

Trabajo Práctico

Primer semestre 2025

Introducción

En este trabajo práctico se explorará el protocolo ICMP, su funcionamiento y cómo se puede utilizar para implementar otras herramientas. El objetivo es implementar la herramienta **Ping** en Python usando la librería **Scapy**¹ y experimentar con la misma, comparándola con la implementación ya existente.

Contexto

Ping es una herramienta de red que permite verificar si un host específico es accesible a través de una red IP y medir la latencia entre dos nodos en una red. Funciona enviando un paquete de datos a un destino y esperando una respuesta, midiendo el tiempo de viaje.

Ping es implementada enviando una cantidad arbitraria de **paquetes ICMP** (echo request) al host de destino y esperando otros paquetes ICMP como respuesta (echo reply). Al recibir respuesta Ping mide el tiempo de ida y vuelta (RTT), registra la pérdida de paquetes y muestra un resumen estadístico de los paquetes de eco recibidos (el mínimo, el máximo y el promedio del RTT y, en algunas versiones, la desviación estándar del promedio). Esta información es extraída de la respuesta. Para implementar **Ping** entonces, basta con enviar paquetes ICMP, registrar respuestas y no respuestas y procesar los paquetes recibidos.

Si el host al que hicimos ping está accesible, está conectado a la red y responde paquetes ICMP, entonces decimos que el ping fue exitoso y obtenemos información sobre el RTT. En caso de que el host no esté accesible no recibiremos respuesta.

Para comenzar con nuestra implementación de **Ping**, podemos tomar como base el siguiente fragmento de código:

```
from scapy.all import *
def ping(host):
    print(f"Ping {host}")
    #COMPLETAR
    return

ping("google.com")
```

¹<https://scapy.readthedocs.io/en/latest/> - Documentación oficial de Scapy
<https://0xbharath.github.io/art-of-packet-crafting-with-scapy/index.html>

Ejercicios:

1. Investigar sobre el protocolo ICMP y responder las siguientes preguntas:
 - a. ¿Cuál es la función del protocolo ICMP?
 - b. Investigar sobre los tipos de mensaje ICMP que existen y sus códigos. ¿Qué tipos de mensaje ICMP se utilizan en el comando ping y cómo funciona el proceso?
 - c. ¿Qué es el programa Traceroute? Describa cómo se puede implementar Traceroute usando mensajes ICMP. (Traceroute utiliza mensajes ICMP del tipo Time Exceeded)
2. Implementar Ping. El programa debe estar implementado en Python 3, utilizando Scapy.
 - a. Para cada respuesta deberán mostrar por terminal longitud del paquete, rtt y ttl (time-to-live) de la misma.
 - b. Al enviar varios paquetes deberán calcular las siguientes estadísticas, las mismas deberán mostrarse al finalizar en envió de los paquetes:
 - i. Cantidad de paquetes enviados
 - ii. Cantidad de paquetes recibidos
 - iii. Cantidad de paquetes perdidos
 - iv. Porcentaje de paquetes perdidos
 - v. RTT promedio
 - vi. RTT máximo
 - vii. RTT mínimo
 - viii. Desvío estándar del RTT promedio (pueden utilizar la función de Python `statistics.stdev()`)
 - c. Recomendamos, pero no es necesario, que armen primero una función que envíe un solo paquete ICMP, guarde y devuelva la respuesta recibida, si la hubo. Y luego reutilizar esa función para enviar varios paquetes y calcular las estadísticas.
3. Modificar la implementación anterior para interpretar los códigos de error de las respuestas ICMP de tipo 3, Destination Unreachable, y mostrar el error correspondiente. Algunos ejemplos de códigos de error de respuestas ICMP son: 0: Destination Network Unreachable, 1: Destination Host Unreachable.

Experimentación e Informe

El último punto del TP consiste en realizar un informe sobre el trabajo realizado. Las preguntas y experimentos detallados a continuación consisten en lo mínimo indispensable a

incluir en el informe. Tienen libertad de agregar cuantos experimentos quieran. El informe debe tener un máximo de 10 páginas (sin contar carátula).

Ejercicios:

4. Ejecutar **Ping** chequeando la conectividad de 5 universidades de diferentes continentes. Responder las siguientes preguntas.
 - a. Analizar la diferencia entre los RTT de los ping a cada universidad. ¿Hay una gran diferencia? ¿A qué creen que se puede deber?
 - b. Analizar las diferencias en los resultados de hacer un ping hacia un mismo host con la herramienta desarrollada por ustedes y el comando ping ya existente en sus computadoras.
 - c. Analizar los resultados obtenidos y armar al menos 2 gráficos (pueden estar incluidos en los incisos anteriores).
5. Realizar mediciones en diferentes momentos del día (mañana, tarde, noche) hacia la misma universidad durante una semana. ¿Hay diferencias en el RTT para diferentes momentos del día? Si las hay, ¿A qué puede deberse?

Modalidad de entrega

El trabajo debe realizarse en grupos de 3 alumnos.

Deberán entregar un solo archivo en formato .zip, el cual deberá contener los siguientes archivos:

- Informe en formato PDF
- Archivo de Python/Jupyter Notebook con la implementación

El TP debe ser entregado a través del campus. La fecha límite de entrega es el **22/06** hasta las 23:59 hs. No se aceptarán TPs entregados después de este horario.