

Trabajo Práctico

Tecnología Digital IV

Profesor:

Marcelo Romeo

Ayudantes:

Emiliana Verdun y Facundo Berasategui

Hecho por:

Lucas Klaus Rehmann

Investigación ICMP

¿Cuál es la función del protocolo ICMP?

El protocolo ICMP es utilizado para la comunicación de información sobre la capa de red entre routers y hosts. Tiene varios usos, pero el más común es el reporte de errores.

Los mensajes ICMP son transportados dentro de datagramas IP, por lo que se podría decir que se encuentra en un nivel más arriba que IP. Sus mensajes contienen el header y los primeros 8 bytes del datagrama IP que causó que el mensaje sea generado. Tienen un campo de tipo y código.

¿Qué tipos de mensaje ICMP se utilizan en el comando ping y cómo funciona el proceso?

El tipo de mensaje ICMP utilizado en el comando ping es un mensaje tipo 8 con código 0. Funciona de forma que una vez que el host de destino recibe el mensaje, este mismo responde enviando un mensaje ICMP tipo 0 con código 0.

¿Qué es el programa Traceroute?

El programa Traceroute tiene como función trazar la ruta entre un host y otro host. Esto lo hace implementando mensajes ICMP. Envía varios datagramas IP que incluyen segmentos UDP con un número de puerto no compatible. Cada vez que el host origen envía un datagrama, comienza un timer.

El TTL de cada uno de estos datagramas va incrementando, es decir, el primero tiene un TTL de 1, el segundo de 2 y así. Cuando uno de estos datagramas llega a un router, este lo descarta ya que nota la terminación del TTL. Al mismo tiempo envía un mensaje ICMP de tipo 11 con código 0 de advertencia, el cual incluye la dirección IP del router y su nombre.

Una vez que este mensaje llega al host de origen, este calcula el RTT con el timer junto a la información recibida con este último mensaje. Como el TTL aumenta con cada datagrama enviado, uno de estos va a llegar al host destino, quien, debido al número de puerto indicado, enviará un mensaje ICMP de tipo 3 código 3 hacia el origen, indicando que el puerto no es alcanzable. Al recibir el mensaje, el host de origen para de enviar paquetes.

Implementación Ping

Para realizar la implementación del programa Ping, se hizo uso de la librería Scapy (<https://scapy.net/>) y de los módulos Time y Statistics.

Primero cree la función `ping`, que toma como parámetro una dirección web (www.nombre.com / www.nombre.edu / [etc.](#)). Lo primero que hace es armar un paquete ICMP con destinación a la dirección web proporcionada por el usuario. Luego de armar el paquete, se registra el tiempo en el que se armó en la variable `envio`, se envía el paquete con un timeout de 5, y la respuesta de este se guarda en la variable `ans`. El tiempo en el que se recibe esta respuesta es guardado en la variable `respuesta`.

Si la respuesta es válida, entonces se calcula el RTT haciendo la diferencia de tiempo entre que se envía y se recibe la respuesta, luego de lo cual se analiza el mensaje para ver el tipo y el código ICMP de este. En caso de que sea de tipo 0, entonces la función devuelve una lista con un bool indicando si recibió respuesta, el RTT calculado, el TTL de la respuesta, la longitud de esta, y el tipo y código (0 y 0).

En el caso de que sea de tipo 3, se devuelve una lista con 0 en los lugares de los valores mencionados, excepto en el de tipo, donde se pone un 3, y en el de código, donde se pone el código del mensaje recibido. En caso contrario se devuelve una lista con todos 0.

Además de esto, también está la función `enviar_varios_ping`, que toma como parámetros una dirección web, y la cantidad de pings a enviar. Lo que hace es que utiliza un for para enviar la cantidad de paquetes indicados, y según los valores de respuesta de cada paquete enviado, los imprime por la terminal. Además de esto, calcula varias estadísticas, como el RTT máximo recibido, el mínimo, el promedio de estos, y la desviación estándar. También indica el porcentaje de paquetes perdidos.

Experimentación

Ping a universidades

Las universidades elegidas (junto con sus distancias medidas desde mi casa) para realizar el experimento de pingear universidades en continentes distintos fueron:

- América del Sur -> UTDT (12 km): www.utdt.edu
- América del Norte -> MIT (8650 km): www.mit.edu
- Europa -> Cambridge (11190 km): www.cam.ac.uk
- Oceanía -> UTS (11800 km): www.uts.edu.au
- Asia -> IISC (14900 km): www.iisc.ac.in
- África -> UKZN (8100 km): ukzn.ac.za

Cabe remarcar que en el caso de las universidades de Asia y África fue necesario cierto tiempo de prueba y error para encontrar servidores de universidades que al hacer ping no se pierdan todos los paquetes.

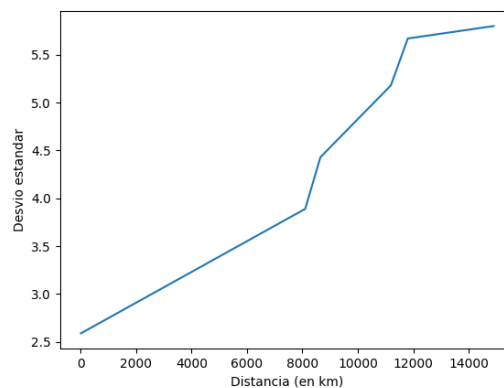
Para realizar el experimento, se mandaron 4 paquetes con un timeout de 5 segundos.

Las estadísticas obtenidas fueron las siguientes:

	Scapy	Ping
UTDT	Enviados: 4 Recibidos: 4 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 23.79971742630005 RTT Maximo: 26.60536766052246 RTT Minimo: 20.45583724975586 Desvio estandar del RTT promedio: 2.5982148236054368	Ping statistics for 104.18.11.140: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 17ms, Maximum = 18ms, Average = 17ms
UKZN	Enviados: 4 Recibidos: 4 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 20.462064743041992 RTT Maximo: 40.68398475646973 RTT Minimo: 12.890815734863281 Desvio estandar del RTT promedio: 3.8998855372278207	Ping statistics for 151.101.2.50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 15ms, Maximum = 19ms, Average = 16ms
MIT	Enviados: 4 Recibidos: 4 Perdidos: 0 Porcentaje perdidos: 0.0%	Ping statistics for 104.104.24.18: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

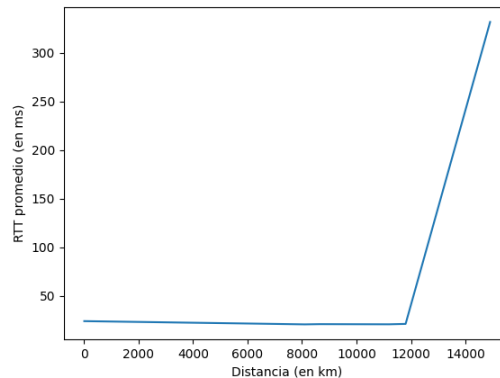
	Promedio RTT: 20.69956064224243 RTT Maximo: 25.53272247314453 RTT Minimo: 14.966964721679688 Desvio estandar del RTT promedio: 4.431591400546995	Minimum = 17ms, Maximum = 19ms, Average = 17ms
Cambridge	Enviados: 4 Recibidos: 4 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 20.533204078674316 RTT Maximo: 26.354551315307617 RTT Minimo: 13.770103454589844 Desvio estandar del RTT promedio: 5.188697580992793	Ping statistics for 23.185.0.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 16ms, Maximum = 20ms, Average = 18ms
UTS	Enviados: 4 Recibidos: 4 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 20.937085151672363 RTT Maximo: 27.14252471923828 RTT Minimo: 13.631105422973633 Desvio estandar del RTT promedio: 5.672471116343933	Ping statistics for 104.18.43.43: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 16ms, Maximum = 18ms, Average = 17ms
IISC	Enviados: 4 Recibidos: 4 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 332.35979080200195 RTT Maximo: 340.1210308074951 RTT Minimo: 326.0517120361328 Desvio estandar del RTT promedio: 5.805770086035277	Ping statistics for 13.71.49.222: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 330ms, Maximum = 344ms, Average = 335ms

Al analizar estos resultados, podemos sacar varias conclusiones. En caso de los RTTs se puede notar cómo a mayor distancia entre host origen y destino, el desvío estándar del RTT promedio tiende a subir. Una explicación a esto es que puede deberse a la cantidad de “hops” que tiene que hacer el paquete para llegar hasta el destino. Al depender de una mayor cantidad de routers, la eficiencia de estos puede variar drásticamente.



En caso de los RTT máximos y mínimos, uno esperaría que siempre a mayor distancia, aumenten estos. Sin embargo, se puede observar que esto no siempre es el caso. Por ejemplo, el RTT máximo registrado al pingear UTDT (con 12 km de distancia) fue ~26

milisegundos, pero al pingear MIT (con 8650 km de distancia), el RTT máximo registrado fue de ~25 milisegundos.



La explicación de esto puede atribuirse a varios factores. Uno de estos, siendo que, aunque la universidad puede estar a una gran distancia, es posible que tenga servidores en la región, los cuales hacen que el RTT no sea el mismo que el caso en el que un paquete vaya hasta la ubicación real. Tal caso no es lo que pasa con la universidad IISC, la cual estando a 14900 kilómetros registró un RTT máximo de ~340 milisegundos. Otra posible explicación es la dependencia en el horario del día en el que se realiza el ping, ya que en ciertos horarios puede que la congestión hacia ese host sea mucho mayor que en otros horarios.

Comparación Ping y Scapy

En prácticamente todos los casos, Ping tuvo tiempos de promedio RTT menores a la herramienta desarrollada con Scapy, excepto al hacer ping a IISC, donde la herramienta tuvo un RTT promedio de ~332 milisegundos, contra Ping que tuvo ~335 milisegundos.

Esto es de esperarse por varias razones. Una de estas es que Python introduce una latencia al ser interpretado, sumado al tiempo de procesamiento por usar librerías tales como Scapy. Además de esto, puede que el registro de tiempo (`time.time()`) tenga menos resolución que el tiempo registrado por Ping.

Varios tiempos del día

Luego de utilizar la herramienta desarrollada para hacer Ping a las universidades mencionadas anteriormente en 3 tiempos diferentes del día durante una semana, se pudieron notar algunas diferencias en los resultados obtenidos. Entrando más en detalle, la

mayor diferencia que se puede ver es en el RTT promedio, y el desvío estándar del RTT promedio.

Estas variaciones se ven repetidas en horarios específicos del día, lo que podría llevar a pensar que en estos momentos es en donde mayor tráfico de red direccionado hacia el host en cuestión hay. Esto puede suceder principalmente en horarios de clase o actividad académica.

Otra posibilidad es que el ping se ejecute en horarios pico del internet, donde los servicios de proveedores de internet (ISPs) están más congestionados en ciertas zonas, o que las rutas de red están más saturadas, haciendo que el sistema elija rutas más largas que introducen mayor retardo.

Cambio de timeout

Otro experimento para realizar es cómo afecta el cambio de timeout a la cantidad de paquetes perdidos.

Para probar esto voy a tomar tres timeouts:

- Normal: 5 segundos
- Corto: 5 microsegundos
- Muy corto: 0.000000000000000000005 microsegundos

Respuestas (ping hecho a www.utdt.edu en la noche):

Timeout normal	Timeout corto	Timeout muy corto
Enviados: 4 Recibidos: 4 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 23.884832859039307 RTT Maximo: 33.248186111450195 RTT Minimo: 15.602350234985352 Desvio estandar del RTT promedio: 7.3171788090623	Enviados: 4 Recibidos: 2 Perdidos: 2 Porcentaje perdidos: 50.0% Promedio RTT: 11.794447898864746 RTT Maximo: 16.779661178588867 RTT Minimo: 6.809234619140625 Desvio estandar del RTT promedio: 7.05015623150831	Enviados: 4 Recibidos: 1 Perdidos: 3 Porcentaje perdidos: 75.0% Promedio RTT: 19.713163375854492 RTT Maximo: 19.713163375854492 RTT Minimo: 19.713163375854492

Por las respuestas recibidas, se puede observar que cuanto menor es el timeout, más paquetes no logran llegar al destino. Esto es por la obvia razón de que al tener un timeout exageradamente chico, estos paquetes son descartados, a menos que lleguen muy rápidamente al destino.

Cantidad de paquetes

Por último, elegí una variedad de números de paquetes a enviar para ver si más paquetes influyen tanto en el desvío (ya que, al haber mayor cantidad de paquetes, pueden haber más valores de RTT), como en la cantidad de paquetes perdidos. Las cantidades elegidas fueron:

- Chica: 20
- Normal: 60
- Grande: 200

Respuestas (ping hecho a www.utdt.edu en la noche con timeout de 5):

Cantidad normal	Cantidad chica	Cantidad grande
Enviados: 20 Recibidos: 20 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 21.908986568450928 RTT Maximo: 55.82785606384277 RTT Minimo: 16.622304916381836 Desvio estandar del RTT promedio: 8.15836987128542	Enviados: 60 Recibidos: 60 Perdidos: 0 Porcentaje perdidos: 0.0% Promedio RTT: 22.752686341603596 RTT Maximo: 110.42022705078125 RTT Minimo: 13.221979141235352 Desvio estandar del RTT promedio: 13.354774796904032	Enviados: 200 Recibidos: 199 Perdidos: 1 Porcentaje perdidos: 0.5% Promedio RTT: 21.020889282226562 RTT Maximo: 55.068016052246094 RTT Minimo: 12.743711471557617 Desvio estandar del RTT promedio: 4.446525056591957

Con las estadísticas de las respuestas recibidas se puede ver que la cantidad de paquetes no influye tanto en la desviación estándar del RTT promedio. Sin embargo, en el caso de paquetes perdidos, si se puede observar que, en el caso de mandar una gran cantidad de paquetes, es posible ver perdida, lo cual puede ser causado por la congestión temporal de enviar tantos paquetes en poco tiempo.