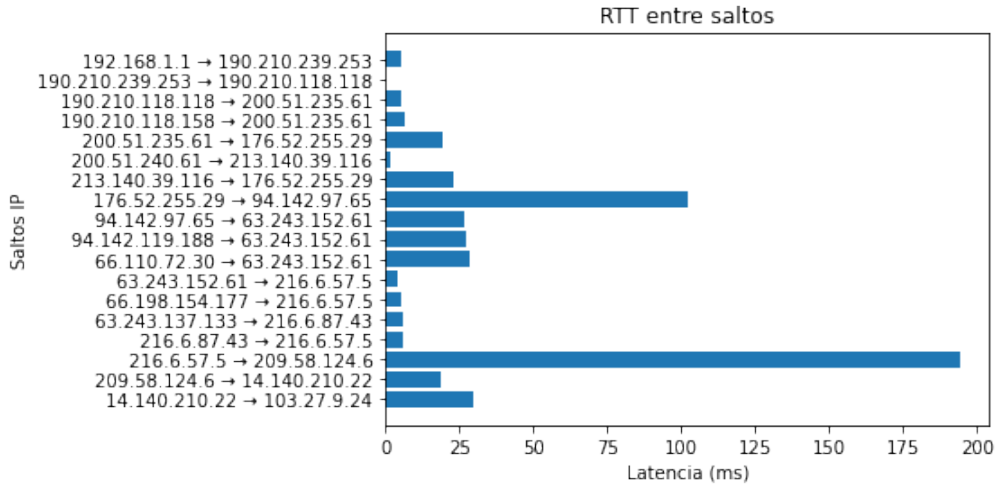


Figura 5: Recorrido ICMP hacia el Institulo tecnológico de Delhi

Analizando el gráfico podemos observar que a simple vista parece haber dos saltos inter-oceánicos: entre 176.52.255.29 y 94.142.97.65 y entre 216.6.57.5 y 209.58.124.6.

Para el primer salto, la IP 176.52.255.29 está gestionada por el prestador ISP "Telefonica Global Solutions" en San Pablo, Brasil, mientras que la IP 94.142.97.65 está gestionada por el mismo prestador pero en la ciudad de Miami, EEUU. Esto tiene sentido ya que Telefónica trabaja con Telxius que gestiona cables submarinos por toda América Latina y Estados Unidos, entre ellos el *SAm-1* que probablemente sea el que está siendo utilizado en esta ocasión [6].

Luego para el segundo salto entre 216.6.57.5 y 209.58.124.6 nos encontramos que ambos hosts están muy separados pero son propiedad de una misma empresa que gestiona cables transatlánticos en todo el mundo. En este caso el primer host está ubicado en Virginia, EEUU y el segundo host en Mumbai, India y la empresa responsable de este enlace es Tata Communications [7].

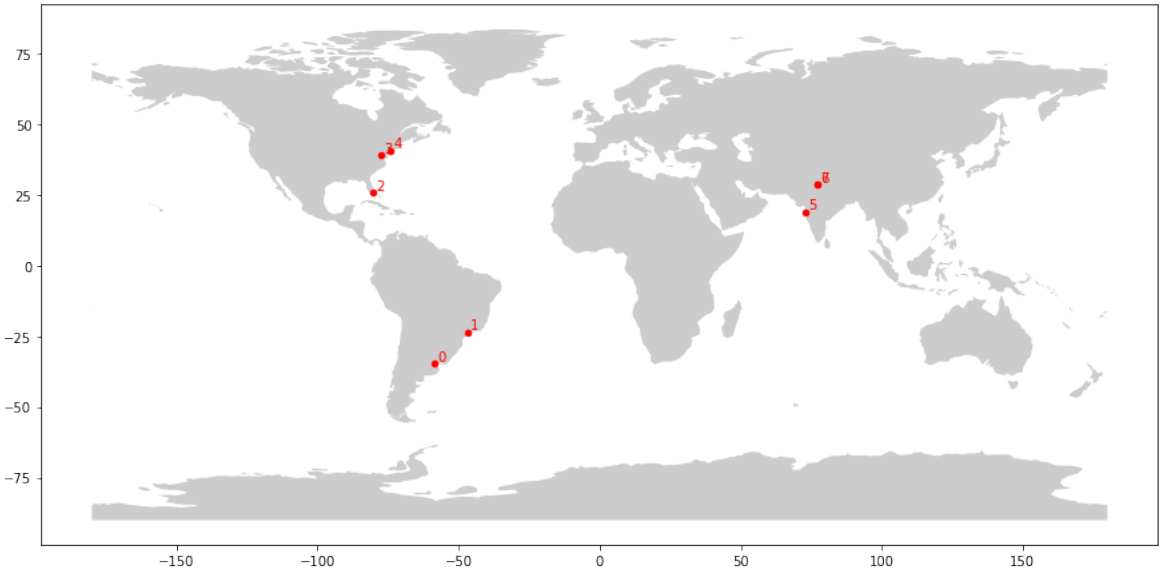


Figura 6: Host visibles en la conexión entre Buenos Aires y el Instituto tecnológico de Delhi

Observamos que la ruta obtenida tiene un recorrido acorde a los cables submarinos existentes, aunque no obtuvimos información de los saltos intermedios entre EE.UU y la India.

Los saltos que analizamos previamente como saltos interoceánicos son el punto *1 a 2* y el *4 a 5* que corresponden a los pares de IP previamente citadas. Entre los pares de puntos que reconocemos como saltos interoceánicos nos encontramos con que faltan algunos hosts intermedios según el mapa de cables submarinos [9]. En los términos del autor del paper [10], esta es una inconsistencia inevitable desde el usuario que analiza las redes porque por optimizaciones en el balanceo de tráfico de redes, grupos de paquetes que van direccionados a un mismo host no muestran información de hosts intermedios por los que pasan.

# 3. Detección de enlaces interoceánicos

Algo que resulta interesante a partir de poder graficar los RTTs entre los saltos IP es que podemos realizar una herramienta que detecte automáticamente enlaces interoceánicos a partir de analizar si aparecen o no valores atípicos en este conjunto de datos. Para esto, vamos a utilizar la técnica propuesta por Cimbala [8] para detectar estos valores en una muestra con única variable, ya que únicamente tenemos las latencias entre dos direcciones IP.

## 3.1. Universidad de Moscú

Utilizamos el algoritmo implementado en la ruta hacia la Universidad de Moscú (www.msu.ru). El recorrido de los paquetes ICMP fue el siguiente:


Figura 7: Recorrido ICMP hacia la Universidad de Moscú

Además, los RTT obtenidos entre direcciones IP fueron los siguientes:

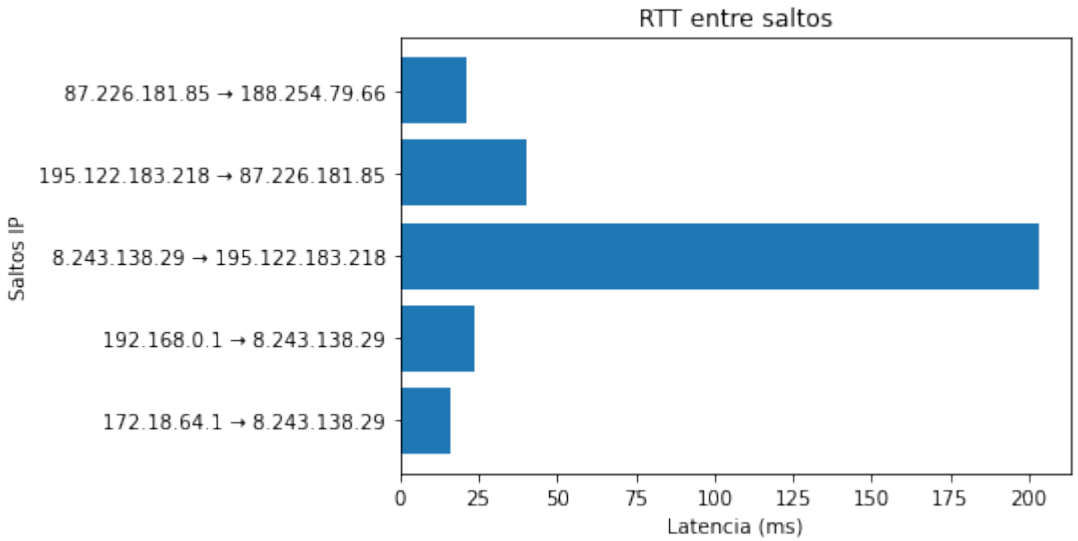


Figura 8: RTT entre IPs hacia la Universidad de Moscú

Los outliers detectados se pueden observar en la siguiente tabla:

| **IP origen** | **IP destino** | **Latencia (ms)** |
|---|---|---|
| 172.18.64.1 | 8.243.138.29 | 16.046186 |
| 8.243.138.29 | 195.122.183.218 | 203.043471 |
| 195.122.183.218 | 87.226.181.85 | 40.272593 |

Cuadro 4: Outliers detectados hacia la Universidad de Moscú

Podemos ver que el método propuesto por Cimbala para esta muestra obtuvo como outliers a los saltos entre las direcciones 172.18.64.1 y 8.243.138.29, 8.243.138.29 y 195.122.183.218 y entre 195.122.183.218 y 87.226.181.85. El salto entre las IPs 172.18.64.1 y 8.243.138.29 no es un salto interoceánico ya que la IP origen es una dirección privada del ordenador que hizo la prueba y la de destino es una dirección IP en Córdoba, Argentina. El resto de los outliers detectados se corresponden exactamente con los enlaces interoceánicos entre Buenos Aires y Texas y entre Texas y Alemania que podemos observar en el mapa de los recorridos en la figura 7.

En este caso utilizando el método Cimbala hubo un falso positivo pero ningún falso negativo ya que el algoritmo detecto los enlaces interoceánicos mas allá del primero que era incorrecto.

## 3.2. Universidad de Singapur

En este caso aplicamos el algoritmo sobre la ruta hacia el Management Development Institute de Singapur (www.mdis.edu.sg). El recorrido de los paquetes ICMP fue el siguiente:

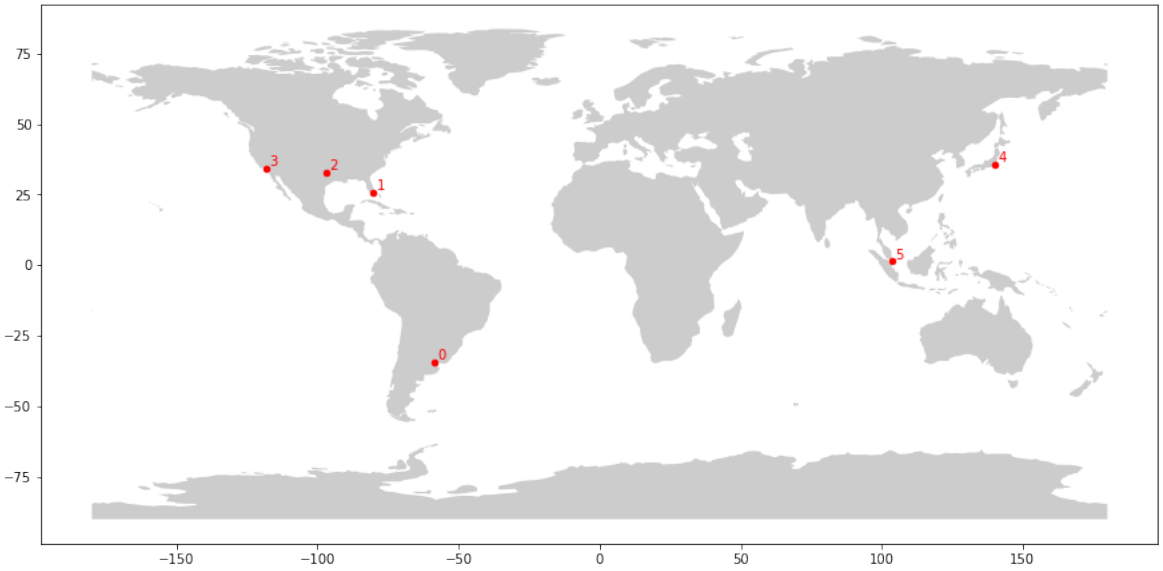


Figura 9: Recorrido ICMP hacia la Universidad de Singapur

Los Round trip Times entre saltos estan dados por:

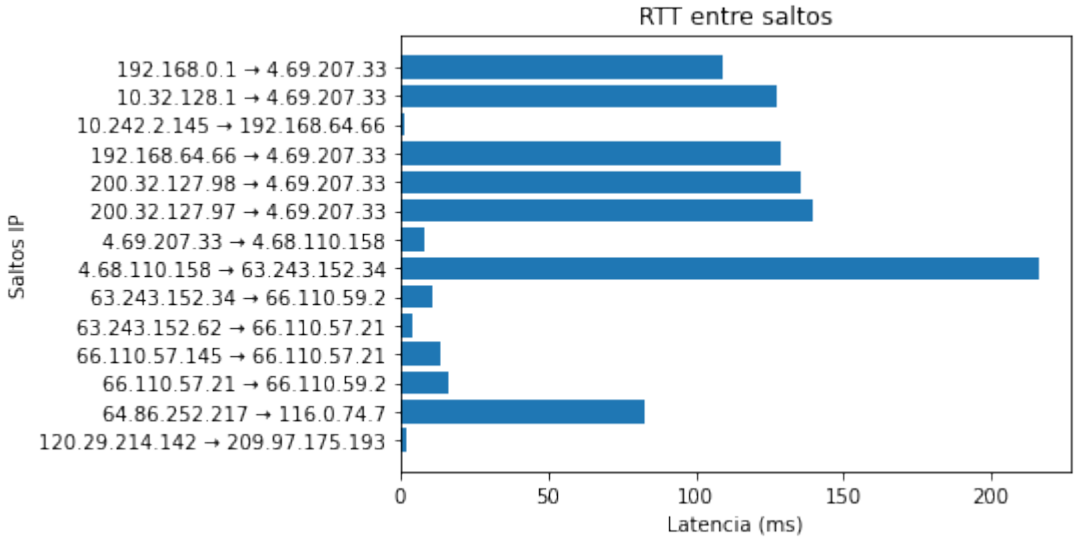


Figura 10: RTT entre IPs hacia la Universidad de Singapur

Los outliers detectados fueron los siguientes:

| IP origen | IP destino | Latencia (ms) |
|---|---|---|
| 172.30.160.1 | 181.96.113.254 | 351.714298 |
| 192.168.0.1 | 181.96.113.254 | 352.967191 |
| 4.68.110.158 | 66.110.72.46 | 190.474188 |
| 8.243.138.29 | 4.69.207.33 | 115.051579 |
| 64.86.252.59 | 116.0.74.7 | 70.264808 |
| 66.110.72.46 | 66.110.57.145 | 30.499659 |
| 181.96.113.254 | 66.110.57.145 | 17.357639 |
| 116.0.74.7 | 180.87.98.37 | 1.934645 |

Cuadro 5: Outliers detectados hacia la Universidad de Singapur

En este caso usando el método Cimbala se encuentran 8 outliers, sin embargo los únicos saltos interoceánicos se dan en:

- `8.243.138.29 (Buenos Aires)` $\longrightarrow$ `4.69.207.33 (Miami)`
- `64.86.252.59 (Tokio)` $\longrightarrow$ `116.0.74.7 (Singapur)`.

Es decir que se tuvo 6 falsos positivos y un falso negativo que sería el salto interoceánico entre `Los Ángeles` y `Tokio`.

Notamos que usando una ruta más larga se obtiene una muestra más grande para analizar, lo cual puede dar resultados más precisos. Sin embargo en rutas intercontinentales suelen usarse routers con tráfico alto, por lo que la variación de latencia entre IPs puede ser muy grande y generar inconsistencias, creemos que este fue el caso en la prueba de Singapur.

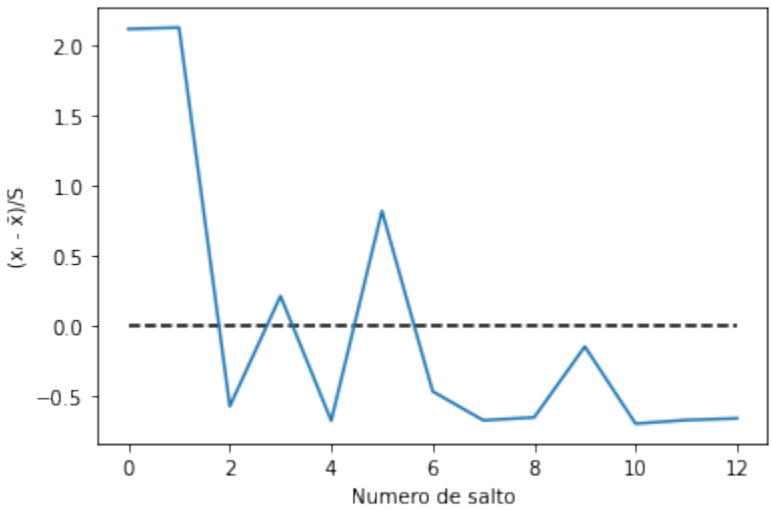


Figura 11: Medidas de dispersión entre saltos hacia Universidad de Singapur

Observamos en la figura 11 que, aún eligiendo un punto de corte fijo considerando la ubicación de los enlaces interoceánicos, seguiríamos obteniendo falsos positivos y negativos debido a las inconsistencias en los tiempos de respuesta obtenidos.

# 4. Conclusiones

En el trabajo desarrollado pudimos ver que a través de una herramienta y simples mensajes utilizando el protocolo ICMP es posible conocer parcialmente el recorrido que un paquete hace desde el origen hasta su destino. Con esta motivación también comprendimos en rasgos generales la topología de las comunicaciones en hosts que se encuentran alrededor del mundo. Además, observamos que estos recorridos pueden tener varios saltos entre distintos países y continentes, siendo así difícil de predecir su recorrido.

Este trabajo nos sirvió para tener una primer introducción al rastreo de paquetes y topología de redes, así también comprender las complicaciones que esto involucra para poder tener un análisis realmente riguroso y los posibles problemas que nos podemos encontrar que requieren un estudio mucho mayor al presente trabajo.

Finalmente, utilizando la herramienta de detección de outliers en la sección 3 pudimos a partir del recorrido y las latencias entre distintos saltos detectar si estos correspondían a enlaces interoceánicos. Observamos que el método de Cimbala tiene la capacidad de detectar parcialmente estos comportamientos, pero al tener un conjunto acotado y variable de datos, puede no funcionar de forma esperada.

# Referencias


[1] NTT - `https://group.ntt/en/`

[2] PC-1 - `https://en.wikipedia.org/wiki/PC-1`

[3] Sparkle - `https://www.tisparkle.com/`

[4] Seabras-1 - `https://www.tisparkle.com/Seabras-1`

[5] IPinfo - `https://ipinfo.io`

[6] Telxius LATAM cables - `https://telxius.com/cable/otros-cables/`

[7] India Tata Communications - `https://shorturl.at/hjFJU`

[8] Cimbala - `https://www.me.psu.edu/cimbala/me345/Lectures/Outliers.pdf`

[9] Cables interoceánicos, mapa interactivo - `https://www.submarinecablemap.com/`

[10] Traceroute Anomalies - `link`