

IXP: Mediciones y monitoreo

Hernán Galperin*, J. Ignacio Alvarez-Hamelin^{†‡§} y
Esteban Carisimo**

* CONICET – Universidad de San Andrés

† Instituto Tecnológico de Buenos Aires

‡ CONICET – Facultad de Ingeniería UBA

§ GRCyCD – Facultad de Ingeniería UBA

<http://cnet.fi.uba.ar/>

** GRCyCD – Facultad de Ingeniería UBA

<http://cnet.fi.uba.ar/>

Noviembre 2014

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

Frases de Lord Kelvin:

- *“Medir es saber”*
- *“Si no puedes medirlo, no puedes mejorarlo”*

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia (*cantidad de saltos*)
- Tasa de pérdida de paquetes

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia (*cantidad de saltos*)
- Tasa de pérdida de paquetes

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia (*cantidad de saltos*)
- Tasa de pérdida de paquetes

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia (*cantidad de saltos*)
- Tasa de pérdida de paquetes

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia (*cantidad de saltos*)
- Tasa de pérdida de paquetes

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia (*cantidad de saltos*)
- Tasa de pérdida de paquetes

Si medir es saber, ¿Qué es lo que quiero saber?

Parámetros más comunes

- Tráfico
- *Hosts* activos
- Latencia
- Distancia (*cantidad de saltos*)
- Tasa de pérdida de paquetes

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute`, `ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute`, `ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute`, `ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute`, `ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Como se lleva adelante el monitoreo?

Por medio de:

- Encuestas SNMP
- Protocolo ICMP (`traceroute`, `ping`)
- Conexiones TCP o datagramas UDP
- Tablas BGP

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

¿Qué herramientas existen?

Proyectos *open-source*:

- Cacti
- SmokePing
- openNMS

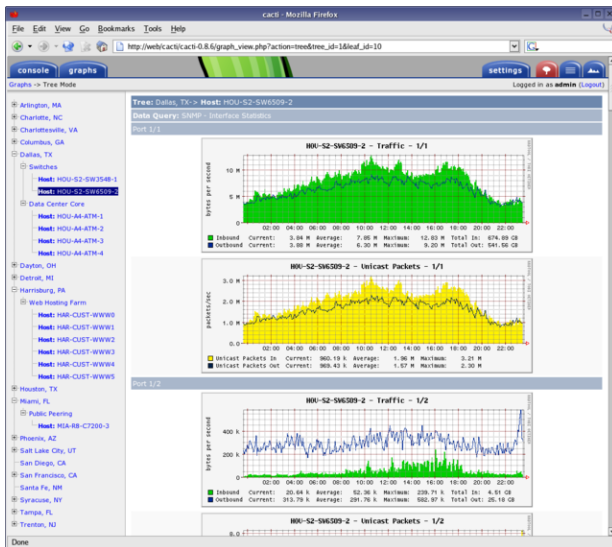
Desarrollada *ad-hoc* para PIT Bolivia:

- PladMeD

Acerca de Cacti:

- Front-end en PHP para generar gráficos de variables de red
- Fuentes de datos:
 - Cualquier fuente externa
 - A través de RRDTool
 - Almacenados en MySQL
- Soporte SNMP y creación de MRTG
- Capacidad para estructurar la información de forma jerárquica a través de árboles

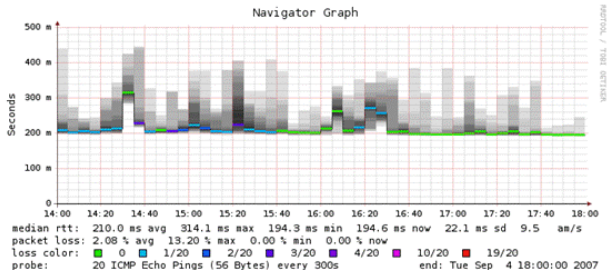
Ejemplo Cacti



Acerca de SmokePing:

- Herramienta para medir latencia y tasa de pérdida de paquetes
- Herramienta dividida en dos:
 - *back-end*: Obtención y almacenamiento de datos
 - *front-end*: Presentación web
- Almacena y gráfica la distribución de los parámetros
- Puede calcular la latencia de distintos protocolos:
 - ICMP (ping)
 - HTTP
 - DNS
- Almacena los datos a través de RRDTool
- Capacidad para generar alarmas
- Capacidad *Master-Slave*: Poder generar pruebas desde puntos remotos

Ejemplo SmokePing



Sistema de monitoreo con multiples prestaciones teniendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
 - Capacidad propia o de fuentes externas para obtener información
 - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
 - Capacidad de almacenamiento de SNMP y JMX
 - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
 - Capacidad de generar gráfico "TOP N"

Sistema de monitoreo con multiples prestaciones teniendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
 - Capacidad propia o de fuentes externas para obtener información
 - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
 - Capacidad de almacenamiento de SNMP y JMX
 - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
 - Capacidad de generar gráfico "TOP N"

Sistema de monitoreo con multiples prestaciones teniendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
 - Capacidad propia o de fuentes externas para obtener información
 - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
 - Capacidad de almacenamiento de SNMP y JMX
 - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
 - Capacidad de generar gráfico "TOP N"

Sistema de monitoreo con multiples prestaciones teniendo como destacadas las siguientes áreas:

- Capacidad de detectar los servicios prestados en la red monitoreada
- Almacenamiento y reportes:
 - Capacidad propia o de fuentes externas para obtener información
 - Disponibilidad para enviar reportes por e-mail o SMS
- Medición de performance
 - Capacidad de almacenamiento de SNMP y JMX
 - Comparación contra umbrales sofisticados (cambios absolutos y relativos)
 - Capacidad de generar gráfico "TOP N"

Ejemplo openNMS (I)

Results 1-10 of 16

1 2 [Next](#) [Last](#)

Ack	ID	Severity	Node	Interface	Service	Count	Last Event Time	First Event Time
			Ackd	Ackd Time				
	1	Critical [+]	172.20.1.201 [+]	0.0.0.0 [+]		3	4/21/05 6:05:41 PM [<] [>]	4/20/05 6:36:26 PM [<] [>]
Node 172.20.1.201 is down.								
	11	Critical [+]	172.20.1.200 [+]	0.0.0.0 [+]		1	4/22/05 6:26:21 PM [<] [>]	4/22/05 6:26:21 PM [<] [>]
Node 172.20.1.200 is down.								
	10	Critical [+]	David-Hustaces-Computer.local [+]	0.0.0.0 [+]		2	4/22/05 6:26:33 PM [<] [>]	4/22/05 2:35:43 PM [<] [>]
Node David-Hustaces-Computer.local is down.								
	3	Major [+]	barbrady.opennms.com [+]	172.20.1.11 [+]	HTTP [+]	2	4/20/05 5:25:51 PM [<] [>]	4/20/05 5:10:43 PM [<] [>]
HTTP outage identified on interface 172.20.1.11.								
	5	Major [+]	barbrady.opennms.com [+]	172.20.1.11 [+]	HTTPS [+]	2	4/20/05 5:25:53 PM [<] [>]	4/20/05 5:10:44 PM [<] [>]
HTTPS outage identified on interface 172.20.1.11.								
	11	Major [+]	barbrady.opennms.com [+]	172.20.1.11 [+]	HTTP-8080 [+]	1	4/22/05 10:58:38 AM [<] [>]	4/22/05 10:58:38 AM [<] [>]
HTTP-8080 outage identified on interface 172.20.1.11.								
	16	Major [+]	carlman.opennms.com [+]	172.20.1.10 [+]	HTTP [+]	1	4/22/05 8:09:44 PM [<] [>]	4/22/05 8:09:44 PM [<] [>]
HTTP outage identified on interface 172.20.1.10.								
	9	Major [+]	172.20.1.201 [+]	172.20.1.201 [+]	SSH [+]	23	4/23/05 7:44:32 AM [<] [>]	4/21/05 3:57:30 PM [<] [>]
SSH outage identified on interface 172.20.1.201.								
		Normal [+]	mrmakey.opennms.com [+]	172.20.1.1 [+]		38/05	4/23/05 11:14:14 AM [<] [>]	4/19/05 4:45:10 PM [<] [>]
Linksys Event: @out TCP from 172.20.1.204:65247 to 198.128.246.160[198.128.246.160]:80.								
	8	Cleared [+]	barbrady.opennms.com [+]	172.20.1.11 [+]	HTTPS [+]	2	4/20/05 5:27:56 PM [<] [>]	4/20/05 5:20:53 PM [<] [>]
The HTTPS outage on interface 172.20.1.11 has been cleared. Service is restored.								

10 alarms

[Acknowledge Alarms](#) [Select All](#) [Reset](#)

Ejemplo openNMS (II)



Siguiente presentación

Plataforma de Medición Distribuida

Experiencia PIT Bolivia

Hernán Galperin*, J. Ignacio Alvarez-Hamelin^{†‡§} y
Esteban Carisimo**

*CONICET – Universidad de San Andrés

†Instituto Tecnológico de Buenos Aires

‡CONICET – Facultad de Ingeniería UBA

§GRCyCD – Facultad de Ingeniería UBA

<http://cnet.fi.uba.ar/>

**GRCyCD – Facultad de Ingeniería UBA

<http://cnet.fi.uba.ar/>

Noviembre 2014

Infraestructura compuesta por:

- sonda: **RaspberryPI** con **Raspbian/Debian** 16GB de almacenamiento (objetivo instalar 12)
- **distribuidas** en distintos puntos de la **red** (a determinar)
- una sonda en el PIT

Características de las sondas:

- cada **sonda** se conecta con una **IP pública** a **Internet**
- **sin** filtrado de paquetes **ICMP**, **UDP** o **TCP**
- **administración** por **ssh**

Infraestructura compuesta por:

- sonda: **RaspberryPI** con **Raspbian/Debian** 16GB de almacenamiento (objetivo instalar 12)
- distribuidas en distintos puntos de la red (a determinar)
- una sonda en el PIT

Características de las sondas:

- cada sonda se conecta con una IP pública a Internet
- sin filtrado de paquetes ICMP, UDP o TCP
- administración por ssh

Infraestructura compuesta por:

- sonda: **RaspberryPI** con **Raspbian/Debian** 16GB de almacenamiento (objetivo instalar 12)
- **distribuidas** en distintos puntos de la **red** (a determinar)
- una sonda en el PIT

Características de las sondas:

- cada **sonda** se conecta con una **IP pública** a **Internet**
- **sin** filtrado de paquetes **ICMP, UDP** o **TCP**
- **administración** por **ssh**

Infraestructura compuesta por:

- sonda: **RaspberryPI** con **Raspbian/Debian** 16GB de almacenamiento (objetivo instalar 12)
- **distribuidas** en distintos puntos de la **red** (a determinar)
- una sonda en el PIT

Características de las sondas:

- cada **sonda** se conecta con una **IP pública** a **Internet**
- **sin** filtrado de paquetes **ICMP, UDP** o **TCP**
- **administración** por **ssh**

Infraestructura compuesta por:

- sonda: **RaspberryPI** con **Raspbian/Debian** 16GB de almacenamiento (objetivo instalar 12)
- **distribuidas** en distintos puntos de la **red** (a determinar)
- una sonda en el PIT

Características de las sondas:

- cada **sonda** se conecta con una **IP pública** a **Internet**
- **sin** filtrado de paquetes ICMP, UDP o TCP
- **administración** por **ssh**

Infraestructura compuesta por:

- sonda: **RaspberryPI** con **Raspbian/Debian** 16GB de almacenamiento (objetivo instalar 12)
- **distribuidas** en distintos puntos de la **red** (a determinar)
- una sonda en el PIT

Características de las sondas:

- cada **sonda** se conecta con una **IP pública** a **Internet**
- **sin** filtrado de paquetes ICMP, UDP o TCP
- **administración** por **ssh**

Infraestructura compuesta por:

- sonda: **RaspberryPI** con **Raspbian/Debian** 16GB de almacenamiento (objetivo instalar 12)
- **distribuidas** en distintos puntos de la **red** (a determinar)
- una sonda en el PIT

Características de las sondas:

- cada **sonda** se conecta con una **IP pública** a **Internet**
- **sin** filtrado de paquetes ICMP, UDP o TCP
- **administración** por **ssh**

¿Qué hemos medido?

Indicador	Fuente	Unidad
Velocidad downlink	Netindex	Mbps
Velocidad uplink	Netindex	Mbps
Distancia	PladMeD	saltos (min, media, mediana y máx)
Latencia	PladMeD	ms (min, media, mediana y máx)
% rutas locales(*)	PladMeD	% (posibles rutas)
% tiempo accesible(*)	PladMeD	% (posibles rutas)
Servicios	Sonda externa	Cantidad

() Parámetros ad-hoc para analizar la incidencia del PIT*

SNMP consultas del **número** de **bytes** y **paquetes**,
transmitidos y recibidos

- PladMeD**
- *Prefijos IP:* **traceroutes** a **una dirección** IP por red asignada por LACNIC a Bolivia.
 - *Servicios:* **Zmap** a **todas las direcciones** asignadas por LACNIC a Bolivia.

SNMP consultas del **número** de **bytes** y **paquetes**,
transmitidos y recibidos

- PladMeD**
- *Prefijos IP:* **traceroutes** a **una dirección**
IP por red asignada por LACNIC a Bolivia.
 - *Servicios:* **Zmap** a **todas** las **direcciones**
asignadas por LACNIC a Bolivia.

SNMP consultas del **número** de **bytes** y **paquetes**,
transmitidos y recibidos

- PladMeD**
- *Prefijos* IP: **traceroutes** a **una dirección** IP por red asignada por LACNIC a Bolivia.
 - *Servicios*: **Zmap** a **todas las direcciones** asignadas por LACNIC a Bolivia.

- Segmentación de la red: *“IPv4 Routed /24 Topology”*
- Cantidad de prefijos:
 - Bolivia: 4438
 - Paraguay: 4155
- traceroutes en simultáneo
 - A través de scamper
 - Utilización de la capacidad: **11 kB/s**

- Segmentación de la red: *“IPv4 Routed /24 Topology”*
- Cantidad de prefijos:
 - Bolivia: 4438
 - Paraguay: 4155
- traceroutes en simultáneo
 - A través de scamper
 - Utilización de la capacidad: **11 kB/s**

- Segmentación de la red: *“IPv4 Routed /24 Topology”*
- Cantidad de prefijos:
 - Bolivia: 4438
 - Paraguay: 4155
- traceroutes en simultáneo
 - A través de scamper
 - Utilización de la capacidad: **11 kB/s**

- Segmentación de la red: *“IPv4 Routed /24 Topology”*
- Cantidad de prefijos:
 - Bolivia: 4438
 - Paraguay: 4155
- traceroutes en simultáneo
 - A través de scamper
 - Utilización de la capacidad: **11 kB/s**

- Segmentación de la red: *“IPv4 Routed /24 Topology”*
- Cantidad de prefijos:
 - Bolivia: 4438
 - Paraguay: 4155
- `traceroutes` en simultáneo
 - A través de `scamper`
 - Utilización de la capacidad: **11 kB/s**

PladMeD

- *% rutas locales* : **traceroutes** a una **dirección** IP por red asignada por LACNIC a Bolivia. Se calcula la **fracción** que pasa por el **PIT**.
- *% tiempo accesible*: en base a los traceroutes, se calcula la **fracción** de veces que se accedió pasando por el PIT.
- *Latencia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y NO se descarta por **umbral**.
- *Distancia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y se descarta por **umbral**.

PladMeD

- *% rutas locales* : **traceroutes** a una **dirección** IP por red asignada por LACNIC a Bolivia. Se calcula la **fracción** que pasa por el **PIT**.
- *% tiempo accesible*: en base a los traceroutes, se calcula la **fracción** de veces que se accedió pasando por el PIT.
- *Latencia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y NO se descarta por **umbral**.
- *Distancia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y se descarta por **umbral**.

PladMeD

- *% rutas locales* : **traceroutes** a una **dirección** IP por red asignada por LACNIC a Bolivia. Se calcula la **fracción** que pasa por el **PIT**.
- *% tiempo accesible*: en base a los traceroutes, se calcula la **fracción** de veces que se accedió pasando por el PIT.
- *Latencia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y NO se descarta por **umbral**.
- *Distancia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y se descarta por **umbral**.

PladMeD

- *% rutas locales* : **traceroutes** a una **dirección** IP por red asignada por LACNIC a Bolivia. Se calcula la **fracción** que pasa por el **PIT**.
- *% tiempo accesible*: en base a los traceroutes, se calcula la **fracción** de veces que se accedió pasando por el PIT.
- *Latencia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y NO se descarta por **umbral**.
- *Distancia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y se descarta por **umbral**.

PladMeD

- *% rutas locales* : **traceroutes** a una **dirección** IP por red asignada por LACNIC a Bolivia. Se calcula la **fracción** que pasa por el **PIT**.
- *% tiempo accesible*: en base a los traceroutes, se calcula la **fracción** de veces que se accedió pasando por el PIT.
- *Latencia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y NO se descarta por **umbral**.
- *Distancia*: Se envían paquetes entre dos **redes** asignadas a **Bolivia** y se descarta por **umbral**.

¿Cómo hemos categorizado?

Según su medio de distribución

- **PIT:** Se detecta que el `traceroute` contiene una IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **P2P:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **Anómalas:** Se detecta que el `traceroute` contiene una IP de la red del PIT y al menos un salto NO pertenecen a las direcciones asignadas por LACNIC a Bolivia.
- **Internacionales:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y al menos un salto NO pertenece las a direcciones asignadas por LACNIC a Bolivia.

¿Cómo hemos categorizado?

Según su medio de distribución

- **PIT:** Se detecta que el `traceroute` contiene una IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **P2P:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **Anómalas:** Se detecta que el `traceroute` contiene una IP de la red del PIT y al menos un salto NO pertenecen a las direcciones asignadas por LACNIC a Bolivia.
- **Internacionales:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y al menos un salto NO pertenece las a direcciones asignadas por LACNIC a Bolivia.

¿Cómo hemos categorizado?

Según su medio de distribución

- **PIT:** Se detecta que el `traceroute` contiene una IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **P2P:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **Anómalas:** Se detecta que el `traceroute` contiene una IP de la red del PIT y al menos un salto NO pertenecen a las direcciones asignadas por LACNIC a Bolivia.
- **Internacionales:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y al menos un salto NO pertenece las a direcciones asignadas por LACNIC a Bolivia.

¿Cómo hemos categorizado?

Según su medio de distribución

- **PIT:** Se detecta que el `traceroute` contiene una IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **P2P:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **Anómalas:** Se detecta que el `traceroute` contiene una IP de la red del PIT y al menos un salto NO pertenecen a las direcciones asignadas por LACNIC a Bolivia.
- **Internacionales:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y al menos un salto NO pertenece las a direcciones asignadas por LACNIC a Bolivia.

¿Cómo hemos categorizado?

Según su medio de distribución

- **PIT:** Se detecta que el `traceroute` contiene una IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **P2P:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **Anómalas:** Se detecta que el `traceroute` contiene una IP de la red del PIT y al menos un salto NO pertenecen a las direcciones asignadas por LACNIC a Bolivia.
- **Internacionales:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y al menos un salto NO pertenece las a direcciones asignadas por LACNIC a Bolivia.

¿Cómo hemos categorizado?

Según su medio de distribución

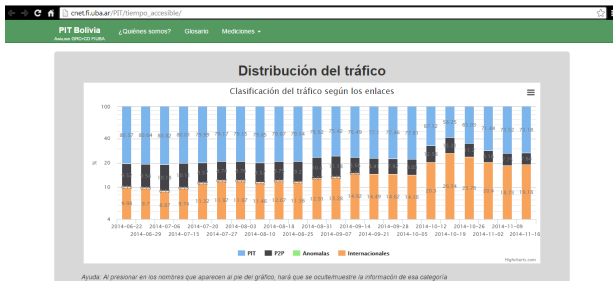
- **PIT:** Se detecta que el `traceroute` contiene una IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **P2P:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y todos los saltos pertenecen a direcciones asignadas por LACNIC a Bolivia.
- **Anómalas:** Se detecta que el `traceroute` contiene una IP de la red del PIT y al menos un salto NO pertenecen a las direcciones asignadas por LACNIC a Bolivia.
- **Internacionales:** Se detecta que el `traceroute` NO contiene ninguna IP de la red del PIT y al menos un salto NO pertenece las a direcciones asignadas por LACNIC a Bolivia.

¿Cómo hemos categorizado?

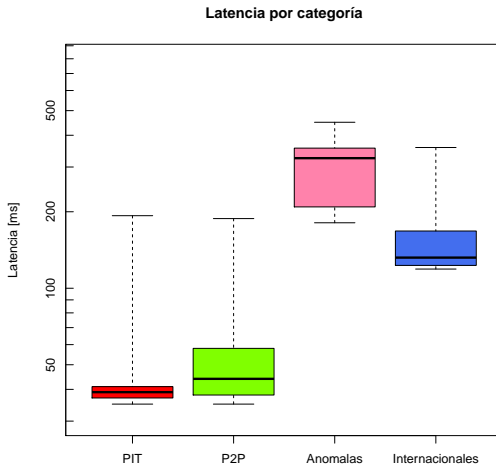
Categoría	Atraviesa el PIT	Sin IPs en el extranjero
PIT	X	X
P2P		X
Anómalas	X	
Internacionales		

¿Cómo hemos presentado la información?

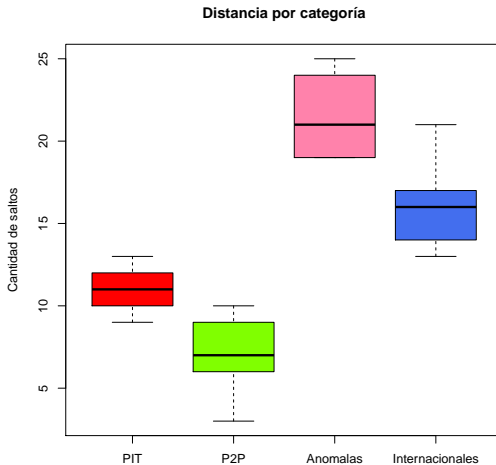
A través de una página web de actualización semanal
<http://cnet.fi.uba.ar/PIT/>



¿Qué resultados hemos obtenido?



¿Qué resultados hemos obtenido?



Gracias por su atención