Teoría de las Comunicaciones

Primer Cuatrimestre de 2013

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

Tp2: capa de red

Grupo:

Integrante	LU	Correo electrónico
Andrés Laurito	27/11	andy.laurito@hotmail.com
Matías Capello	006/02	matiascapello@gmail.com
Santiago Hernández	48/11	santi-hernandez@hotmail.com

Índice

Índice de figuras

Abstract

Hacer abstract

1. Introducción

En este taller nos proponemos experimentar con herramientas y técnicas frecuentes a nivel de red. Más particularmente nos centraremos en dos muy conocidas y utilizadas: `ping` y `traceroute`. El objetivo es entender los protocolos involucrados. Para ello, desarrollaremos nuestras propias implementaciones de las herramientas de manera de afianzar los conocimientos. Todo lo anterior se realizará en un marco analítico que nos permitirá razonar sobre lo hecho y comprender mejor qué pasa detrás de bambalinas.

1.1. ICMP

El Protocolo de Mensajes de Control de Internet o ICMP es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta `ping` y `traceroute`, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

Los mensajes ICMP son comúnmente generados en respuesta a errores en los datagramas de IP o para diagnóstico y ruteo. IP encapsula el mensaje ICMP apropiado con una nueva cabecera IP (para obtener los mensajes de respuesta desde el host original que envía), y transmite el datagrama resultante de manera habitual.

Por ejemplo, cada router que reenvía un datagrama IP tiene que disminuir el campo de tiempo de vida (TTL) de la cabecera IP en una unidad; si el TTL llega a 0, un mensaje ICMP "Tiempo de Vida se ha excedido en transmitirse" es enviado a la fuente del datagrama. Cada mensaje ICMP es encapsulado directamente en un solo datagrama IP, y por tanto no garantiza la entrega del ICMP. Aunque los mensajes ICMP son contenidos dentro de datagramas estándar IP, los mensajes ICMP se procesan como un caso especial del procesamiento normal de IP, algo así como el procesamiento de un sub-protocolo de IP. En muchos casos es necesario inspeccionar el contenido del mensaje ICMP y entregar el mensaje apropiado de error a la aplicación que generó el paquete IP original, aquel que solicitó el envío del mensaje ICMP.

La utilidad del protocolo ICMP es controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado.

Muchas de las utilidades de red comunes están basadas en los mensajes ICMP. El comando `traceroute` está implementado transmitiendo datagramas UDP con campos especiales TTL IP en la cabecera, y buscando los mensajes de "Tiempo de Vida en tránsito" y "Destino inalcanzable" generados como respuesta. La herramienta `ping` está implementada utilizando los mensajes "Echo request" y "Echo reply" de ICMP.

1.2. Ping

Como programa, `ping` es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

Ejecutando `ping` de solicitud, el Host local envía un mensaje ICMP, incrustado en un paquete IP. El mensaje ICMP de solicitud incluye, además del tipo de mensaje y el código del mismo, un número identificador y una secuencia de números, de 32 bits, que deberán coincidir con el mensaje ICMP de respuesta; además de un espacio opcional para datos. Muchas veces se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos.

1.3. Traceroute

`traceroute` es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de red). Se obtiene además una estadística del RTT o latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación.

Entre los datos que se obtienen están: el número de salto, el nombre y la dirección IP del nodo por el que pasa y el tiempo de respuesta para los paquetes enviados (un asterisco indica que no se obtuvo respuesta).

`traceroute` utiliza el campo Time To Live (TTL) de la cabecera IP. Este campo sirve para que un paquete no permanezca en la red de forma indefinida (por ejemplo, debido a la existencia en la red de un bucle cerrado en la ruta). El campo TTL es un número entero que es decrementado por cada nodo por el que pasa el paquete. De esta forma, cuando el campo TTL llega al valor 0 ya no se reenviará más, sino que el nodo que lo esté manejando en ese momento lo descartará. Lo que hace `traceroute` es mandar paquetes a la red de forma que el primer paquete lleve un valor TTL=1, el segundo un TTL=2, etc. De esta forma, el primer paquete será eliminado por el primer nodo al que llegue (ya que éste nodo decrementará el valor TTL, llegando a cero). Cuando un nodo elimina un paquete, envía al emisor un mensaje de control especial indicando una incidencia. `traceroute` usa esta respuesta para averiguar la dirección IP del nodo que desechó el paquete, que será el primer nodo de la red. La segunda vez que se manda un paquete, el TTL vale 2, por lo que pasará el primer nodo y llegará al segundo, donde será descartado, devolviendo de nuevo un mensaje de control. Esto se hace de forma sucesiva hasta que el paquete llega a su destino.

2. Desarrollo

2.1. Implementación ping

Para la implementación de ping utilizamos scapy en python para armar y enviar un paquete ip con el destino deseado, de tipo ICMP echo request.
Al momento de enviar el paquete iniciamos un contador y al obtener respuesta lo detenemos, de forma de obtener su RTT.

2.2. Implementación traceroute

La implementación de traceroute consiste en comenzando con ttl = 1, enviar tres pings a la ip destino, de forma que si el tiempo de vida del mensaje llega a cero antes de llegar al destino, el salto intermedio nos envia un mensaje informandonos que el paquete expiró. Así es que incrementando el ttl en uno sucesivamente obtenemos respuesta de los hops intermedios.
El motivo por el cual enviamos tres pings con el mismo ttl es para agregar confiabilidad a la respuesta obtenida, debido a que podríamos no obtener respuesta o el paquete podría seguir una ruta alternativa.
Para realizar los análisis pedidos en el trabajo desarrollamos un traceroute que presenta el número de cada hop en la ruta al destino, la IP del hop, su RTT, coordenadas terrestres, distancia al hop anterior, distancia hasta ese hop, el RTT teórico esperado hasta él y al finalizar el traceroute generamos un mapa mostrando el recorrido realizado por los paquetes para llegar hasta el destino.

2.2.1. Geolocalización direcciones IP

Para geolocalizar la dirección IP de las respuestas obtenidas al hacer el traceroute utilizamos el servicio gratuito provisto por **dazzlepod.com/ip** una vez obtenida la respuesta, quien nos devuelve entre otros datos, las coordenadas terrestres aproximadas de la posición de la ip en un json.
Luego notamos que si bien este es un buen servicio las posiciones provistas no son tan precisas como el de **ip2location.com**, por lo que para gráficar la posición final de los enlaces encontrados, utilizamos este ultimo, que como desventaja solo permite una cantidad limitada de usos diarios a modo de demostración.

2.2.2. Calculo de la distancia entre coordenadas

Una vez obtenidas las coordenadas terrestres de los hops del traceroute utilizamos la **fórmula del haversine** para calcular la distancia en kilómetros entre un hop y el anterior.
Fórmula de Haversine $= 2 * r * arcsin\left(\sqrt{sin^2\left(\frac{\phi_1-\phi_2}{2}\right) + cos(\phi_1) * cos(\phi_2) * sin^2\left(\frac{\lambda_1-\lambda_2}{2}\right)}\right)$

Donde r es el radio medio de la tierra en kilómetros (en nuestra implementación utilizamos 6371Km), ϕ_1 y ϕ_2 son la latitud de la coordenada 1 y 2, respectivamente, y λ_1 y $\lambda 2$ son la longitud de la coordenada 1 y 2.

2.2.3. Calculo del RTT real y teórico

Para calcular el RTT mínimo suponiendo que los enlaces son de fibra óptico, siendo su tiempo de propagación de $2 * 10^5 Km/s$, tomamos la distancia en kilómetros entre los nodos calculadas anteriormente y la dividimos por el tiempo de propagación.

Por otro lado para calcular el RTT real aproximado iniciamos un contador antes de enviar el paquete y lo detenemos al obtener su respuesta correspondiente.

2.2.4. Gráfico mapa traceroute

Una vez terminado el traceroute utilizamos la api de **google static maps** para obtener graficamente en un mapamundi el recorrido realizado para alcanzar el destino. El servicio nos devuelve una imagen en formato png, la cual guardamos, luego de hacer un request a la dirección base de google static maps añadiendole los pins y caminos a agregar.

Para hacer el pedido utilizamos la dirección base
http://maps.googleapis.com/maps/api/staticmap?zoom=1&size=600x400&scale=2&sensor=false&maptype=roadmap
a la cual le agregamos para cada ip que contesto un pin: &markers=label:**label**|**latidud**,**longitud**, y finalmente trazamos los caminos entre las ips que contestaron una después de la otra, también agregando a la dirección &path=color:0xff0000|weight:2| seguido de las coordenadas de cada ip separadas por un pipe (|).

Una descripción detallada del uso de google static maps se puede encontrar en:
https://developers.google.com/maps/documentation/staticmaps/

3. Resultados

Aclaraciones:

Para la obtención de los resultados hicimos traceroutes a direcciones ips pertenecientes a sitios web hosteados en Europa. También experimentamos bastante con sitios de Asia, Oceania y Africa, aunque estos no fueron utilizados para los resultados ya que no obtuvimos enlaces transatlánticos distintos a los obtenidos con los sitios Europeos y notamos un mayor tiempo de respuesta hacia estos.

Una vez obtenidos los enlaces, para obtener la variación del RTT hacia los mismos a lo largo del día realizamos 20 pings sucesivos a cada enlace, cada 1 hora, durante 24 horas, y consideramos el promedio de esos pings. En caso de obtener un timeout entre los 20 pings, dicho ping fue descartado a la hora de sacar el promedio.

3.1. Enlaces transatlánticos

Figura 1: Enlaces transatlánticos

A pesar de realizar muchas pruebas con traceroute a varias universidades al otro lado del Atlántico, sólo pudimos observar 2 enlaces transatlánticos diferentes, uno al apuntar a la University of London, que utilizó un enlace entre Miami y Londres, y el otro al apuntar a la Universidade de Cabo Verde, que usa un enlace entre Nueva York y Londres. El resto de los sitios probados usaba uno esos dos enlaces, o los datos que obteniamos no eran coherentes con lo esperado por un enlace submarino.

Pin	Dirección IP	Coordenadas	Distancia total recorrida hasta él en Km	RTT mínimo en ms
1	213.200.84.37	(25.77427,-80.19366)	7097	35.485
2	141.136.107.41	(51.50853,-0.12574)	11130	55.65
3	94.142.122.217	(40.71427,-74.00597)	8527	42.635
4	84.16.12.21	(51.50853,-0.12574)	11130	55.65
5	66.110.9.61	(25.77427,-80.19366)	12224.18	61.12
6	80.231.158.42	(38.71667,-9.13333)	17491.59	87.45

Enlace	Distancia en Km	RTT mínimo en ms
1 - 2	7126	35.63
3 - 4	5570	27.85
5 - 6	6671	33.35

3.2. Variación del RTT a lo largo del día

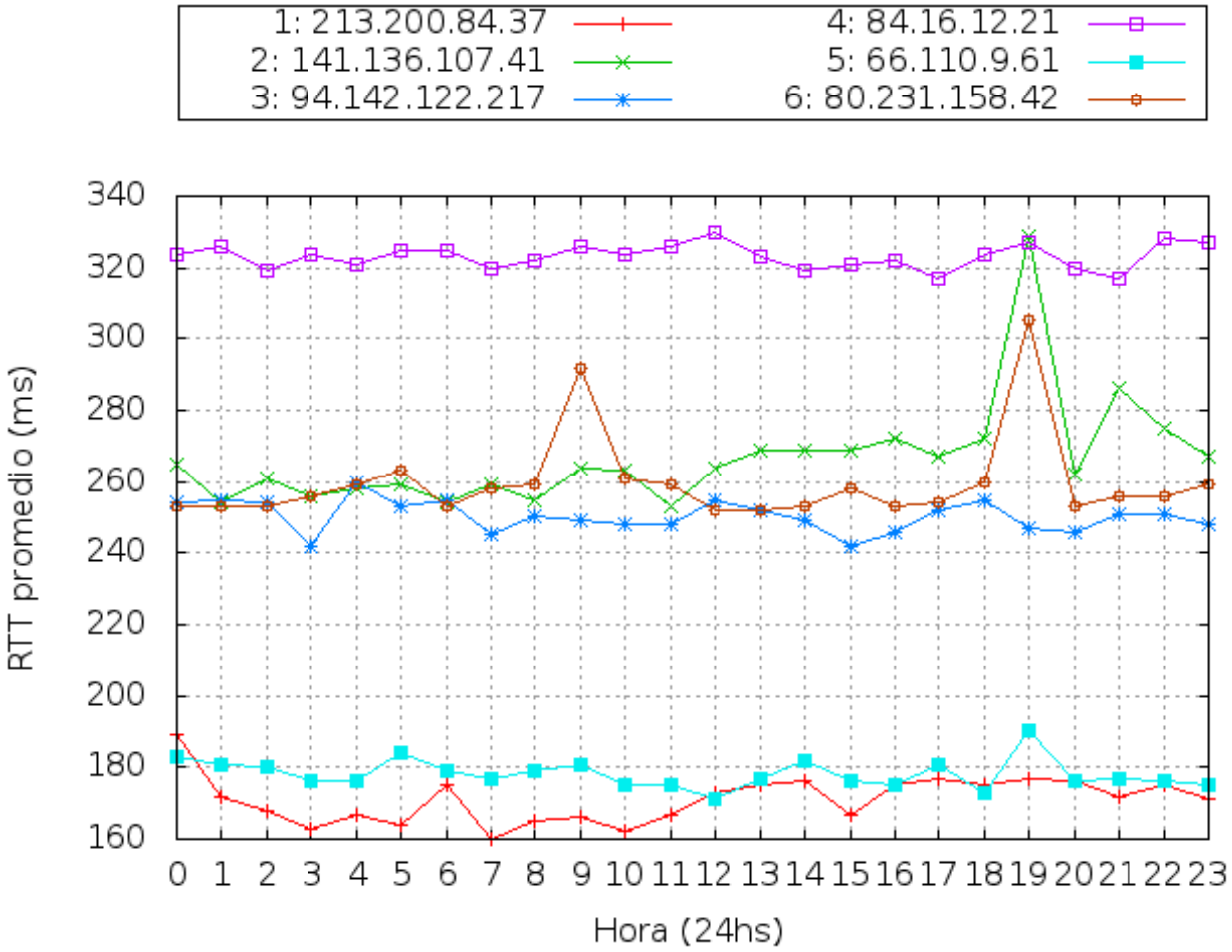

Figura 2: Tiempo de respuesta de los enlaces transatlánticos a lo largo del día

3.3. Enlace transpacífico

Figura 3: Enlace transpacífico

Pin	Dirección IP	Coordenadas	Distancia total recorrida hasta él en Km	RTT mínimo en ms
1	89.221.35.141	(37.9283,-122.0566)	11179.8250554	55.9
2	202.158.194.173	(-35.28,149.22)	24234.7289268	121.17

Enlace	Distancia en Km	RTT mínimo en ms
1 - 2	12222	61.11

3.4. Variación del RTT a lo largo del día

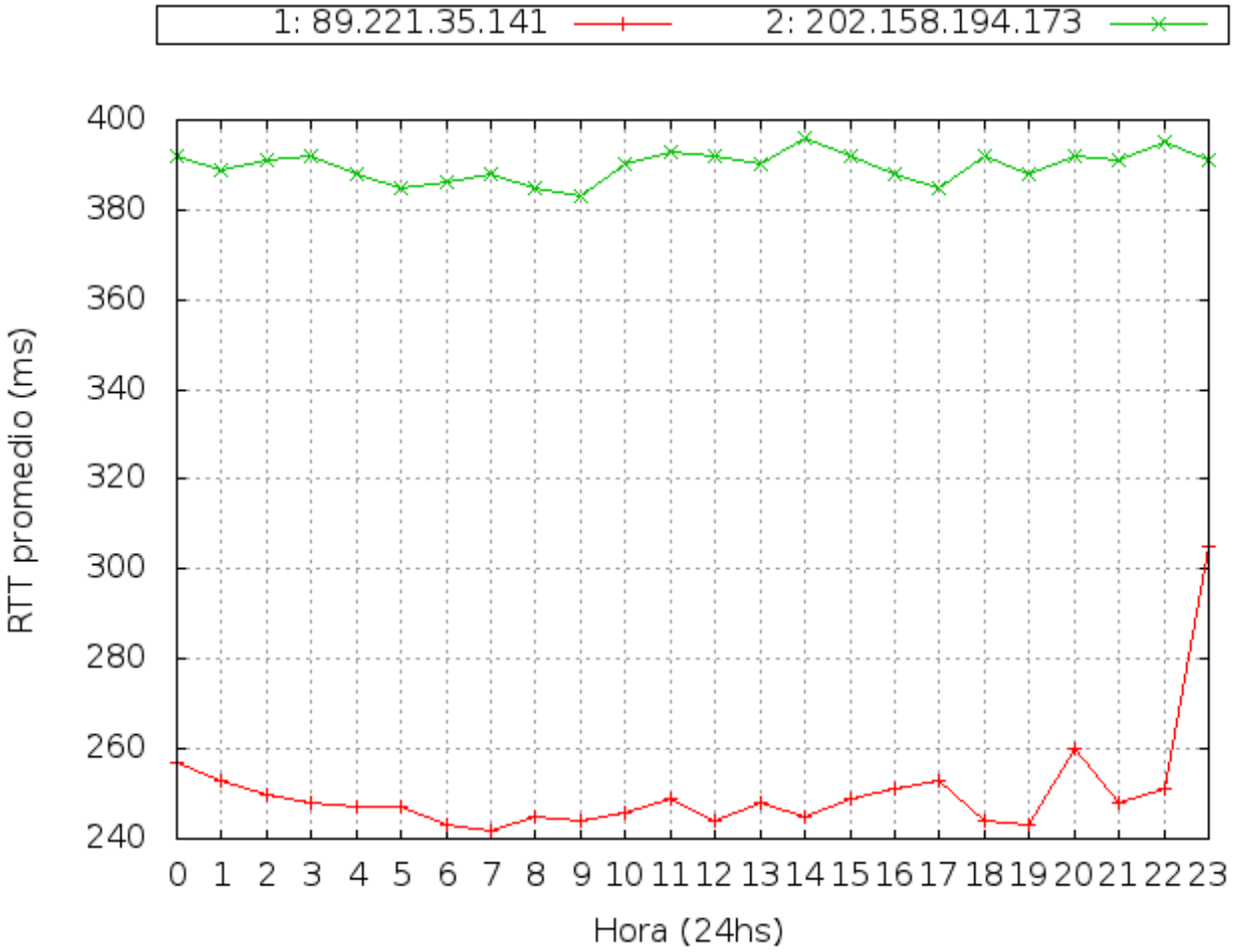

Figura 4: Tiempo de respuesta del enlace a Australia a lo largo del día

3.5. Casos curiosos

Figura 5: Traceroute a perfil.com.ar

En este caso al hacer un traceroute desde una dirección IP en Argentina a perfil.com.ar, un sitio web hosteado en Argentina, observamos que el tráfico primero se dirige a los Estados Unidos y luego vuelve al país para acceder al sitio.

Figura 6: Traceroute a newzealand.govt.nz

Realizamos un traceroute a una página web en Nueva Zelanda y obtuvimos que los paquetes se dirigieron primero a Estados Unidos, luego a Asia, de ahí vuelven a Norte América para dirigirse a España. Finalmente vuelven a Estados Unidos para ser enviados a Nueva Zelanda.

Al intentar reproducir los resultados días más tarde no obtuvimos los mismos resultados, en una ocasión iba directo desde Estados Unidos y en otras fue a través de Asia.

4. Análisis de resultados

Si bien en submarinecablemap.com se ve una gran cantidad de enlaces que cruzan el atlántico, notamos que sólo un par son los utilizados para llegar del otro lado del océano. Suponemos que ésto puede estar relacionado con los ISPs utilizados (telecentro, fibertel). Incluso en pruebas que trataron de forzar el uso de los enlaces que van a Africa desde Brasil, el resultado incluía un enlace USA - Londres. Esto también puede indicar que estos enlaces sean de mayor velocidad que los anteriores, por lo que son los elegidos para llegar a destino.

Como se puede ver en la figura 2 2, a lo largo del día en todos los enlaces el RTT hacia el extremo del enlace en los Estados Unidos es menor al del RTT hacia el extremo del enlace perteneciente a Europa, lo que se corresponde con que ambos pertenezcan al mismo enlace.

A su vez podemos observar que la diferencia entre los RTTs es considerablemente superior al RTT mínimo esperado, por lo que podemos suponer que gran parte de la diferencia entre los RTTs de los extremos del enlace y el RTT mínimo esperado, sea el tiempo de ser despachado de un extremo al otro, es decir:

$$RTT_{Europa} - RTT_{USA} - RTT_{USA/Europaminimo} = T_{QueueUsa}$$

5. Conclusiones

A pesar de haber intentando encontrar enlaces transatlánticos reales tales como son mostrados en **submarinecablemap.com** y **cablemap.info** nos resulto extremadamente dificil lograrlo. A continuación enumeramos posibles motivos por lo cual puede haber ocurrido esto y nuestras conclusiones:

1. Desde las conexiones a internet desde las que pudimos experimentar (con telecentro como ISP), para ir a cualquier host situado al otro lado del oceano Atlántico, nuestro tráfico debe ir primero a los Estados Unidos y desde allí o bien se dirige a Europa o se dirige hacia el Pacífico. Como los enlaces deben ser transatlánticos, debimos descartar los enlaces que atraviesan el oceano Pacífico.

2. Con los enlaces obtenidos entre Estados Unidos y Europa (la ultima y la primera ip antes y después de cruzar el oceano, respectivamente), utilizamos los servicios de geolocalización de direcciones IP ofrecidos gratuitamente en internet. Solo en dos ocasiones ambas posiciones coincidieron, aproximadamente, con las posiciones de un enlace real. En general o bien el extremo en Estados Unidos o el extremo en Europa o ambos no coincidían con el de un enlace real. Suponiendo que las direcciones ip obtenidas son efectivamente las de los enlaces, esto podría deberse a la precisión de los servicios de geolocalización.

3. Después de experimentar con direcciones al azar sin éxito, decidimos probar haciendo traceroute a páginas web hosteadas en ciudades cercanas a enlaces transatlánticos o en la misma ciudad que el enlace, de acuerdo a las direcciones y coordenadas obtenidas, observamos que el tráfico no necesariamente se dirige por alguno de los enlaces más cercanos al destino. Por ejemplo para llegar a un sitio web en Francia con un enlace cercano, la ruta puede cruzar desde Estados Unidos a un enlace en el sur de España o del Reino Unido.

4. Teniendo en cuenta la importancia de los enlaces, y posiblemente también la sensitividad de las direcciónes ip asignadas a los extremos de los mismos, es posible que se utilizen tuneles para evitar revelar esta información de los enlaces y que de esta forma la información obtenida no coincida con la real en su totalidad.