

TESIS DE GRADO DE INGENIERÍA ELECTRÓNICA

TOMOGRAFÍA DE INTERNET:
ADQUISICIÓN Y ESTUDIO
DE PARÁMETROS DINÁMICOS DE LA RED

Autor: Mauricio Anderson Ricci

Director: Dr. Ing. J.I. Alvarez-Hamelin

FIUBA

Octubre 2016

TABLA DE CONTENIDOS

- 1 INTRODUCCIÓN Y ESTADO DEL ARTE
- 2 MAGALLANES
- 3 DESPLIEGUE DE EXPERIMENTOS
- 4 CONCLUSIONES

TABLA DE CONTENIDOS

1 INTRODUCCIÓN Y ESTADO DEL ARTE

2 MAGALLANES

3 DESPLIEGUE DE EXPERIMENTOS

4 CONCLUSIONES

INTRODUCCIÓN

Adquisición y análisis de datos de la topología de Internet

"Tomografía de Red"

- *Internet Tomography* (K. Claffy, T. Monk y D. McRobb)
- Mediciones externas → Estado interno

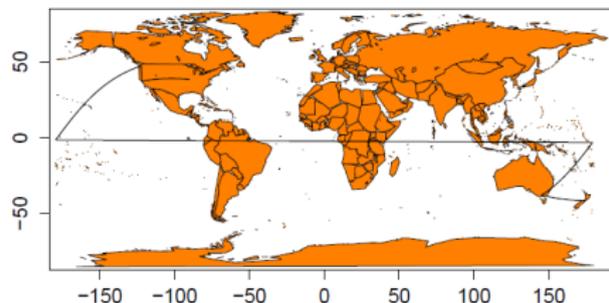
INTRODUCCIÓN

Adquisición y análisis de datos de la topología de Internet

"Tomografía de Red"

- *Internet Tomography* (K. Claffy, T. Monk y D. McRobb)
- Mediciones externas → Estado interno

Ejemplo:



tracert from 130.195.4.68 to 8.8.8.8

```
1 130.195.4.65 0.731 ms
2 *
3 *
4 210.7.39.101 1.052 ms
5 210.7.39.249 9.057 ms
6 210.7.39.248 9.203 ms
7 182.255.119.202 9.940 ms
8 113.197.15.66 32.908 ms
.
.
.
```

ESTADO DEL ARTE

TOMOGRAFÍA DE LA RED

- Determinar como se interconectan las redes

ESTADO DEL ARTE

TOMOGRAFÍA DE LA RED

- Determinar como se interconectan las redes
- Determinar cuanto demora y por cuantos saltos pasa un paquete entre origen y destino

ESTADO DEL ARTE

TOMOGRAFÍA DE LA RED

- Determinar como se interconectan las redes
- Determinar cuanto demora y por cuantos saltos pasa un paquete entre origen y destino
- Analizar la frecuencia y el patrón que siguen el cambio de las rutas

ESTADO DEL ARTE

TOMOGRAFÍA DE LA RED

- Determinar como se interconectan las redes
- Determinar cuanto demora y por cuantos saltos pasa un paquete entre origen y destino
- Analizar la frecuencia y el patrón que siguen el cambio de las rutas
- Visualizar mediante un grafo las formas que toma Internet

ESTADO DEL ARTE

ETAPAS

- **Exploración** → Datos de rutas
 - ping, traceroute

ESTADO DEL ARTE

ETAPAS

- **Exploración** → Datos de rutas
 - ping, traceroute
- **Resolución de alias** → Asignación de @IP a *routers*
 - Técnicas Pasivas: DisCarte, Kapar
 - Técnicas Activas: Mercator, Ally, MIDAR

ESTADO DEL ARTE

ANTECEDENTE Y PROYECTOS DE INVESTIGACIÓN ACTUALES

- 1 Route Views (www.routeviews.org), tablas BGP

ESTADO DEL ARTE

ANTECEDENTE Y PROYECTOS DE INVESTIGACIÓN ACTUALES

- 1 Route Views (www.routeviews.org), tablas BGP
- 2 CAIDA (www.caida.org), traceroutes
 - 1 Skitter → 30 puntos de medición
 - 2 Ark → 168 puntos de medición, Scamper, MIDAR
 - 3 Investigaciones en diversas áreas

ESTADO DEL ARTE

ANTECEDENTE Y PROYECTOS DE INVESTIGACIÓN ACTUALES

- ① Route Views (www.routeviews.org), tablas BGP
- ② CAIDA (www.caida.org), traceroutes
 - ① Skitter → 30 puntos de medición
 - ② Ark → 168 puntos de medición, Scamper, MIDAR
 - ③ Investigaciones en diversas áreas
- ④ DIMES (www.netdimes.org), traceroutes

ESTADO DEL ARTE

ANTECEDENTE Y PROYECTOS DE INVESTIGACIÓN ACTUALES

- ① Route Views (www.routeviews.org), tablas BGP
- ② CAIDA (www.caida.org), traceroutes
 - ① Skitter → 30 puntos de medición
 - ② Ark → 168 puntos de medición, Scamper, MIDAR
 - ③ Investigaciones en diversas áreas
- ④ DIMES (www.netdimes.org), traceroutes
- ⑤ iPlane (web.eecs.umich.edu/~harshavm/iplane), traceroutes

TABLA DE CONTENIDOS

- 1 INTRODUCCIÓN Y ESTADO DEL ARTE
- 2 MAGALLANES
- 3 DESPLIEGUE DE EXPERIMENTOS
- 4 CONCLUSIONES

MAGALLANES

MOTIVACIÓN Y FILOSOFÍA

Motivación

- Múltiples herramientas para cada tarea
- Plataformas de medición adaptadas a cada proyecto
- Nuestra propia plataforma → MAGALLANES

Motivación

- Múltiples herramientas para cada tarea
- Plataformas de medición adaptadas a cada proyecto
- Nuestra propia plataforma → MAGALLANES

Filosofía

- **Todo en uno** → Integración de herramientas
- **Modular** → Independencia de tareas
- **Configurable** → Selección de parámetros

MAGALLANES

ENTORNO DE TRABAJO

open source

MAGALLANES

ENTORNO DE TRABAJO

open source

- Sistema Operativo: Linux
- Programación: Python
- Base de Datos: Postgres
- Control de Versiones: GitHub

MAGALLANES

ENTORNO DE TRABAJO

open source

- Sistema Operativo: Linux
- Programación: Python
- Base de Datos: Postgres
- Control de Versiones: GitHub
- Servidores: **PlanetLab**
- Traceroutes: **Scamper**
- Resolución de alias: **MIDAR**

Plataforma de investigación a escala planetaria

30 países → 717 sitios → 1.353 nodos (servidores)



<https://www.planet-lab.org/generated/World50.png>

MAGALLANES

ENTORNO DE TRABAJO: PLANETLAB

Plataforma de investigación a escala planetaria

30 países → 717 sitios → 1.353 nodos (servidores)



<https://www.planet-lab.org/generated/World50.png>

PLANETLAB

Slices → Asignación de nodos → Espacios virtuales

- CAIDA → Ark

- CAIDA → Ark

- Integra múltiples herramientas
 - traceroute
 - ping
 - tracelb
 - neighbor discovery
 - etc

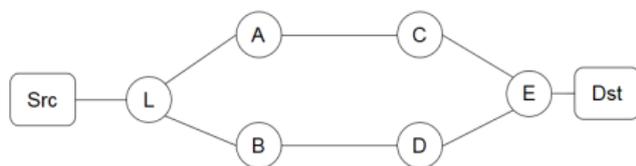
- CAIDA → Ark

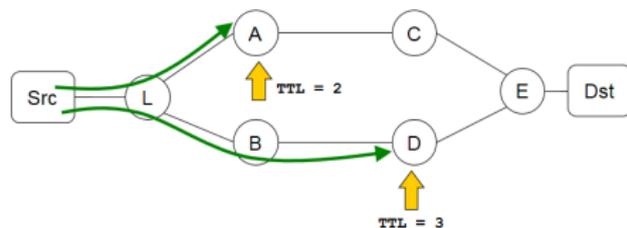
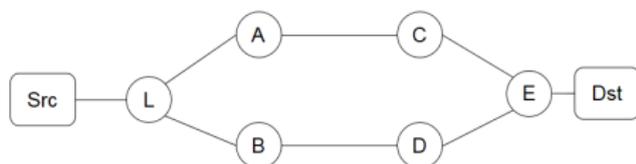
- Integra múltiples herramientas
 - traceroute
 - ping
 - tracelb
 - neighbor discovery
 - etc

- Traceroute → Paris-Traceoute + Paralelización

MAGALLANES

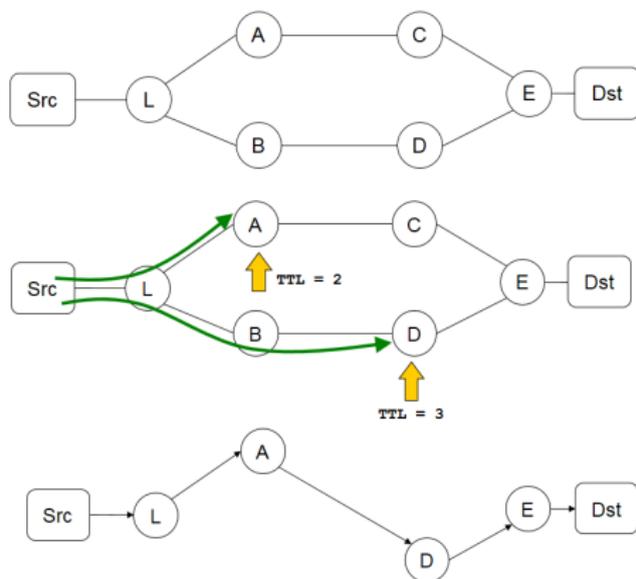
ENTORNO DE TRABAJO: SCAMPER





MAGALLANES

ENTORNO DE TRABAJO: SCAMPER



Nodo L

- *balanceo de carga*
 - Por paquete
 - Por flujo (El mas usual)
(IP_S , IP_D , $Port_S$, $Port_D$, $prot$)
- inferencia errónea

<https://paris-traceroute.net/images/imc2006.ppt>

Resolución de alias

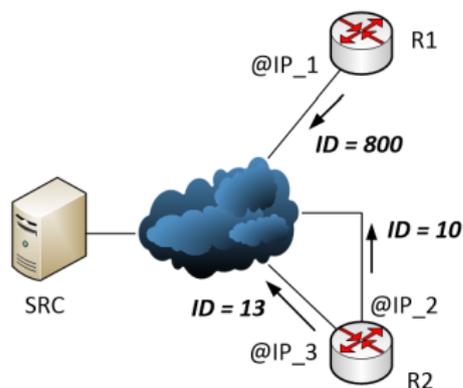
Mayoría de *routers* → Contador común → IP-ID

Idea → Detectar contadores comunes → Sondar a interfaces

Resolución de alias

Mayoría de *routers* → Contador común → IP-ID

Idea → Detectar contadores comunes → Sondar a interfaces



Ejemplo → 3 @IP a resolver

- Sondar → Series de tiempo
- Comparar → MBT (*monotonic bounds test*)
- Eliminar falsos-positivos

MAGALLANES

MÓDULOS

Administración

- Administración del *slice* → Mediante una API que provee PlanetLab
 - Consultar estados de los nodos
 - Agregar nodos al *slice*
 - Quitar nodos del *slice*
- Instalación de paquetes y programas en nodos
- Mantenimiento de tabla de bloques de direcciones IP

MAGALLANES

MÓDULOS

Administración

- Administración del *slice* → Mediante una API que provee PlanetLab
 - Consultar estados de los nodos
 - Agregar nodos al *slice*
 - Quitar nodos del *slice*
- Instalación de paquetes y programas en nodos
- Mantenimiento de tabla de bloques de direcciones IP

Exploración

- **Programar nuevas exploraciones**
- Almacenar exploración
- Resolución de alias y creación de grafos

Usuario

- Monitores
- Target
- Periodo de *traceroute*
- Duración
- Tipo de paquete
- etc

Usuario

- Monitores
- Target
- Periodo de *traceroute*
- Duración
- Tipo de paquete
- etc

Magallanes

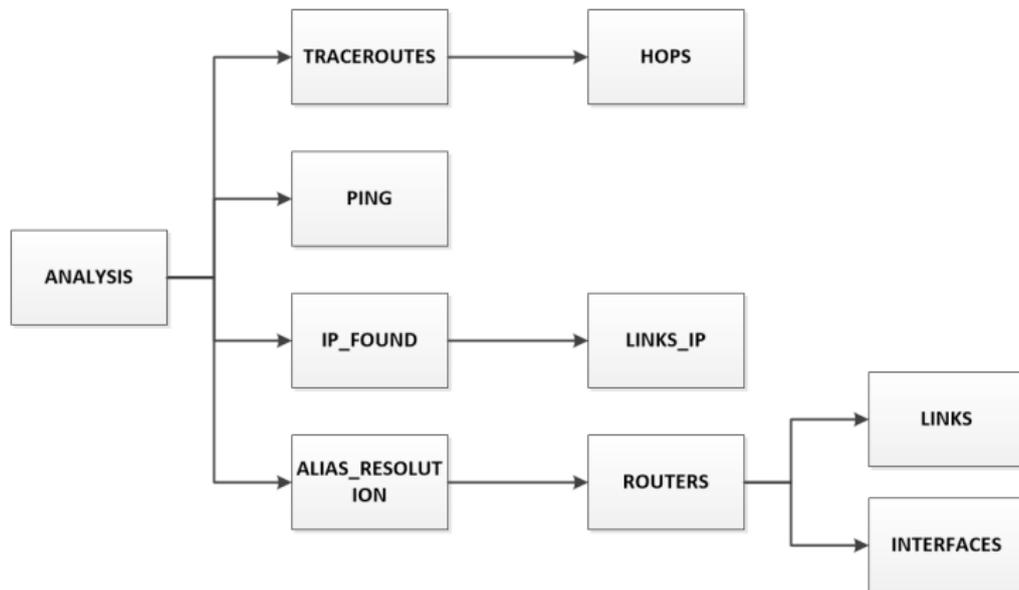
Genera:

- Archivo con el *target*
- Script de ejecución

Transferiere

Ejecuta

ESTRUCTURA DE LA BASE DE DATOS



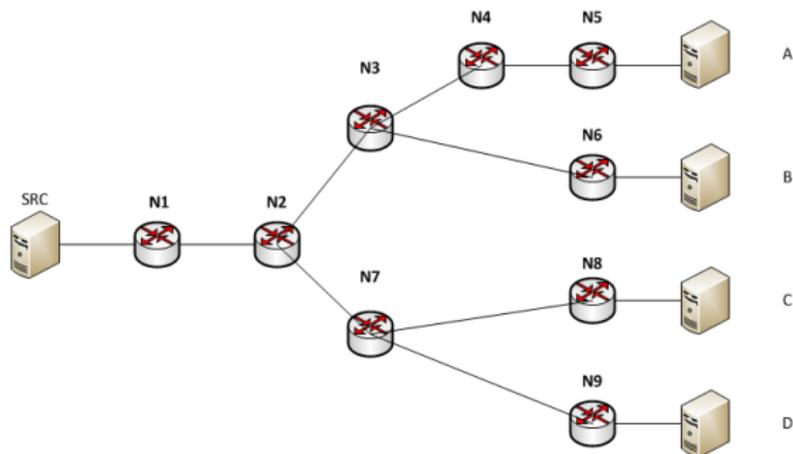
- 1 nodos de PlanetLab por *node_id*
- 2 nodos de PlanetLab aleatorios
- 3 Direcciones públicas por @IP manual
- 4 **Direcciones públicas por @IP aleatorias**

Exploración → Lo más abarcativa → Nodos distribuidos

¿Cómo? → GeoLite2 (MaxMind)

| Continente | #Prefijos | Proporción |
|-------------------|-----------|------------|
| Europa (EU) | 78.433 | 46.8 % |
| Norteamérica (NA) | 49.784 | 29.7 % |
| Asia (AS) | 23.172 | 13.8 % |
| Oceanía (OC) | 6.631 | 3.9 % |
| Sudamérica (SA) | 5.622 | 3.3 % |
| África (AF) | 3.990 | 2.3 % |
| Antártida (An) | 18 | 0.01 % |

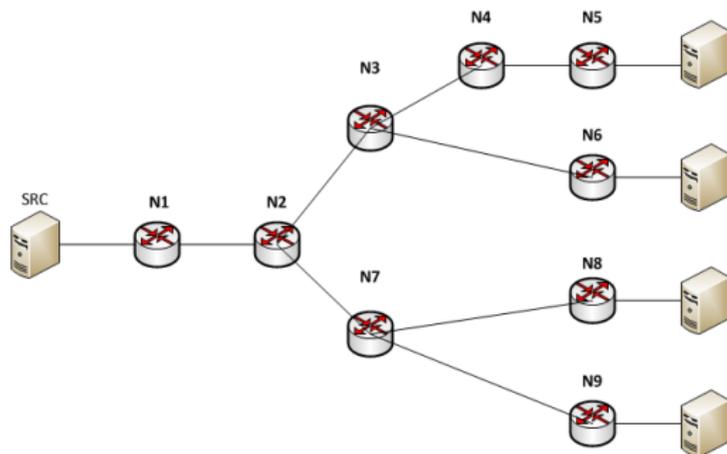
Problema → Sobrecarga hops + Desbalance de mediciones



$$TTL_{Inicial} = 1 \forall @IP_{Dest}$$

| Nodo | #Paquetes |
|------|-----------|
| N1 | 4 |
| N2 | 4 |
| N3 | 2 |
| N4 | 1 |
| N5 | 1 |
| N6 | 1 |
| N7 | 2 |
| N8 | 1 |
| N9 | 1 |

Problema → Sobrecarga *hops* + Desbalance de mediciones

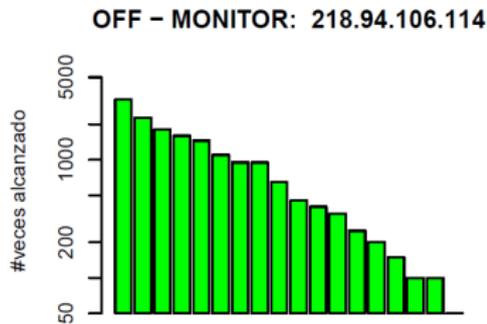


$TTL_{Inicial}$ adaptado a cada $@IP_{Dest}$

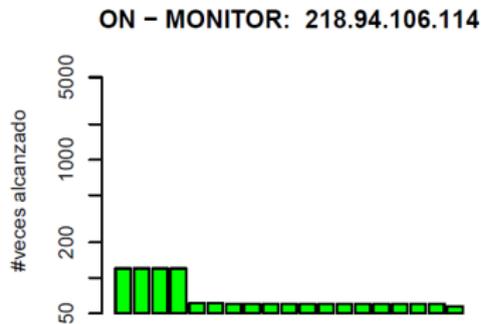
| Nodo | First Hop |
|------|-----------|
| A | 1 |
| B | 4 |
| C | 3 |
| D | 4 |

Ahora todos los hops son muestreados igual cantidad de veces

Ejemplo → 1 nodo, 100 destinos, 50 rondas de traceroutes



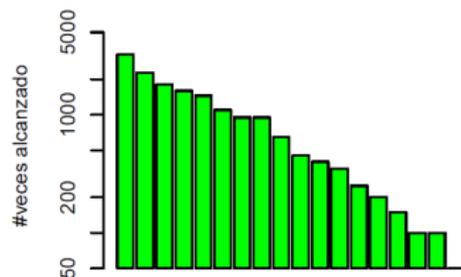
IPs (Hop<=4)



IPs (Hop<=4)

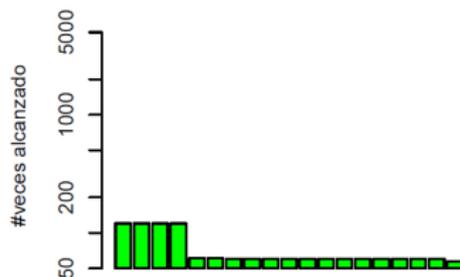
Ejemplo → 1 nodo, 100 destinos, 50 rondas de traceroutes

OFF - MONITOR: 218.94.106.114



IPs (Hop<=4)

ON - MONITOR: 218.94.106.114



IPs (Hop<=4)

CONCLUSIÓN

Se ha reducido la variación en la cantidad de veces que cada @IP es muestreada

MIDAR: 2 modos de funcionamiento

- **Local** → hasta 40.000 IPs → no alcanza
- **Distribuido** → varios millones de IP → no podemos ejecutarlo

MIDAR: 2 modos de funcionamiento

- **Local** → hasta 40.000 IPs → no alcanza
- **Distribuido** → varios millones de IP → no podemos ejecutarlo

Solución (**Ken Keys** - CAIDA) → dividir conjunto de @IPs y resolver en local

- menor a 40.000 IP
- mismo *método preferido* (UDP, TCP, ICMP)
- primer byte de dirección IP idéntico

TABLA DE CONTENIDOS

1 INTRODUCCIÓN Y ESTADO DEL ARTE

2 MAGALLANES

3 DESPLIEGUE DE EXPERIMENTOS

4 CONCLUSIONES

1 Exploración de la red

- 1 Exploración de la red
- 2 Adquisición de datos para trabajo sobre MPLS

- 1 Exploración de la red
- 2 Adquisición de datos para trabajo sobre MPLS
- 3 Adquisición de datos para trabajo sobre RTT

DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: OBJETIVO Y PREPARACIÓN

Objetivo: Priorizar cantidad de IPs y Enlaces

Relación de compromiso entre parámetros

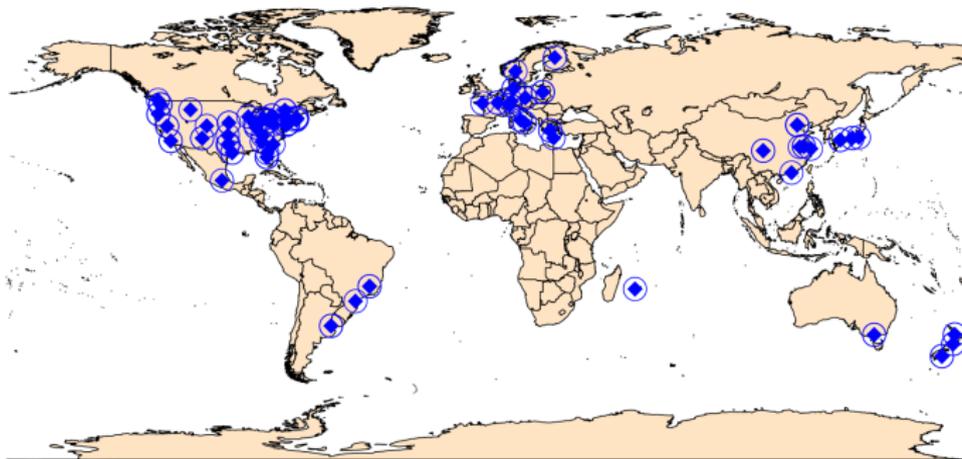
DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: OBJETIVO Y PREPARACIÓN

Objetivo: Priorizar cantidad de IPs y Enlaces

Relación de compromiso entre parámetros

- #Monitores: 104
- #Target: 100.000 IP/Monitor
- Periodo: 3600s
- Duración: 12h
- pps: 350
- Sonda: UDP-Paris
- Recalculo de FH



DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: RESULTADOS Y ANÁLISIS

Primeros resultados

~1.3M de IPs → ~2.3M de enlaces → 102K alias agrupando 402 mil IPs (31%)

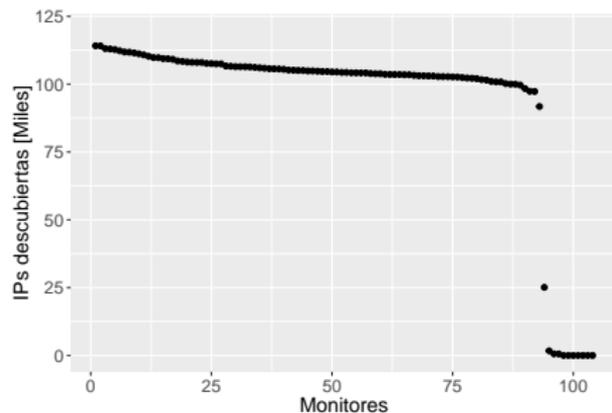
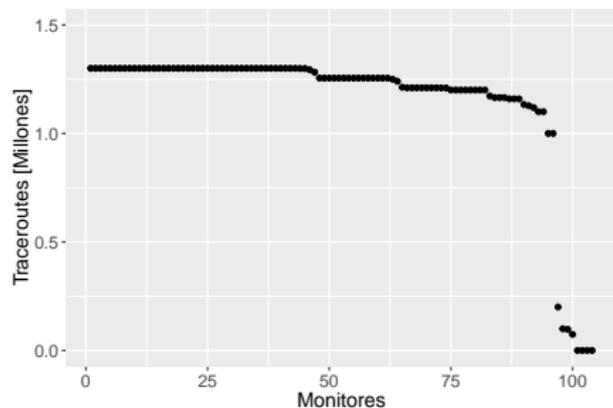
| Continente | #IP | Proporción |
|-------------------|---------|------------|
| Europa (EU) | 578.800 | 43.9 % |
| Norteamérica (NA) | 378.369 | 28.7 % |
| Asia (AS) | 231.092 | 17.5 % |
| Sudamérica (SA) | 50.230 | 3.8 % |
| Oceanía (OC) | 26.726 | 2.0 % |
| África (AF) | 21.577 | 1.6 % |
| Antártida (An) | 18 | 0.0 % |
| no localizables | 32.065 | 2.4 % |

| | AF | SA | OC | AS | NA | EU |
|----|--------|--------|--------|---------|---------|---------|
| EU | 5.920 | 6.629 | 902 | 21.722 | 148.228 | 977.776 |
| NA | 5.179 | 14.193 | 5.352 | 35.590 | 517.006 | 148.228 |
| AS | 1.277 | 422 | 4.374 | 394.699 | 35.590 | 21.722 |
| OC | 294 | 12 | 34.792 | 4.374 | 5.352 | 902 |
| SA | 119 | 39.077 | 12 | 422 | 14.193 | 6.629 |
| AF | 19.367 | 119 | 294 | 1.277 | 5.179 | 5.920 |

DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: RESULTADOS Y ANÁLISIS

Resultados por nodo



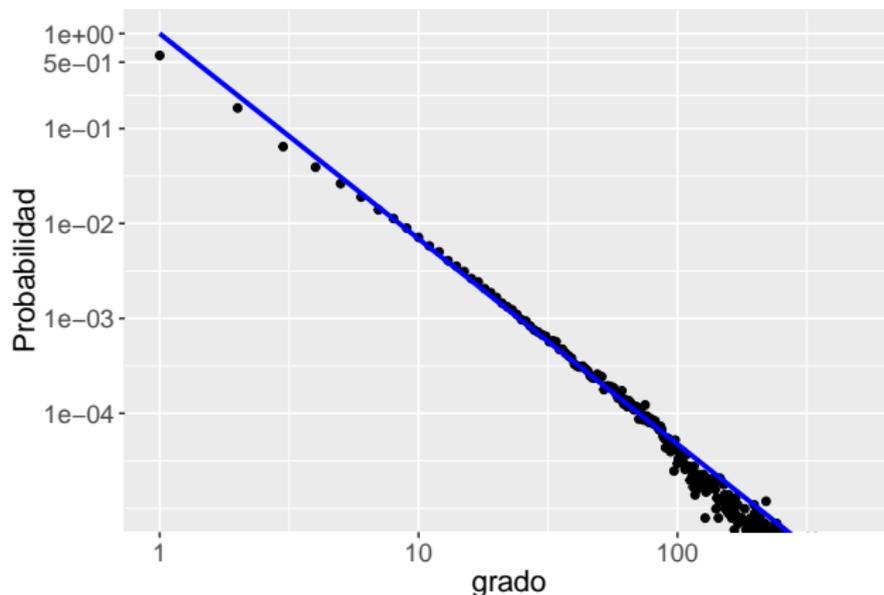
DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: RESULTADOS Y ANÁLISIS

Distribución de grado

$P(k)$ con cola pesada

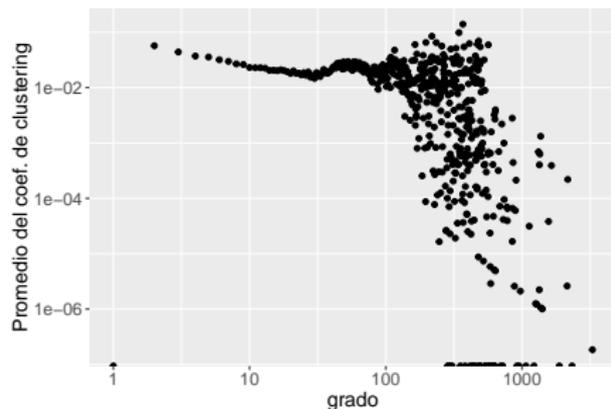
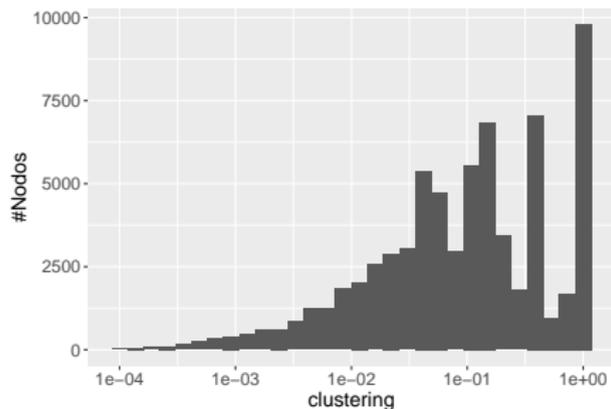
$\rightarrow P(k) \sim k^{-2.162}$, $p_{value} < 0.01$ para $k_{min} = 5$ (Clauset, Shalizi, Newman)



DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: RESULTADOS Y ANÁLISIS

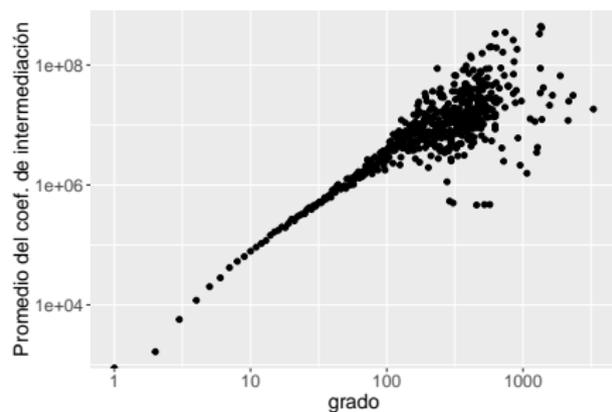
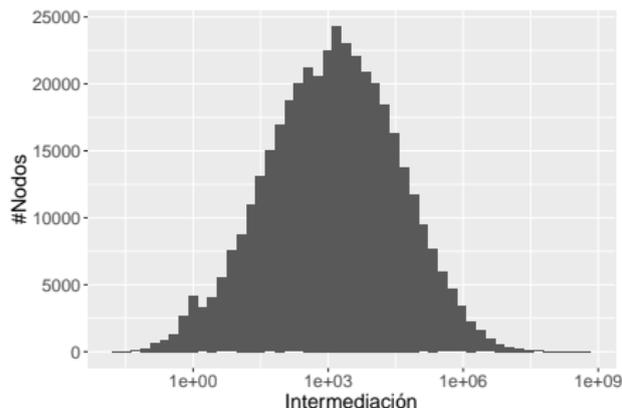
Coeficiente de agrupamiento (*clustering*)



DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: RESULTADOS Y ANÁLISIS

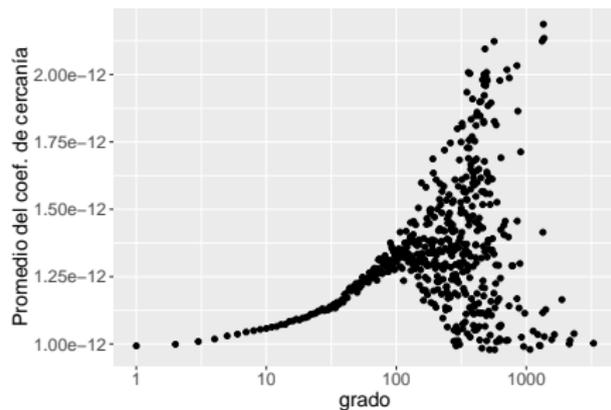
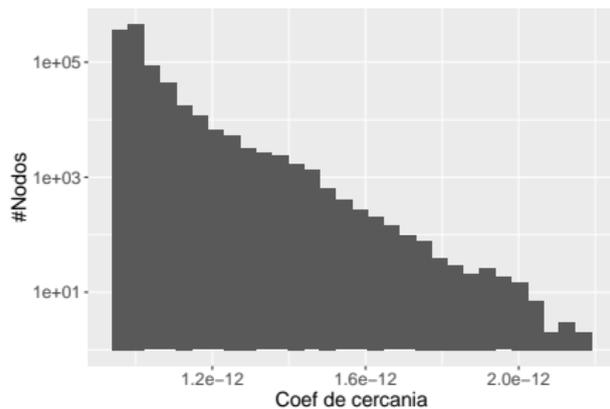
Intermediación (*betweenness*)



DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: RESULTADOS Y ANÁLISIS

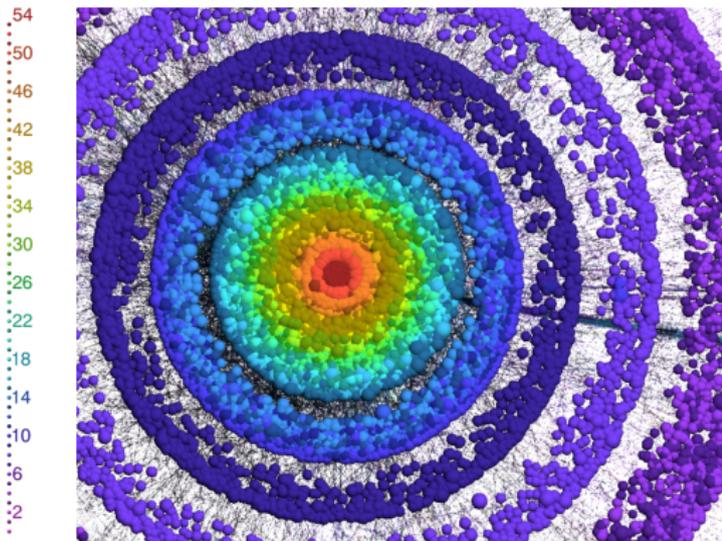
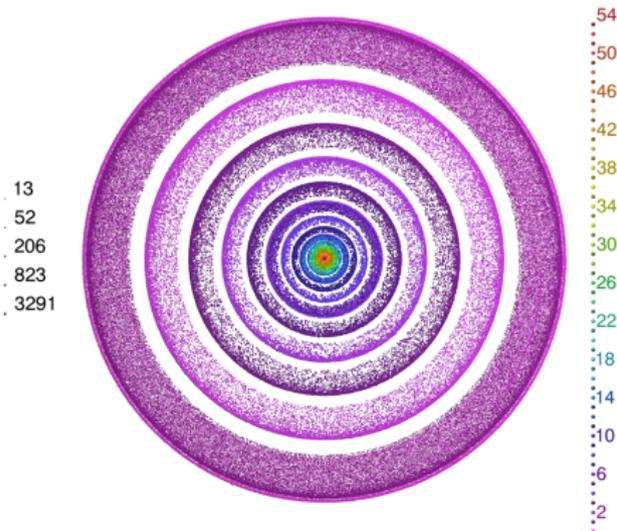
Cercanía (*closeness*)



DESPLIEGUE DE EXPERIMENTOS

EXPLORACIÓN: RESULTADOS Y ANÁLISIS

Visualización de la topología descomposición en k-núcleos \rightarrow LaNet-vi



DESPLIEGUE DE EXPERIMENTOS

REVELANDO LA ESTRUCTURA MPLS EN LA TOPOLOGÍA DE INTERNET

Unveiling the MPLS Structure on Internet Topology

(Fernando Davila Revelo, Mauricio Anderson Ricci, Benoit Donnet y José Ignacio Alvarez-Hamelin. En *International Workshop for Traffic Monitoring and Analysis 2016*)

DESPLIEGUE DE EXPERIMENTOS

REVELANDO LA ESTRUCTURA MPLS EN LA TOPOLOGÍA DE INTERNET

Unveiling the MPLS Structure on Internet Topology

(Fernando Davila Revelo, Mauricio Anderson Ricci, Benoit Donnet y José Ignacio Alvarez-Hamelin. En *International Workshop for Traffic Monitoring and Analysis 2016*)

Objetivo:

- Estudiar el nivel de implementación de MPLS
- Evaluar técnicas para detección de túneles

DESPLIEGUE DE EXPERIMENTOS

REVELANDO LA ESTRUCTURA MPLS EN LA TOPOLOGÍA DE INTERNET

Unveiling the MPLS Structure on Internet Topology

(Fernando Davila Revelo, Mauricio Anderson Ricci, Benoit Donnet y José Ignacio Alvarez-Hamelin. En *International Workshop for Traffic Monitoring and Analysis 2016*)

Objetivo:

- Estudiar el nivel de implementación de MPLS
- Evaluar técnicas para detección de túneles

Resultados y conclusiones:

- Uso extendido de MPLS en Internet.
- 44% de los *traceroutes* con etiquetas MPLS; 34% atraviesan túneles explícitos, y 42% ya sea explícitos o implícitos.
- En detección de túneles implícitos las firmas *u-turn* están sesgadas por balanceo por flujo en caminos de retorno

DESPLIEGUE DE EXPERIMENTOS

MEDICIÓN DEL RTT EN LOS PRIMEROS HOPS

RTT → tiempo que tarda un paquete en ir y volver hasta receptor

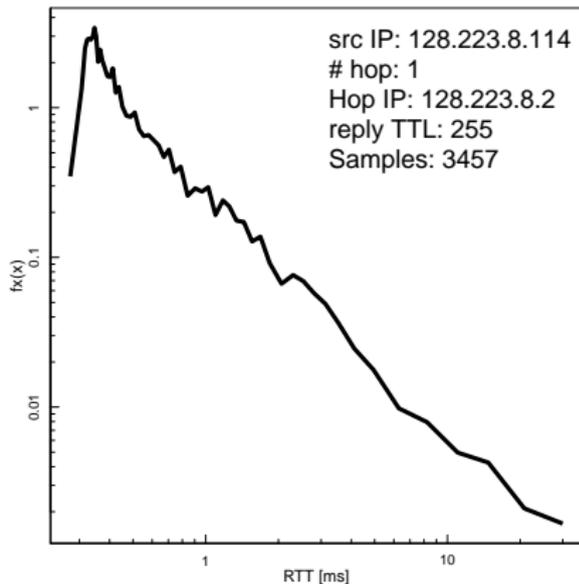
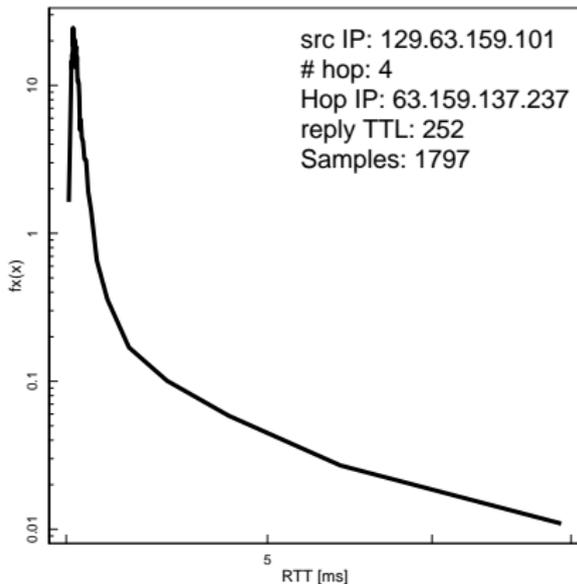
CoNexDat → estudio del RTT en los primeros hops → MAGALLANES

DESPLIEGUE DE EXPERIMENTOS

MEDICIÓN DEL RTT EN LOS PRIMEROS HOPS

RTT → tiempo que tarda un paquete en ir y volver hasta receptor

CoNexDat → estudio del RTT en los primeros hops → MAGALLANES



DESPLIEGUE DE EXPERIMENTOS

MEDICIÓN DEL RTT EN LOS PRIMEROS HOPS

RTT → tiempo que tarda un paquete en ir y volver hasta receptor

CoNexDat → estudio del RTT en los primeros hops → MAGALLANES

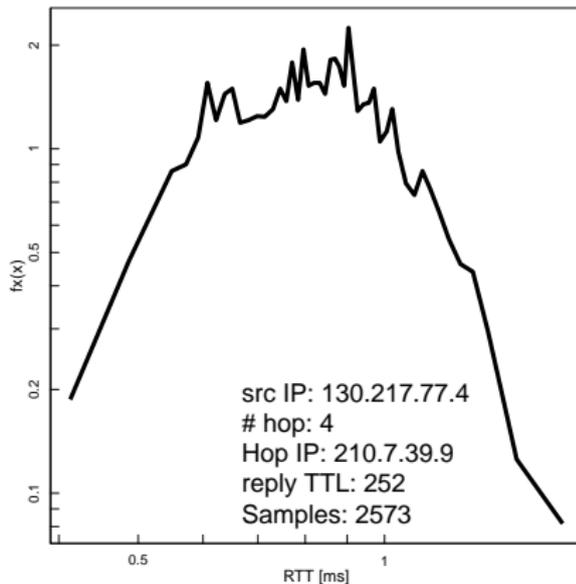
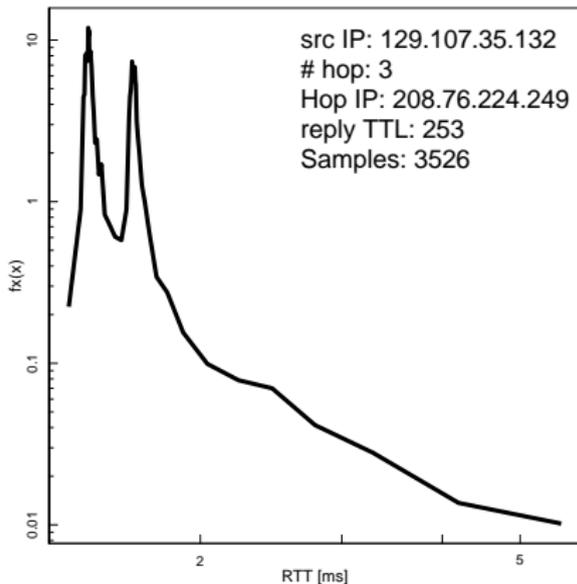


TABLA DE CONTENIDOS

- 1 INTRODUCCIÓN Y ESTADO DEL ARTE
- 2 MAGALLANES
- 3 DESPLIEGUE DE EXPERIMENTOS
- 4 CONCLUSIONES

Contribuciones de esta tesis

- Plataforma de medición → MAGALLANES (*open source*)
- Exploración de la red, Análisis de túneles MPLS, Mediciones RTT
- Publicación en *International Workshop for Traffic Monitoring and Analysis 2016*

Contribuciones de esta tesis

- Plataforma de medición → MAGALLANES (*open source*)
- Exploración de la red, Análisis de túneles MPLS, Mediciones RTT
- Publicación en *International Workshop for Traffic Monitoring and Analysis 2016*

Trabajos futuros

- Estudio de la red por región
- Estudio de otros parámetros de la topología → latencias, disponibilidad, frecuencia de cambio en las rutas, etc
- Ampliar las capacidades de la plataforma → mapeo a ASN

Gracias