# Taller de Traceroute

Teoría de las Comunicaciones

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

10.04.2021

# Bibliografía

The TCP/IP Guide Version 3.0 Charles M. Kozierok. Pags 602 - 649

# Agenda

# Motivación

## 1. Introducción

En este trabajo práctico nos proponemos experimentar con herramientas y técnicas de uso frecuente a nivel de red. Particularmente, la versión de `traceroute` basada en los mensajes *echo request/reply* del protocolo ICMP [2, 1].

# Motivación

## 1. Introducción

En este trabajo práctico nos proponemos experimentar con herramientas y técnicas de uso frecuente a nivel de red. Particularmente, la versión de `traceroute` basada en los mensajes *echo request/reply* del protocolo ICMP [2, 1].

# Agenda

- Conceptos
  - ICMP
  - Traceroute
- Taller
  - Scapy 2.0
  - Ejercicios
- Presentación de TP2

# Dónde estamos parados?

# Dónde estamos parados?

- Internet Protocol (IP)
  - Qué características tiene?

# Dónde estamos parados?

- Internet Protocol (IP)
  - Qué características tiene?
- Pista: Best Effort..

# Dónde estamos parados?

- Internet Protocol (IP)
  - Qué características tiene?
- Pista: Best Effort..
  - Sin conexión.

# Dónde estamos parados?

- Internet Protocol (IP)
  - Qué características tiene?
- Pista: Best Effort..
  - Sin conexión.
  - Sin confianza.

# Dónde estamos parados?

- Internet Protocol (IP)
  - Qué características tiene?
- Pista: Best Effort..
  - Sin conexión.
  - Sin confianza.
  - Sin reconocimiento.

# Dónde estamos parados?

- Internet Protocol (IP)
  - Qué características tiene?
- Pista: Best Effort..
  - Sin conexión.
  - Sin confianza.
  - Sin reconocimiento.
- Sin embargo, ante cualquier error no tenemos forma de hacer nada.

# El protocolo ICMP

- *Internet Control Message Protocol*.

# El protocolo ICMP

- *Internet Control Message Protocol*.
- Protocolo de control que forma parte integral de la capa de red.
  - *Dato de color: Es tan necesario que cuando se desarrolló IPV6, se desarrolló ICMPv6*

# El protocolo ICMP

- *Internet Control Message Protocol*.
- Protocolo de control que forma parte integral de la capa de red.
  - *Dato de color: Es tan necesario que cuando se desarrolló IPV6, se desarrolló ICMPv6*
- IP se encarga del *direccionamiento*, *encapsular los datos* y *ruteo*

# El protocolo ICMP

- *Internet Control Message Protocol*.
- Protocolo de control que forma parte integral de la capa de red.
  - *Dato de color: Es tan necesario que cuando se desarrolló IPV6, se desarrolló ICMPv6*
- IP se encarga del *direccionamiento*, *encapsular los datos* y *ruteo*
- ICMP asiste a IP.
  - Reportes de error

# El protocolo ICMP

- *Internet Control Message Protocol*.
- Protocolo de control que forma parte integral de la capa de red.
  - *Dato de color: Es tan necesario que cuando se desarrolló IPV6, se desarrolló ICMPv6*
- IP se encarga del *direccionamiento*, *encapsular los datos* y *ruteo*
- ICMP asiste a IP.
  - Reportes de error
  - Feedback

# El protocolo ICMP

- *Internet Control Message Protocol*.
- Protocolo de control que forma parte integral de la capa de red.
  - *Dato de color: Es tan necesario que cuando se desarrolló IPV6, se desarrolló ICMPv6*
- IP se encarga del *direccionamiento*, *encapsular los datos* y *ruteo*
- ICMP asiste a IP.
  - Reportes de error
  - Feedback
  - Testing

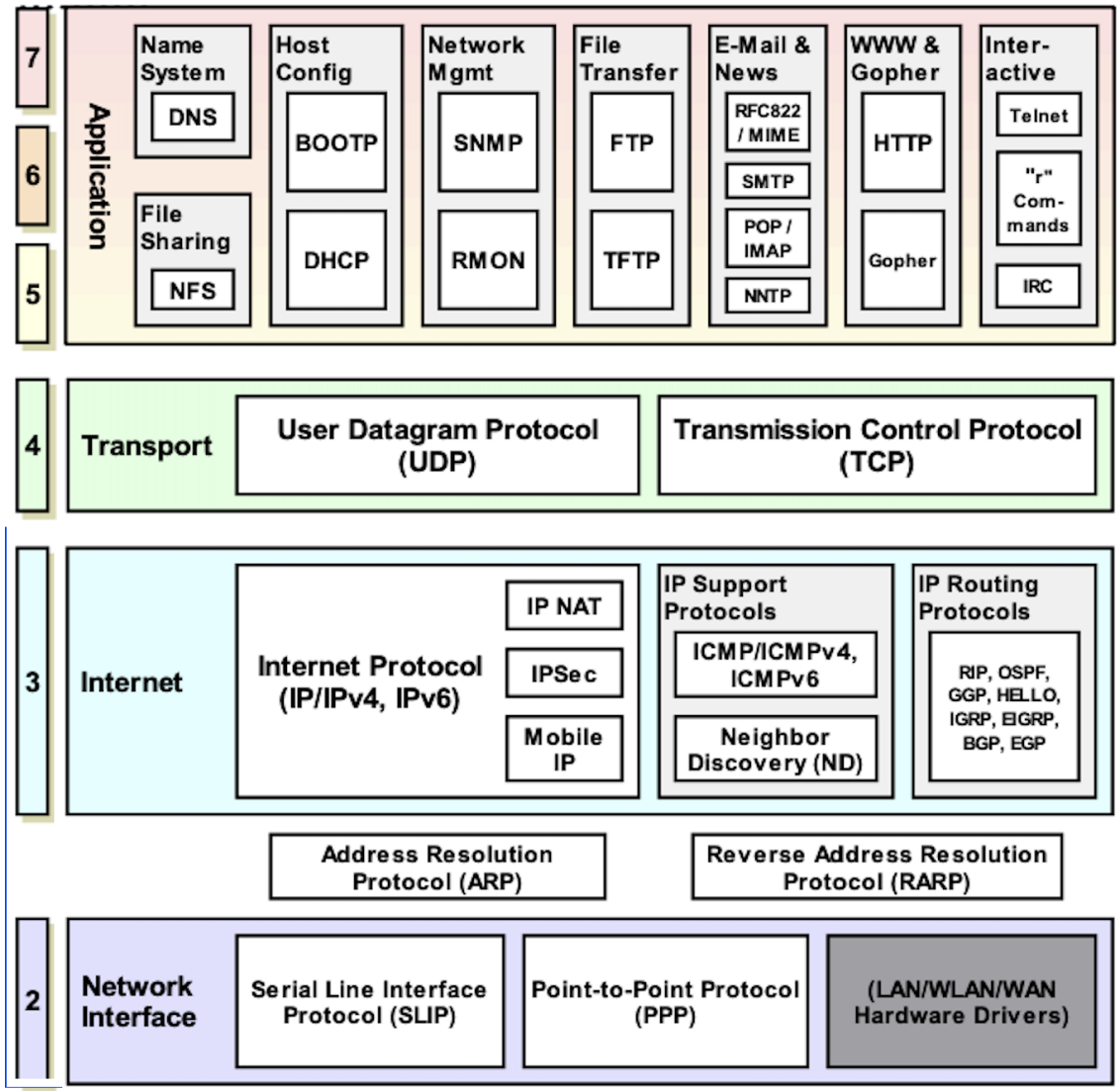
# El protocolo ICMP

- *Internet Control Message Protocol*.
- Protocolo de control que forma parte integral de la capa de red.
  - *Dato de color: Es tan necesario que cuando se desarrolló IPV6, se desarrolló ICMPv6*
- IP se encarga del *direccionamiento*, *encapsular los datos* y *ruteo*
- ICMP asiste a IP.
  - Reportes de error
  - Feedback
  - Testing
  - **No intercambia datos**

# El protocolo ICMP

- *Internet Control Message Protocol*.
- Protocolo de control que forma parte integral de la capa de red.
  - *Dato de color: Es tan necesario que cuando se desarrolló IPV6, se desarrolló ICMPv6*
- IP se encarga del *direccionamiento*, *encapsular los datos* y *ruteo*
- ICMP asiste a IP.
  - Reportes de error
  - Feedback
  - Testing
  - **No intercambia datos**
- Especificado en el RFC 792 (IP: RFC791)

# El protocolo ICMP



# ICMP: Cómo y dónde se usa

- Es un protocolo simple. Únicamente **intercambia** información.

# ICMP: Cómo y dónde se usa

- Es un protocolo simple. Únicamente **intercambia** información.
- Pueden ser enviados tanto por routers como por hosts arbitrarios.

# ICMP: Cómo y dónde se usa

- Es un protocolo simple. Únicamente **intercambia** información.
- Pueden ser enviados tanto por routers como por hosts arbitrarios.
- ICMP no define el uso que se le da a sus mensajes.

# ICMP: Cómo y dónde se usa

- Es un protocolo simple. Únicamente **intercambia** información.
- Pueden ser enviados tanto por routers como por hosts arbitrarios.
- ICMP no define el uso que se le da a sus mensajes.
- Son generados a causa de:
  - Errores en los datagramas IP.
  - Necesidad de comunicar información de diagnóstico.
  - Necesidad de comunicar información de ruteo.

# ICMP: Cómo y dónde se usa

- Es un protocolo simple. Únicamente **intercambia** información.
- Pueden ser enviados tanto por routers como por hosts arbitrarios.
- ICMP no define el uso que se le da a sus mensajes.
- Son generados a causa de:
  - Errores en los datagramas IP.
  - Necesidad de comunicar información de diagnóstico.
  - Necesidad de comunicar información de ruteo.

# ICMP: Limitaciones

- Por cómo está implementado IP, el datagrama IP **sólo** contiene *fuente* y *destino*.

¿Qué problema trae esto?

# ICMP: Mensajes

- Se dividen en dos clases:

# ICMP: Mensajes

- Se dividen en dos clases:
- Mensajes de error
  - Proveen feedback sobre un error.

# ICMP: Mensajes

- Se dividen en dos clases:
- Mensajes de error
  - Proveen feedback sobre un error.
  - Usualmente son en respuesta a alguna acción.

# ICMP: Mensajes

- Se dividen en dos clases:
- Mensajes de error
  - Proveen feedback sobre un error.
  - Usualmente son en respuesta a alguna acción.
  - Los errores pueden ser:
    - ★ Estructura o contenido del datagrama.
    - ★ Problemas de la red mientras se “routea” el datagrama.
- Información

# ICMP: Mensajes

- Se dividen en dos clases:
- Mensajes de error
  - Proveen feedback sobre un error.
  - Usualmente son en respuesta a alguna acción.
  - Los errores pueden ser:
    - ★ Estructura o contenido del datagrama.
    - ★ Problemas de la red mientras se “routea” el datagrama.
- Información
  - Permite que dispositivos intercambien información

# ICMP: Mensajes

- Se dividen en dos clases:
- Mensajes de error
  - Proveen feedback sobre un error.
  - Usualmente son en respuesta a alguna acción.
  - Los errores pueden ser:
    - ★ Estructura o contenido del datagrama.
    - ★ Problemas de la red mientras se “routea” el datagrama.
- Información
  - Permite que dispositivos intercambien información
  - Testing

# ICMP: Mensajes

- Se dividen en dos clases:
- Mensajes de error
  - Proveen feedback sobre un error.
  - Usualmente son en respuesta a alguna acción.
  - Los errores pueden ser:
    - ★ Estructura o contenido del datagrama.
    - ★ Problemas de la red mientras se "routea" el datagrama.
- Información
  - Permite que dispositivos intercambien información
  - Testing
  - No suelen dispararse en respuesta a un envío normal de paquete IP.
  - Tienen un formato *request*/*reply*

# ICMP: Formato de los paquetes

- Se dividen en dos clases:
  - Mensajes de error: Mensajes de feedback al emisor del datagrama, sea por un error en el formato del datagrama o de ruteo, entre otros.
  - Información: Permite a los dispositivos intercambiar información entre sí.
- Los paquetes constan de un header de 4 bytes y una sección de datos variable.
- **Header**:
  - `Type` (1 byte): indica el tipo del mensaje y define el formato de lo que sigue. (256 posibles).
  - `Code` (1 byte): especifica el subtipo de cada tipo (256 posibles).
  - `Checksum` (2 bytes): usa el msimo algoritmo de IP.
  - `Message body/data` Campos específicos según el tipo.

# ICMP: Formato de los paquetes

- Se dividen en dos clases:
  - Mensajes de error: Mensajes de feedback al emisor del datagrama, sea por un error en el formato del datagrama o de ruteo, entre otros.
  - Información: Permite a los dispositivos intercambiar información entre sí.
- Los paquetes constan de un header de 4 bytes y una sección de datos variable.
- **Header**:
  - `Type` (1 byte): indica el tipo del mensaje y define el formato de lo que sigue. (256 posibles).
  - `Code` (1 byte): especifica el subtipo de cada tipo (256 posibles).
  - `Checksum` (2 bytes): usa el msimo algoritmo de IP.
  - `Message body/data` Campos específicos según el tipo.

Por ejemplo, el *type* puede ser Destination Unreachable (3), y el *code* Network Unreachable o Host Unreachable (0 y 1 respectivamente). Luego en Message iría el datagrama IP que generó el error.

| Type | Name |
|---|---|
| 0 | Echo Reply |
| 1 | Unassigned |
| 2 | Unassigned |
| 3 | Destination Unreachable |
| 4 | Source Quench |
| 5 | Redirect |
| 6 | Alternate Host Address |
| 7 | Unassigned |
| 8 | Echo |
| 9 | Router Advertisement |
| 10 | Router Selection |
| 11 | Time Exceeded |
| 12 | Parameter Problem |
| 13 | Timestamp |
| 14 | Timestamp Reply |
| 15 | Information Request |
| 16 | Information Reply |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |
| 19 | Reserved (for Security) |
| 20-29 | Reserved (for Robustness Experiment) |

# ICMP: Formato de los paquetes

Algunos códigos o subtipos de **Destination Unreachable**

- 0 Network Unreachable
- 1 Host Unreachable
- 2 Protocol unreachable
- 3 Port unreachable
- ..
- 15 Precedence Cutoff in Effect (?

# ICMP: Resúmen

- Es un paquete de control (testing, feedback, reportes de error).
- Es simple. No hay algoritmos, cómo se utiliza ICMP va por fuera del protocolo.
- Asiste a y se encapsula en IP.
- Sus mensajes se dividen en información y error.

# Taller

- Vamos a hacer el taller con modalidad parecida al taller 1.
- Recomendable hacer los ejercicios para poder entender y modificar el código del TP2.

# ¿Qué es `traceroute`?

- Es una herramienta de diagnóstico para averiguar las rutas que atraviesan los paquetes en Internet.
- La mayoría de los sistemas operativos actuales proveen alguna implementación. Ejemplos:
  - `tracert` en Windows.
  - `traceroute` en Unix.
- Al correr la herramienta, se debe indicar hacia qué host destino se desea trazar la ruta.
- La salida obtenida suele mostrar las direcciones IP de los hops sucesivos y el respectivo tiempo de respuesta esperado.

# Los distintos sabores

- Existen varias maneras de implementar `traceroute`.
- Usualmente consisten en enviar paquetes IP donde se incremente progresivamente el campo `TTL`.
- El efecto colateral de esto es recibir respuestas ICMP sucesivas informando que el tiempo de vida del paquete acaba de expirar.
- En lo que sigue describiremos dos implementaciones de `traceroute`:
  - Enviando paquetes ICMP de tipo *Echo Request* ajustando el `TTL`. (Listo)
  - Utilizando las opciones de los datagramas IP (RFC 1393).

# `traceroute` sobre ICMP

- Implementa (esencialmente) el siguiente algoritmo:
  1. Sea $h$ la IP del host destino y sea `ttl` $= 1$.
  2. Repetir los siguientes pasos hasta obtener una respuesta ICMP de tipo *Echo Reply* por parte de $h$:
  3. Enviar un paquete ICMP de tipo *Echo Request* al host $h$ cuyo campo `TTL` en el header IP valga `ttl`.
  4. Si se recibe una respuesta ICMP de tipo *Time Exceeded*, anotar la IP origen de dicho paquete. En otro caso, marcar como desconocido (*) el hop.
  5. Incrementar `ttl`.

# `traceroute` sobre ICMP: observaciones

- Usualmente suele enviarse una serie de paquetes por cada valor de `ttl` (por lo general tres).
- A través de esto, puede estimarse el tiempo medio de respuesta.
- El host origen define un timeout para esperar por cada respuesta. Pasado este intervalo, el hop actual se asume desconocido.
- Observar que las rutas no necesariamente serán siempre iguales!

# `traceroute` sobre ICMP: observaciones

- Veamos que sucede cuándo corremos traceroute en la consola.

# `traceroute` utilizando opciones IP

- Problemas del enfoque anterior:
  - Se generan muchos paquetes: $\geq 2n$, siendo $n$ la cantidad de hops.
  - La ruta puede cambiar en el transcurso del algoritmo.
- El RFC 1393 especifica un algoritmo nuevo de `traceroute` que utiliza las opciones IP.
- Es más eficiente: genera $n + 1$ paquetes y no sufre del cambio de rutas dado que el origen envía un único paquete.

# El algoritmo básico

- La idea: enviar un paquete arbitrario con la opción IP de `traceroute` adjuntada.
- Cada hop intermedio notará su presencia y devolverá un paquete ICMP de tipo 30 (*Traceroute*) con información apropiada.
- Desventaja: los routers deben implementar esta nueva funcionalidad.

# Formato de la opción IP

- La opción de `traceroute` definida en el RFC esencialmente contiene estos campos:
  - `ID Number`: valor arbitrario para identificar las respuestas ICMP.
  - `Hop Count`: número de routers a través de los cuales pasó hasta el momento el paquete original.
  - `Originator IP Address`: dirección IP del host que origina el `traceroute`. Los routers utilizan este campo para devolver las respuestas ICMP.

# La implementación nativa de Scapy

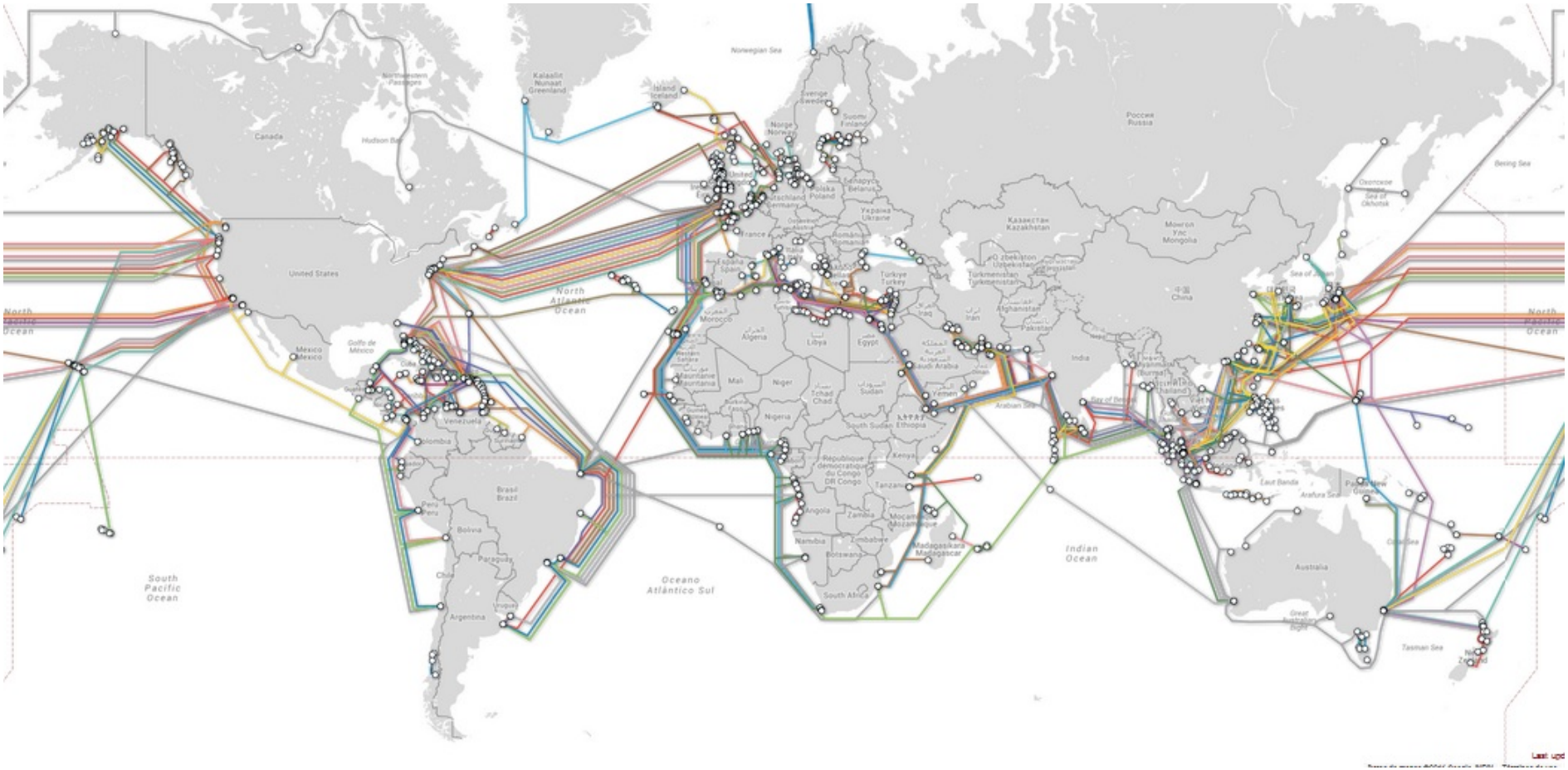
- Scapy provee una implementación propia de `traceroute`.
- Utiliza conceptos de nivel de transporte (puntualmente TCP).

```
>>> traceroute('www.dc.uba.ar')
**********************Finished to send 30 packets.
   157.92.27.21:tcp80
1  192.168.0.3     11          10 190.220.179.1   11
2  190.246.18.1    11          11 190.220.176.34  11
6  200.89.165.117  11          12 190.220.179.122 11
7  200.89.165.1    11          14 157.92.47.13    11
8  200.89.165.250  11          15 157.92.18.21    11
9  200.49.69.165   11          16 157.92.27.21    SA
```

- 11 indica el tipo ICMP: *Time to Live Exceeded*.
- SA indica la contestación positiva del destino (SYN-ACK).

# Trabajo práctico: Rutas en Internet

# Trabajo práctico: Rutas en Internet



# Objetivos

- Experimentar con herramientas y técnicas frecuentes a nivel de red: `traceroute`.
- Entender los protocolos involucrados.
- Desarrollar implementaciones propias para afianzar los conocimientos.
- Continuar con el enfoque analítico de la instancia anterior.

# Fecha límite de entrega

- Hasta el 24 de Mayo del 2022

# Herramientas adicionales

- Recomendamos el uso de herramientas de geolocalización (ver referencias en el enunciado).
- Nos permiten ubicar en el mapa la localización aproximada de una dirección IP.
- En nuestro caso serán las direcciones de los hops encontrados en las rutas.

Todo por hoy

- Vamos a ver el TP
- Preguntas.