Detectando y midiendo NAT en Internet

Alejandro Acosta
Alejandro @ lacnic.net
@ITandNetworking

Midiendo NAT desde el navegador

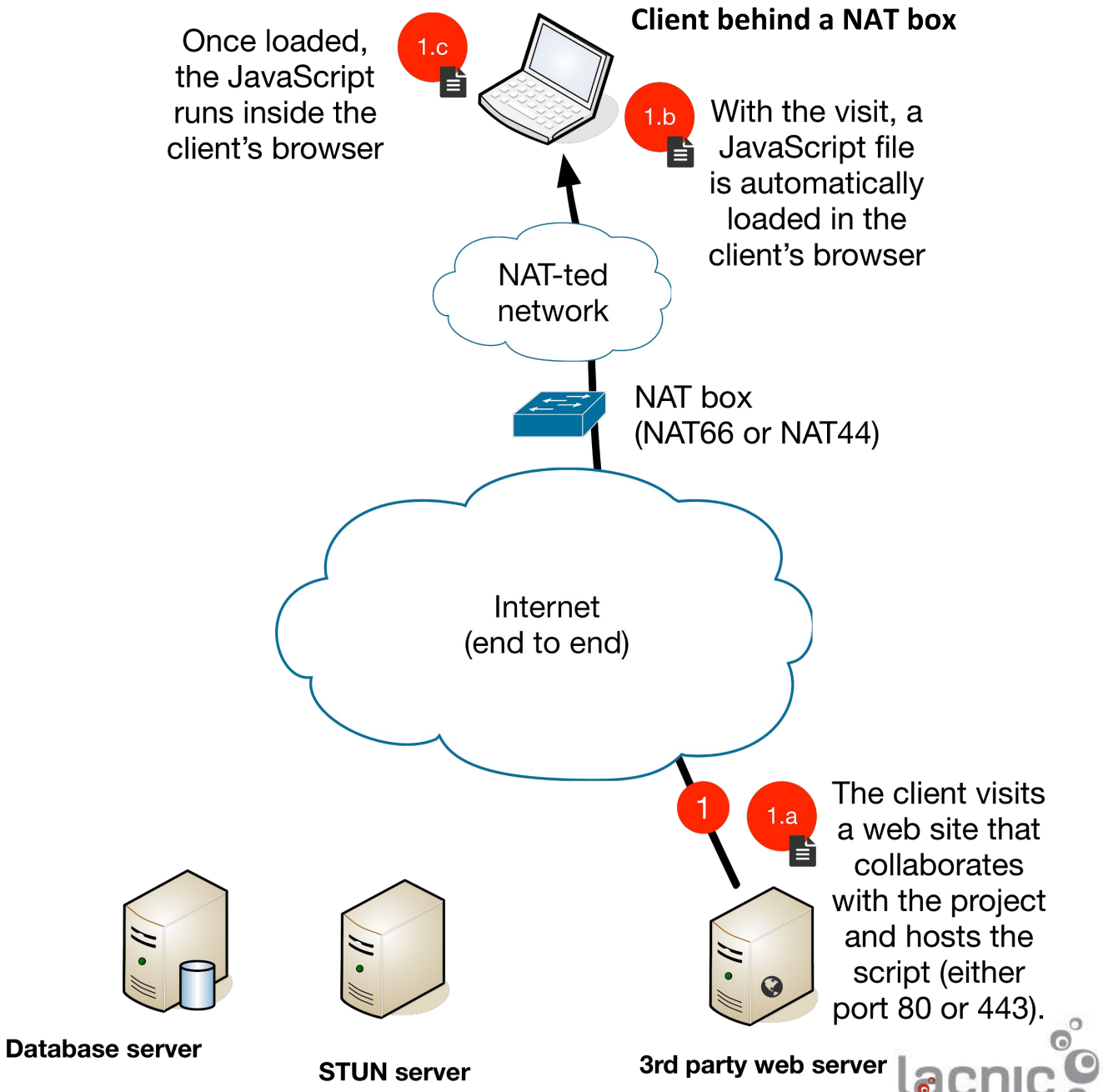
- Detectar si un navegador se encuentra detrás de un equipo que haga NAT/PAT. ¿Se puede?. Si, ejecutando un Código Javascript y con un poco de apoyo externo
  - Gracias a **WebRTC** que se encuentra disponible en la mayoría de los navegadores comunes. Adicionalmente soporta solicitudes stun.
    - Se obtiene la respuesta STUN al momento de crear “ RTC Peer Connection”.
    - Es completamente transparente al usuario final.

WebRTC & STUN

- **WebRTC** gratuito, de especificaciones abiertas. Utilizado por navegadores para ofrecer Comunicaciones en tiempo real (RTC) a través de APIs sencillas.
- **STUN** (Simple Traversal of UDP through NATs (Network Address Translation)) es un protocolo que asiste a dispositivos para comprender como se ven desde Internet (también soporta TCP)
  - RFC 5389 redefines the term STUN as 'Session Traversal Utilities for NAT' (voip-info.org/wiki/view/STUN)

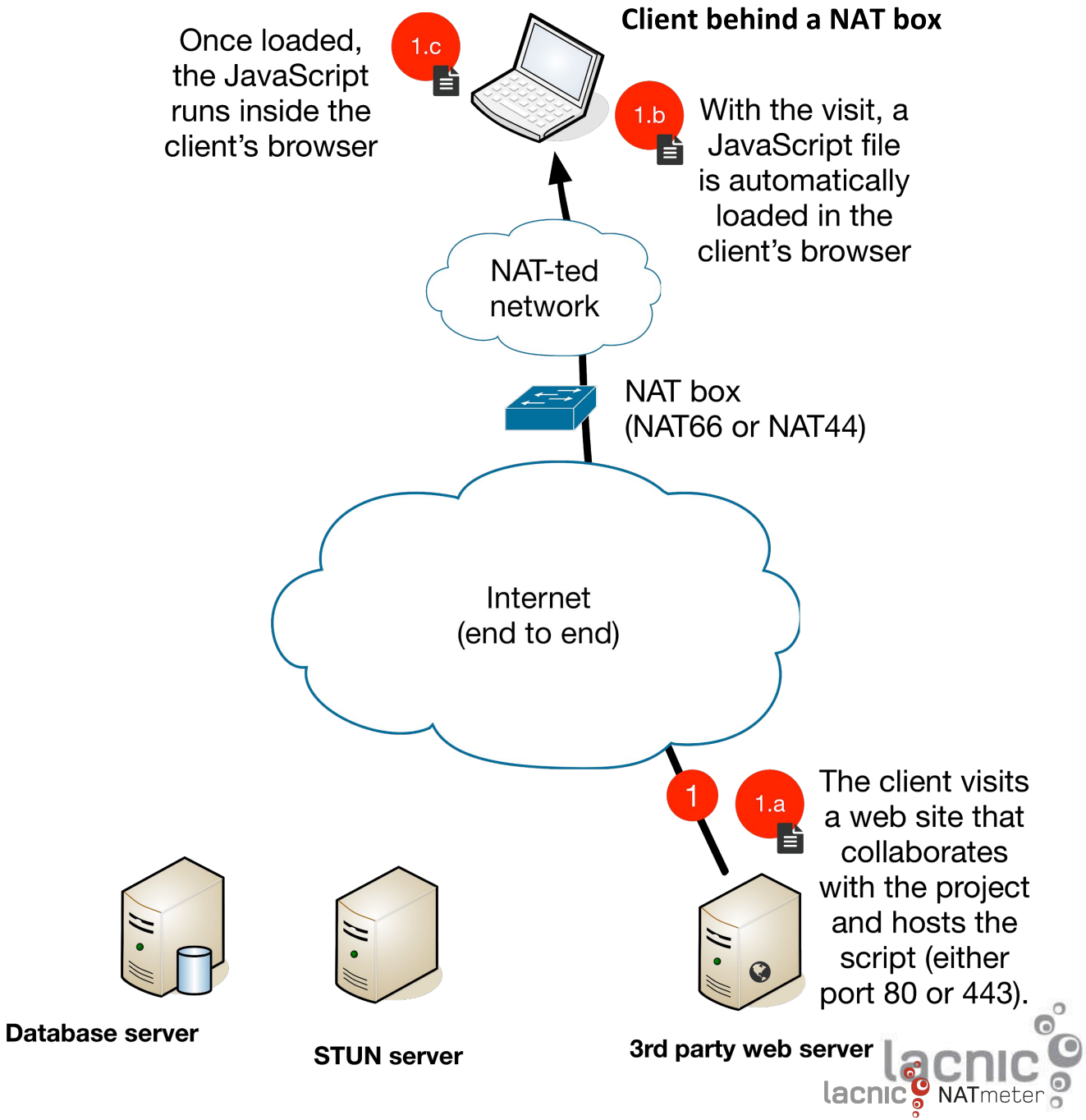
¿Cómo funciona?

1. Un código javascript se encuentra disponible en Internet
    a. Un usuario (navegador) que visite el una página que referencie al código indicado en “1”, carga el mismo y lo ejecuta.



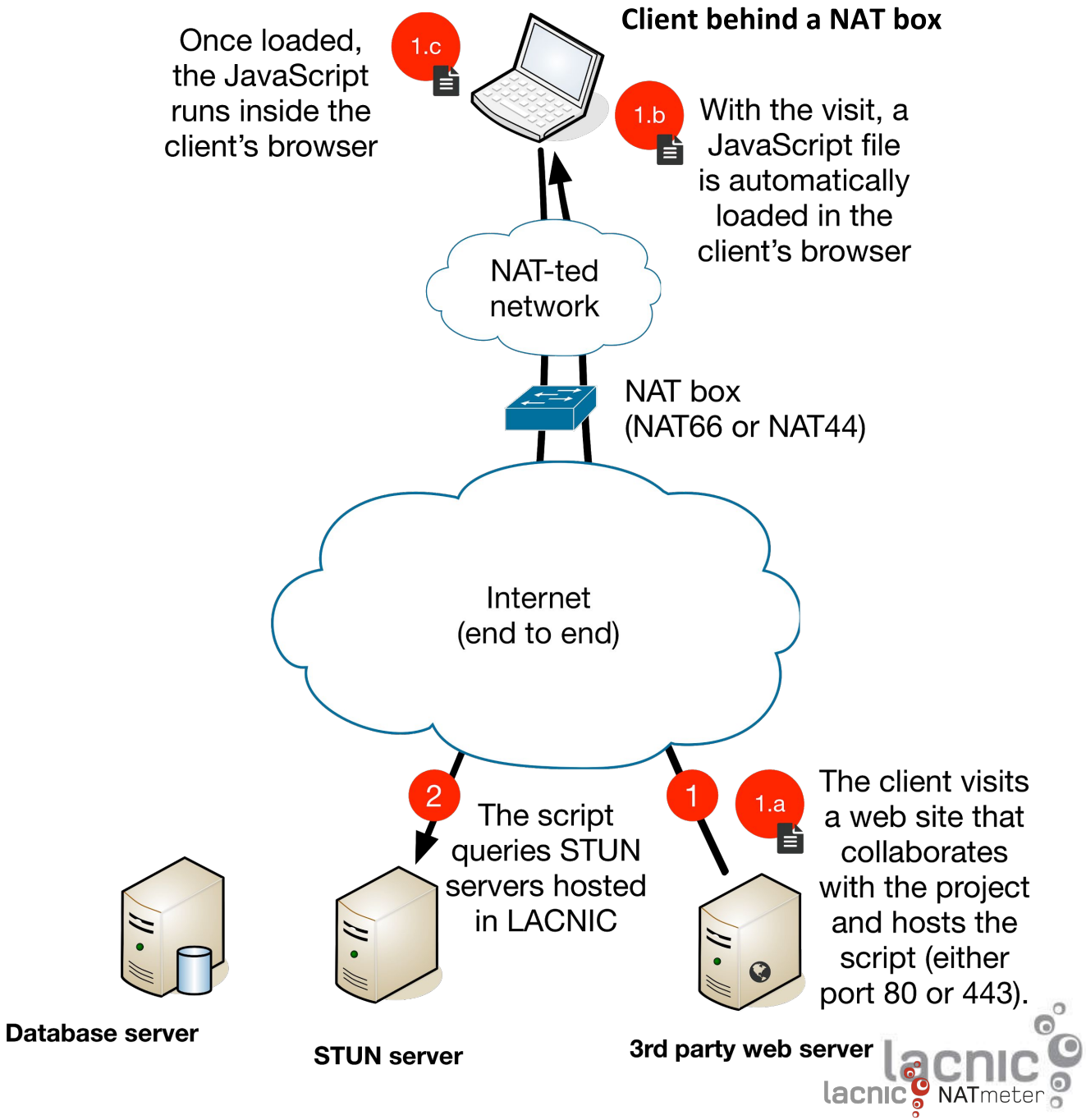
¿Cómo funciona?

1. Un código javascript se encuentra disponible en Internet
    a. Un usuario (navegador) que visite el una página que referencie al código indicado en “1”, carga el mismo y lo ejecuta.
    b. Lo ejecuta silenciosamente en backgound



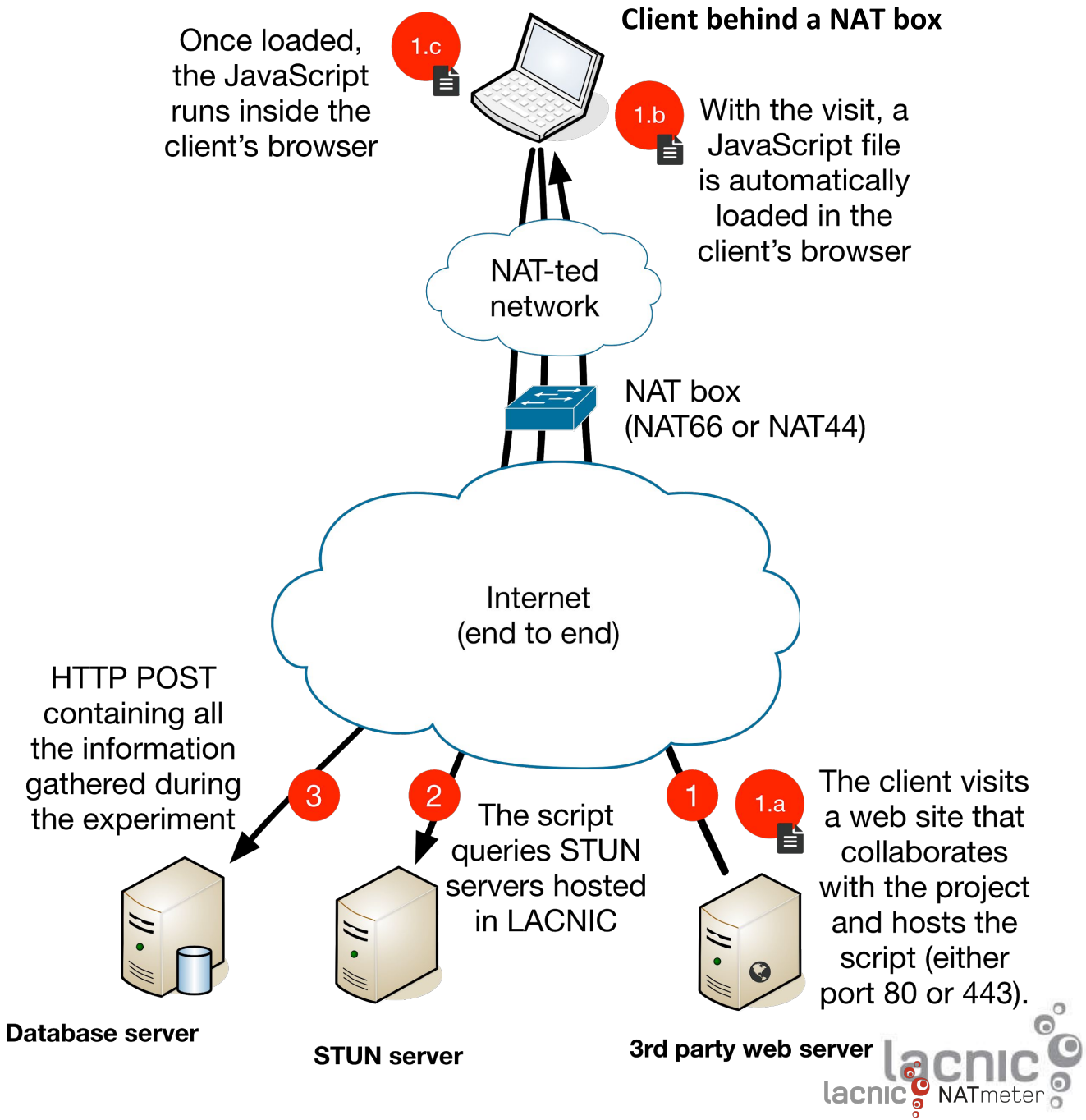
¿Cómo funciona?

1. Un código javascript se encuentra disponible en Internet
    a. Un usuario (navegador) que visite el una página que referencie al código indicado en “1”, carga el mismo y lo ejecuta.
    b. Lo ejecuta silenciosamente en backgound
2. El cliente “habla” con el STUN



¿Cómo funciona?

1. Un código javascript se encuentra disponible en Internet
    a. Un usuario (navegador) que visite el una página que referencie al código indicado en “1”, carga el mismo y lo ejecuta.
    b. Lo ejecuta silenciosamente en background
2. El cliente “habla” con el STUN
3. El cliente envía los resultados a un servidor central



Un poco más de explicación

- El script JS ejecutará al menos dos "**`new RTCPeerConnection`**" dirigidos a:
  - localhost
  - v4-only y v6-only (servidores STUN ubicados en LACNIC).
- Localhost devuelve las direcciones IP (v4 & v6) del computador que ejecuta el JS. Los STUN servers responden con la dirección IP con la cual se percibe el cliente desde Internet
  - Voila!!. Cuando la dirección IP de localhost != STUN entonces el equipo se encuentra detrás de un NAT
- Resultados son enviados a un server para colección y procesamiento

Note: Currently running Stuntman version 1.2.8 (http://www.stunprotocol.org/) on Ubuntu 13.04. Two separate servers, one for IPv4 and one for IPv6

lacnic lacnic NATmeter

Ejemplos de NAT66

```
alejandro@simon:~$ ./nat_measurements.py NAT66
('Natted IPv6 Host', ['2800:XX::2'], 'IPv6 private addresses: ', [['fd00:88aa:cafe::3']])
('Natted IPv6 Host', ['2001:XX:abdc'], 'IPv6 private addresses: ', [['fc00:XX:abcd']])
('Natted IPv6 Host', ['2a03:XX::9e'], 'IPv6 private addresses: ',
[['fdd8:a2de:468c:72::107e']])
('Natted IPv6 Host', ['2001:XX:c44c'], 'IPv6 private addresses: ', [['2001:XX:ff31']])
('Natted IPv6 Host', ['2001:XX:ce0d'], 'IPv6 private addresses: ',
[['4006:e024:680:ce0c:3435:ed62:b2a9:5f60']])
('Natted IPv6 Host', ['2001:XX:ce0d'], 'IPv6 private addresses: ',
[['4006:e024:680:ce0c:3435:ed62:b2a9:5f60']])
('Natted IPv6 Host', ['2001:XX:3ad5'], 'IPv6 private addresses: ', [['2001:XX:3ad5']])
('Natted IPv6 Host', ['2001:XX:8678'], 'IPv6 private addresses: ', [['2001:XX:fe99']])
('Natted IPv6 Host', ['2001:XX:77d8'], 'IPv6 private addresses: ', [['2001:XX:fedc']])
('Natted IPv6 Host', ['2001:XX:1005'], 'IPv6 private addresses: ', [['2001:XX:fffb']])
```

Ejemplos de NAT44

```
alejandro@simon:~$ ./nat_measurements.py NAT44
('Natted IPv4 Host', [['172.16.29.52']], 'public', [['196.XX.114']])
('Natted IPv4 Host', [['10.200.41.45']], 'public', [['200.XX.253']])
('Natted IPv4 Host', [['10.181.28.199']], 'public', [['201.XX.37']])
('Natted IPv4 Host', [['10.0.80.227']], 'public', [['208.XX.64']])
('Natted IPv4 Host', [['192.168.177.1'], ['192.168.224.1'], ['192.168.0.11']], 'public',
[['186.XX.95']])
```

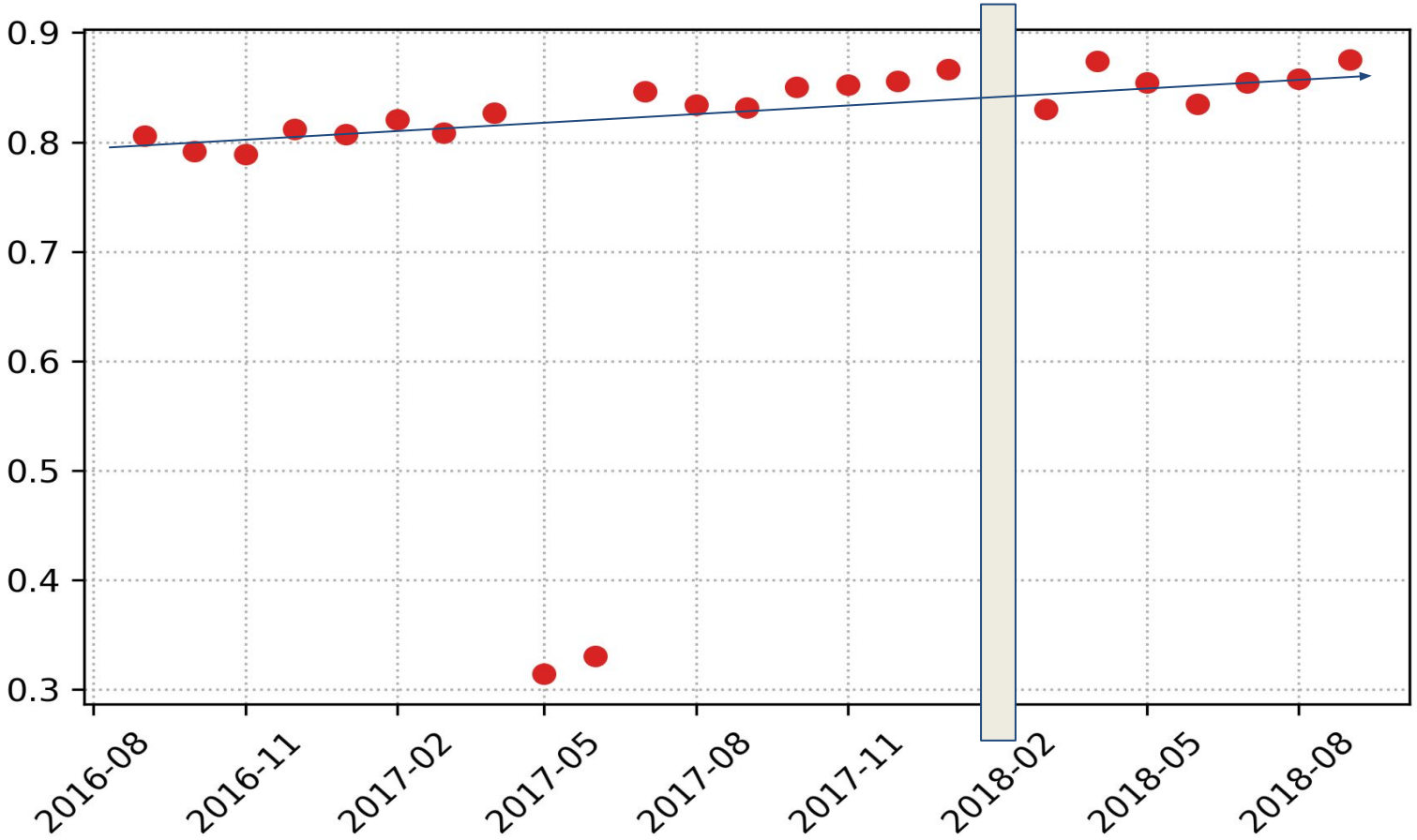
Revisemos con detalle NAT66 (¡¡por diversion !)

- Pareciera que hay una tendencia de utilizar direcciones “privadas” en IPv6 ULA. Pensamos que eso está bien! (ojo, no nos gusta el NAT, pero bueno)
- Existe uso de direcciones IPv6 no asignadas como privadas. Uff, no aprendimos nada de IPv4: *'4006:e024:680:ce0c:3435:ed62:b2a9:5f60’, ¡no está bien!*
- Conseguimos casos interesantes de NAT donde la “privada” y la “nateada” pertenecen al mismo /64

Algunos resultados

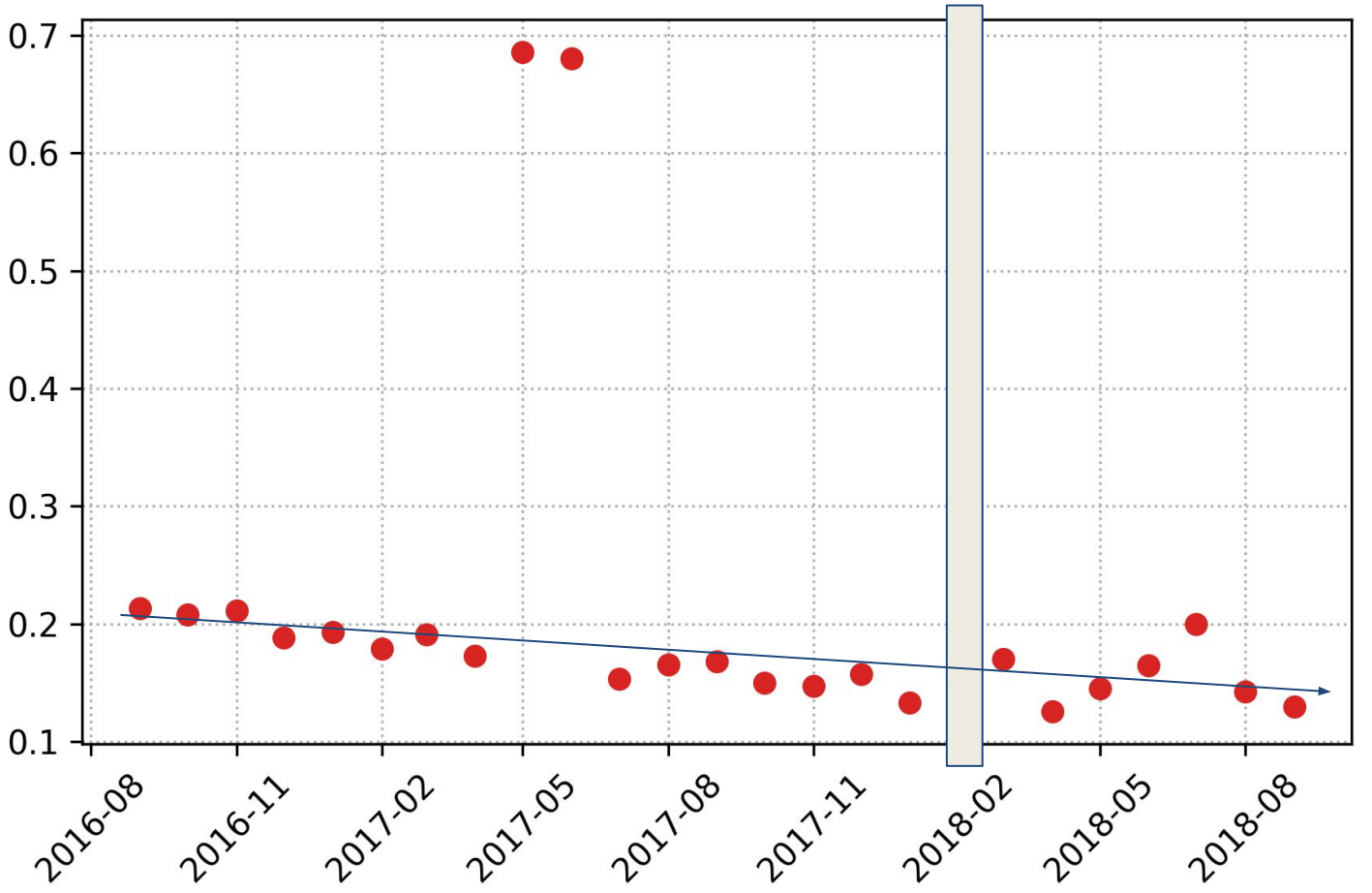
lacnic
lacnic NATmeter

NAT 44



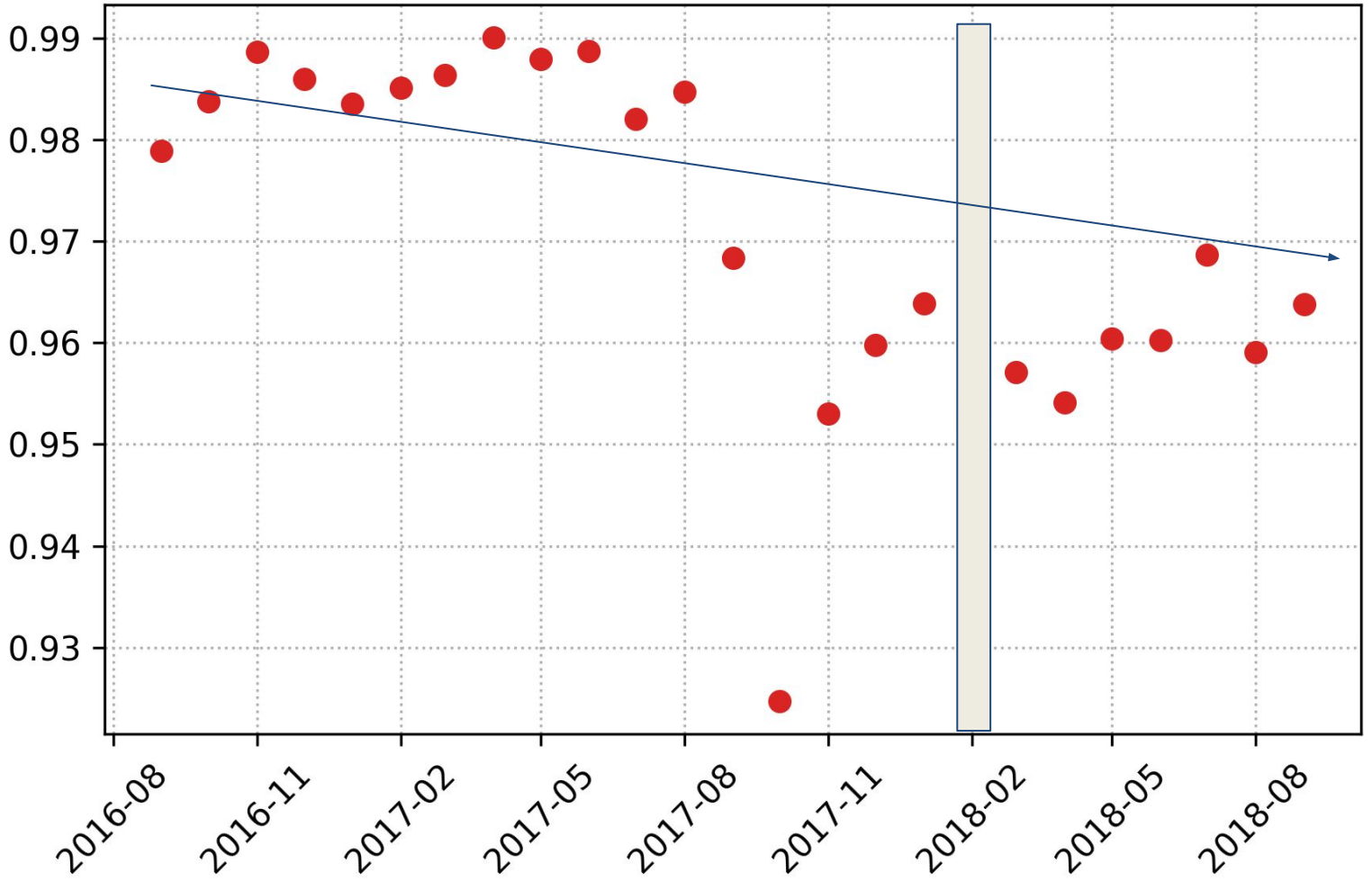
lacnic NATmeter

No-NAT 44



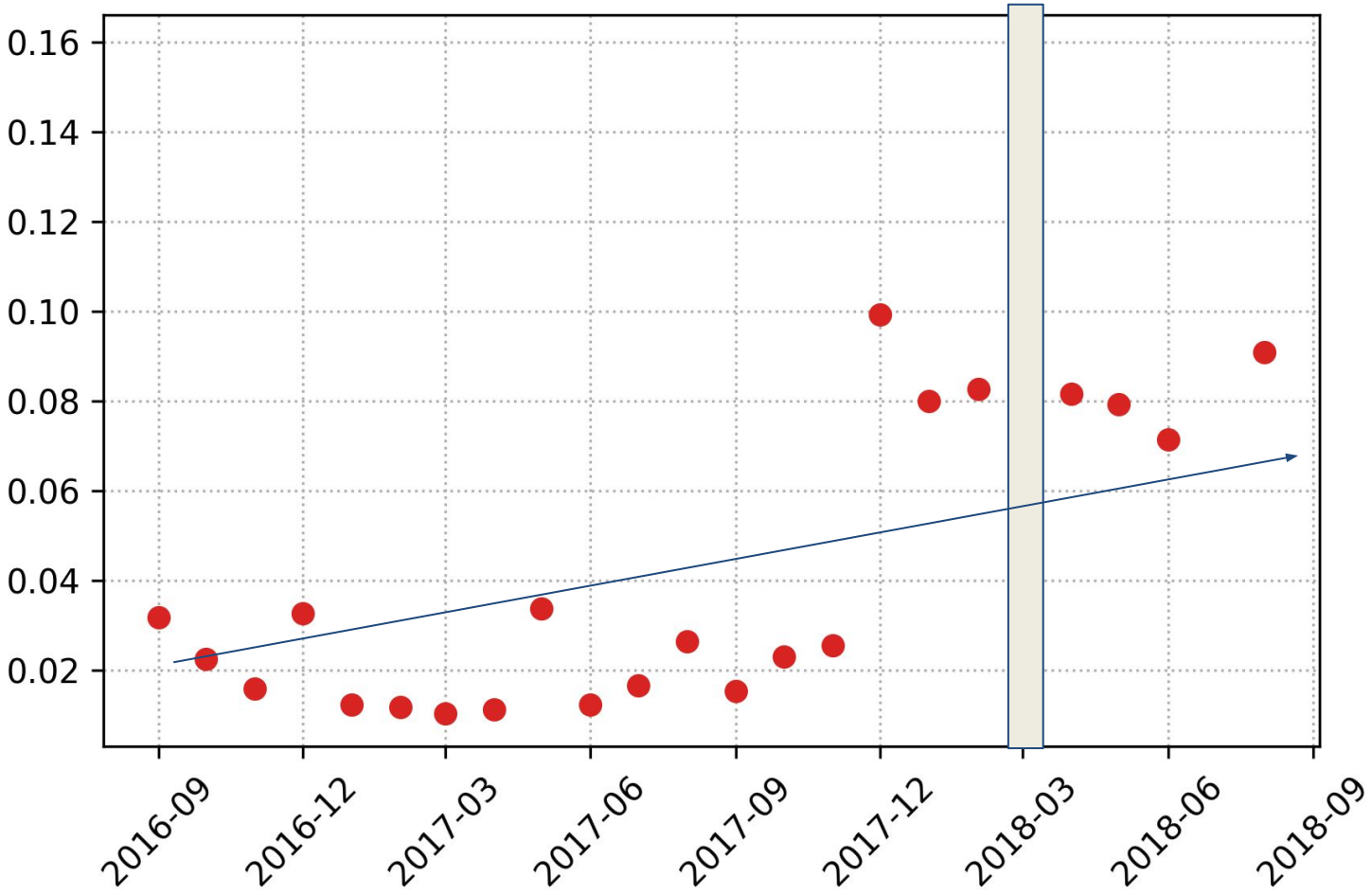
lacnic
lacnic NATmeter

Hosts v4 only



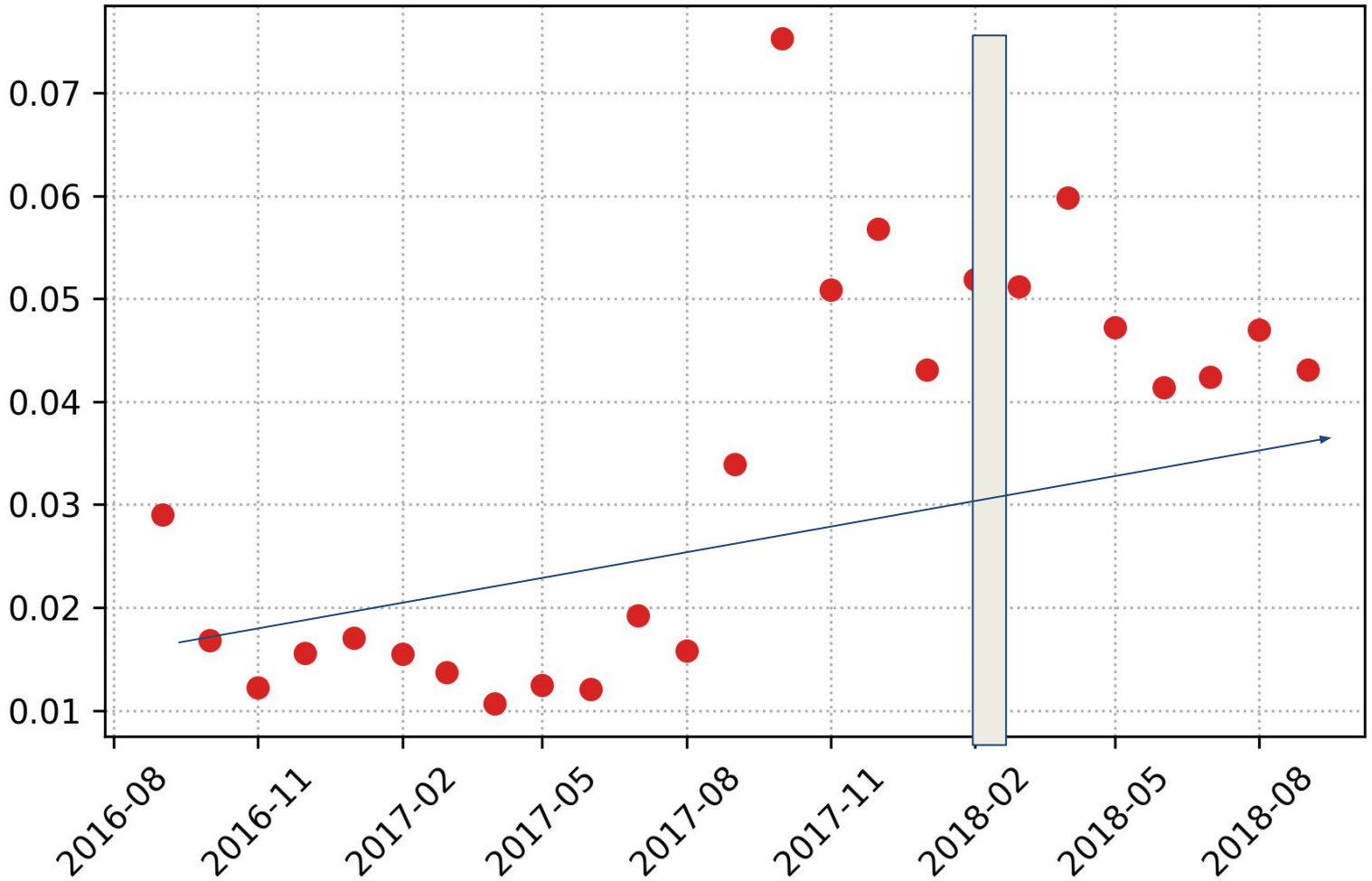
lacnic
lacnic NATmeter

NAT 66



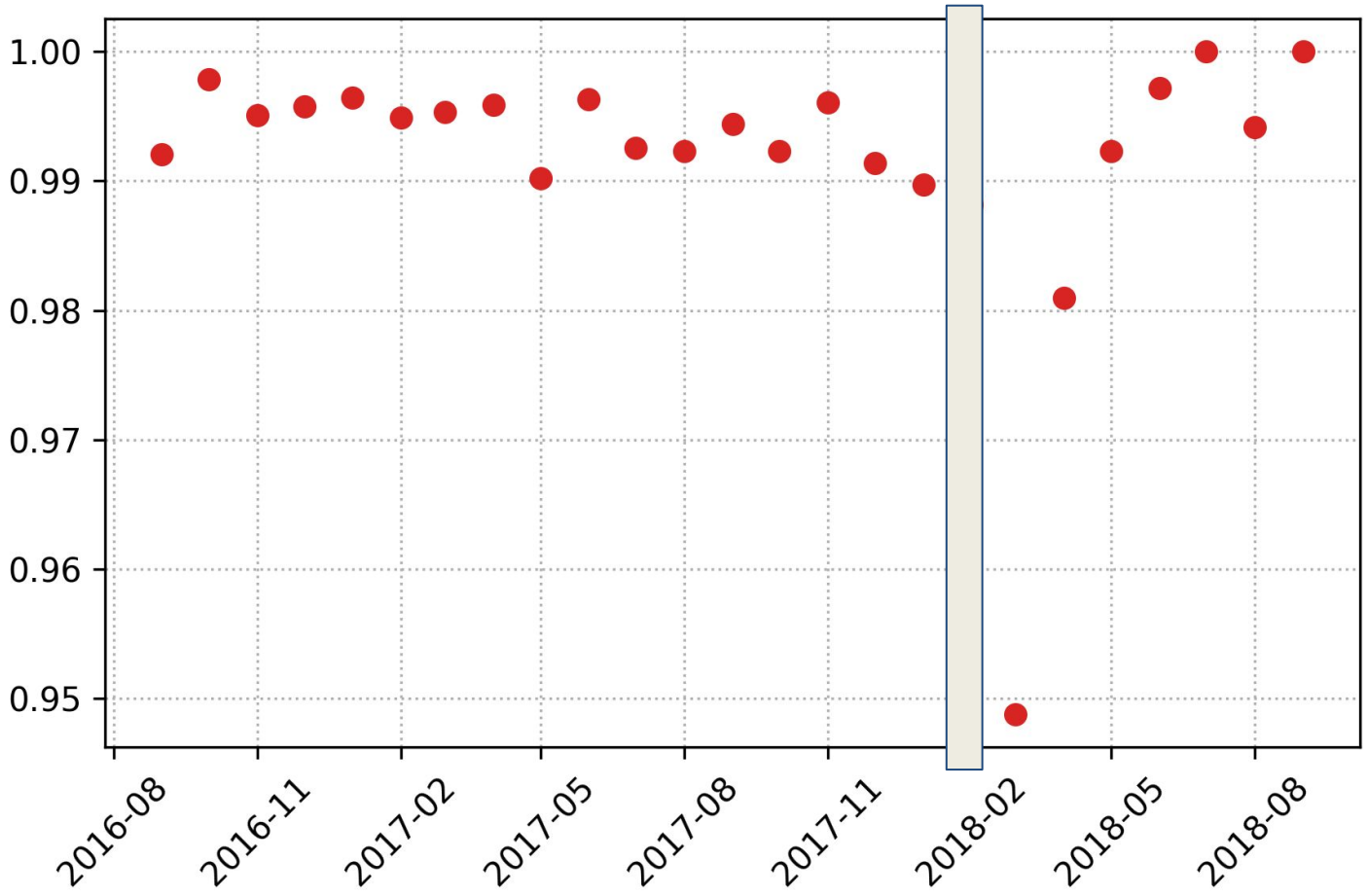
0.16
0.14
0.12
0.10
0.08
0.06
0.04
0.02
2016-09
2016-12
2017-03
2017-06
2017-09
2017-12
2018-03
2018-06
2018-09

Hosts v6-only



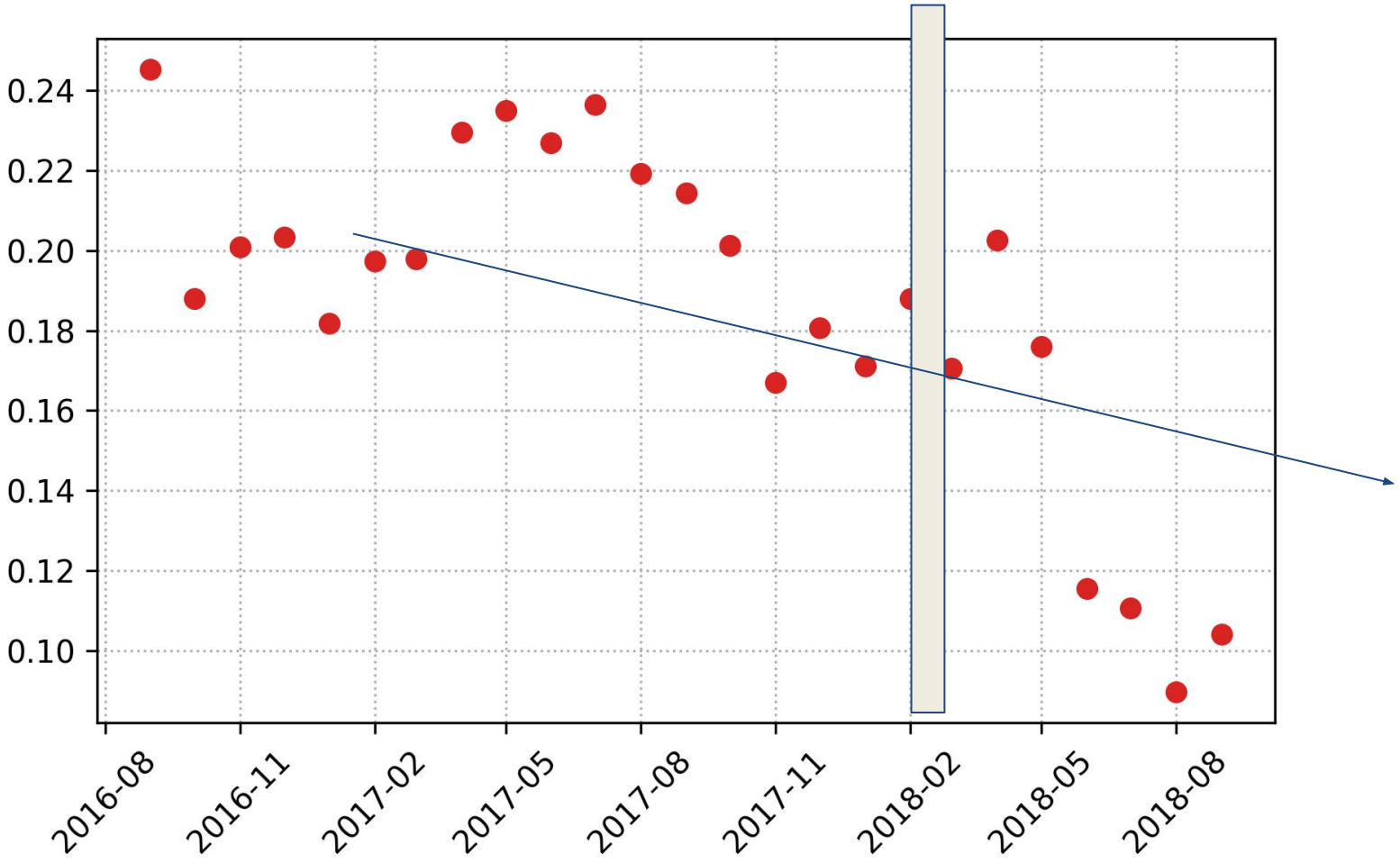
lacnic
lacnic NATmeter

No-NAT 66



lacnic
lacnic NATmeter

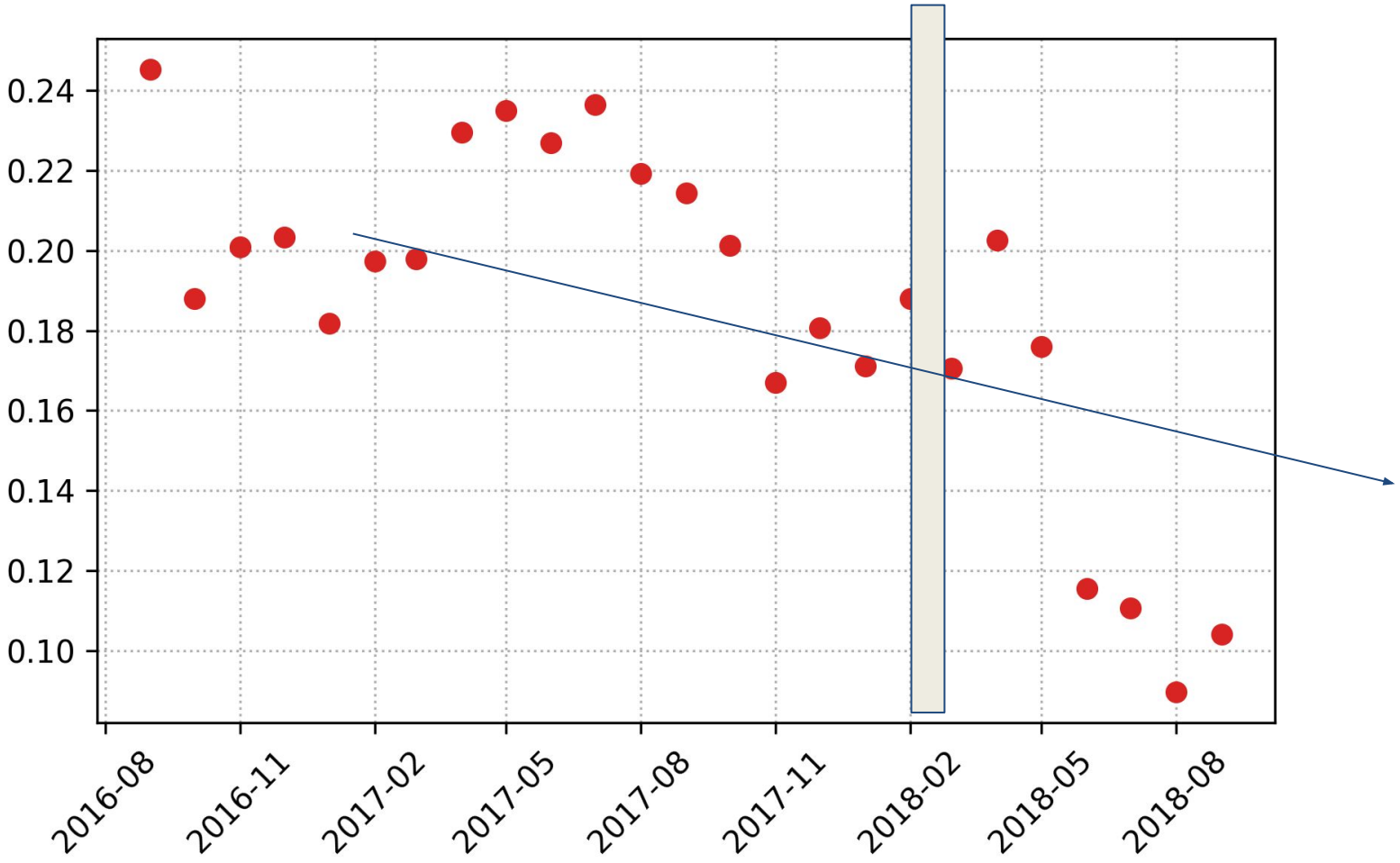
Dualstack hosts



¿Tiene sentido?

lacnic NATmeter

Dualstack hosts



¿Tiene sentido?

Quizás porque IPv6-Only hosts se ha incrementado

lacnic NATmeter

Network Prefix Translation

https://tools.ietf.org/html/rfc6296

lacnic
lacnic NATmeter

Network Prefix Translation

```
Host Nateado NAT66 y con NPT ['200                    5e:38c5:b7b:c40e'] ['2                    5e:38c5:b7b:c40e']
Host Nateado NAT66 y con NPT ['fe80::2834:3b20:4cce:fc0d'] ['200                :2834:3b20:4cce:fc0d']
Host Nateado NAT66 y con NPT ['20                ::6666'] ['26                ::6666']
Host Nateado NAT66 y con NPT ['fe80::37:1885:408e:b9e'] ['200                :37:1885:408e:b9e']
```

https://tools.ietf.org/html/rfc6296

lacnic NATmeter

Pasemos a medir CGN

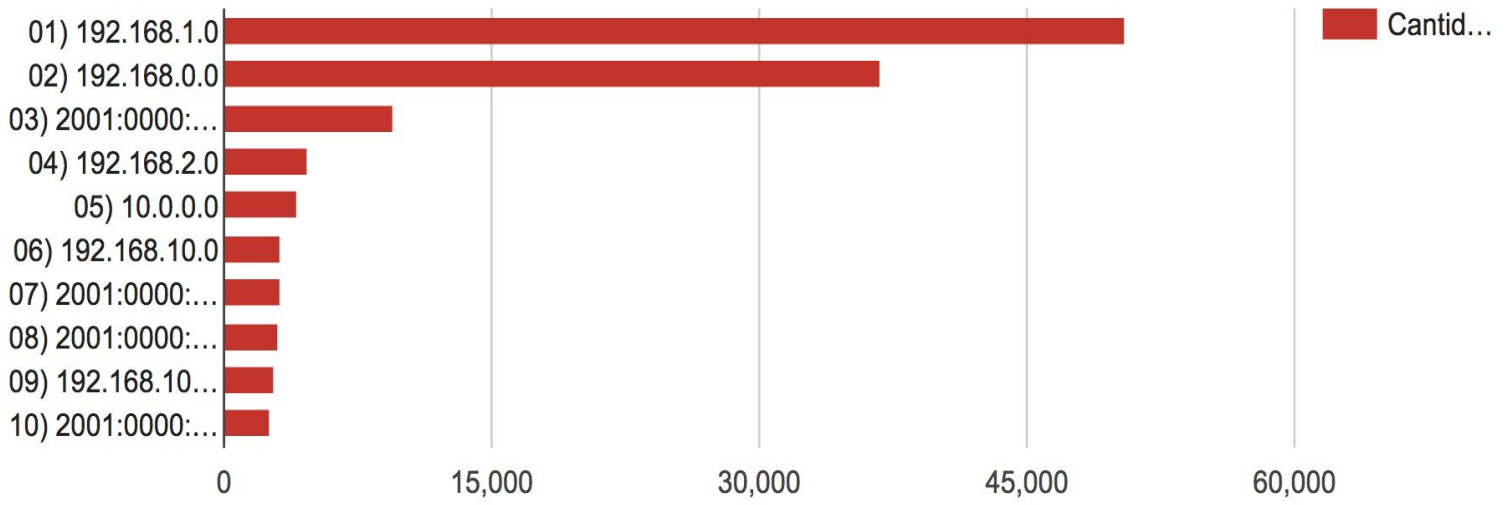
lacnic NATmeter

Algunos resultados sumarizados

	LAC region	All results
Measurements behind NAT	83.6%	73.4%
Measurements behind NAT 44	82.5%	73.4%
Measurements behind NAT 66	0.2%	0.1%
Measurements through NPT (v6)	0%	0%
Clients behind NAT		50%

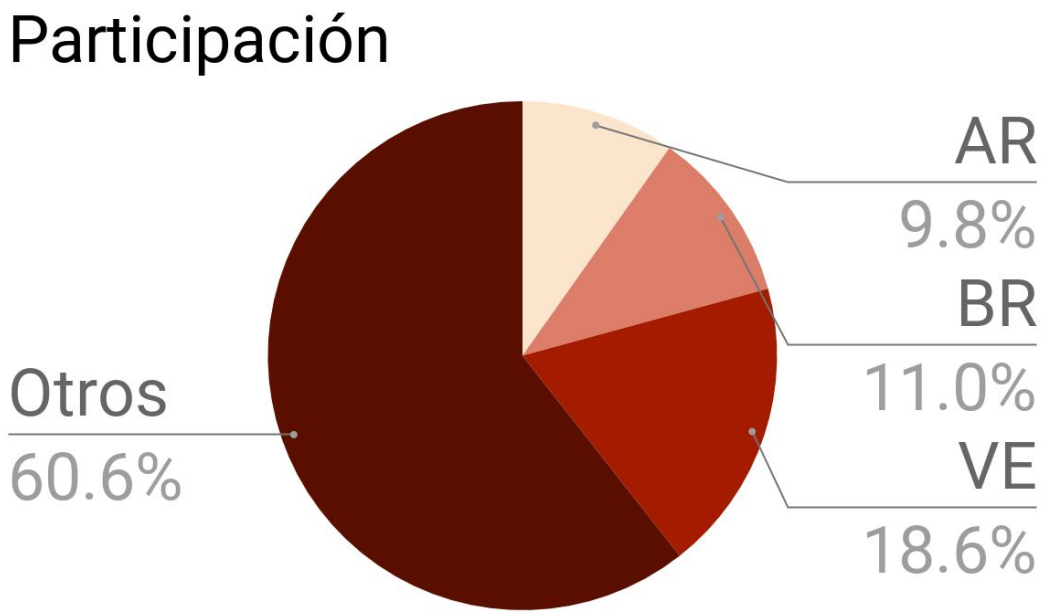
lacnic NATmeter

¿Que direcciones IP “privadas” utilizan los hosts?



lacnic NATmeter

Participación por país



lacnic
lacnic NATmeter

CGN (1/3)

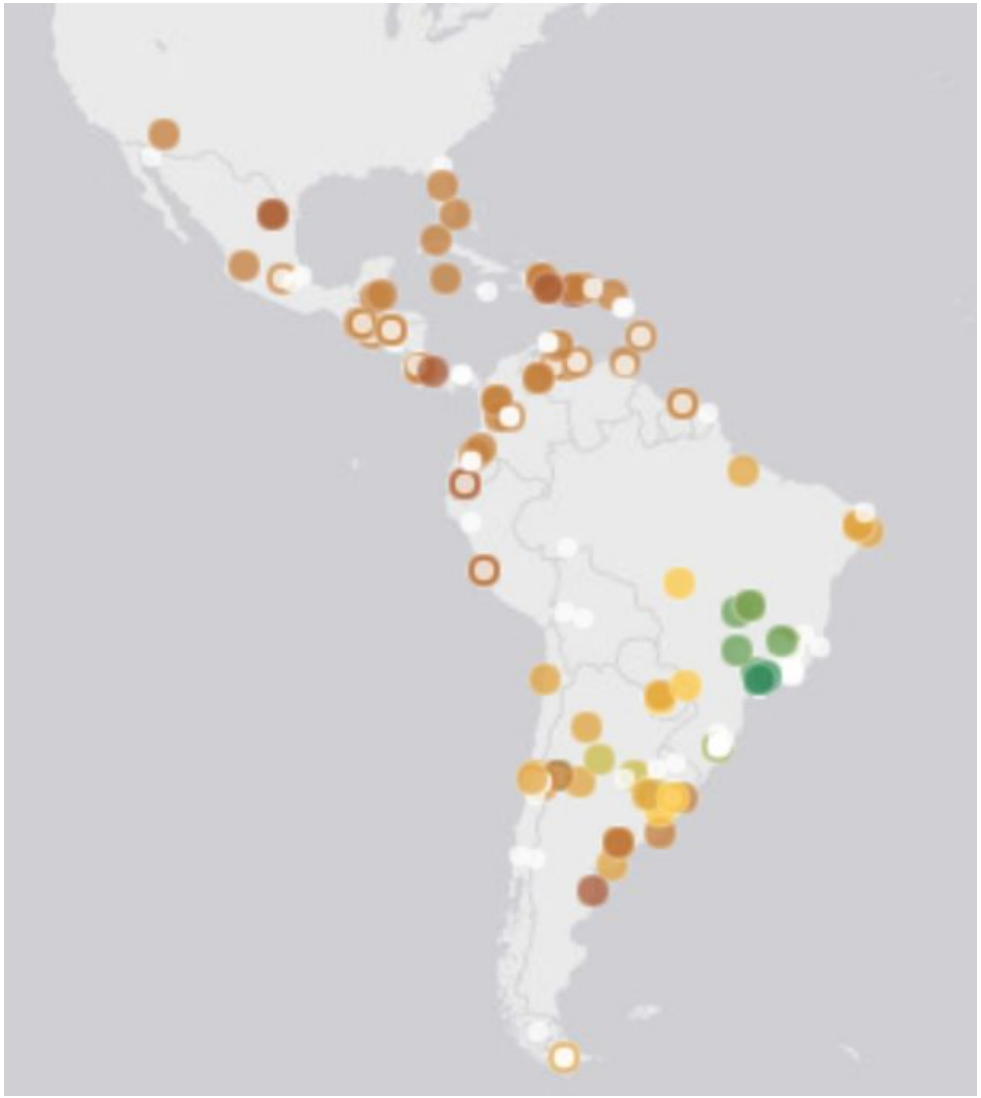
CGN detection experiment

General Information | Probes | Map | LatencyMON | TraceMON | IPmap (beta) | Results

Type	Traceroute
Public measurement?	Yes
Target	www.lacnic.net
Resolve on Probe	No
Interval / spread	Every 86400 seconds / default spread
Timing	2017-02-14 15:05 - 2017-11-16 01:50
Costs	30 per result, 7380 per day
Response timeout	4000
First hop	1
Paris	16
Packets	3
Protocol:icmp	True
Max hops	32

lacnic NATmeter

CGN (2/3)



CGN detection experiment

General Information | Probes | Map | LatencyMON | TraceMON | IPmap (beta) | Time Travel

Results

Probe	ASN (IPv4)	ASN (IPv6)	Time (UTC)	RTT	Hops	Success
51	7418		2017-11-15 10:14	77.704	16	✔
100	28017		2017-11-16 00:47	165.880	14	✔
132	27699	27699	2017-11-15 15:00	4.345	11	✔
243	10318		2017-11-16 00:47	48.914	16	✔
342	28000	28000				No recent report available
390	27678	27678	2017-11-15 14:18	51.085	9	✔
863	6057					No recent report available
927	6057		2017-11-15 14:18	47.124	16	✔
1117	6057	6057				No recent report available
1170	10481		2017-11-15 14:18	40.193	19	✔
1174	13489		2017-11-15 12:49	158.707	17	✔
1190	27699		2017-11-16 00:47	32.628	11	✔
2712	22047					No recent report available

lacnic NATmeter

CGN (3/3) --- ¿En qué consiste?

Búsqueda del prefijo 100.64.0.0/10 en las respuestas de un traceroute como se encuentra especificado en el RFC 6598

https://tools.ietf.org/html/rfc6598

lacnic
lacnic NATmeter

Que conseguimos en el experimento de CGN

lacnic
lacnic NATmeter

Que conseguimos en el experimiento de CGN

3% de
operadores con
CGN

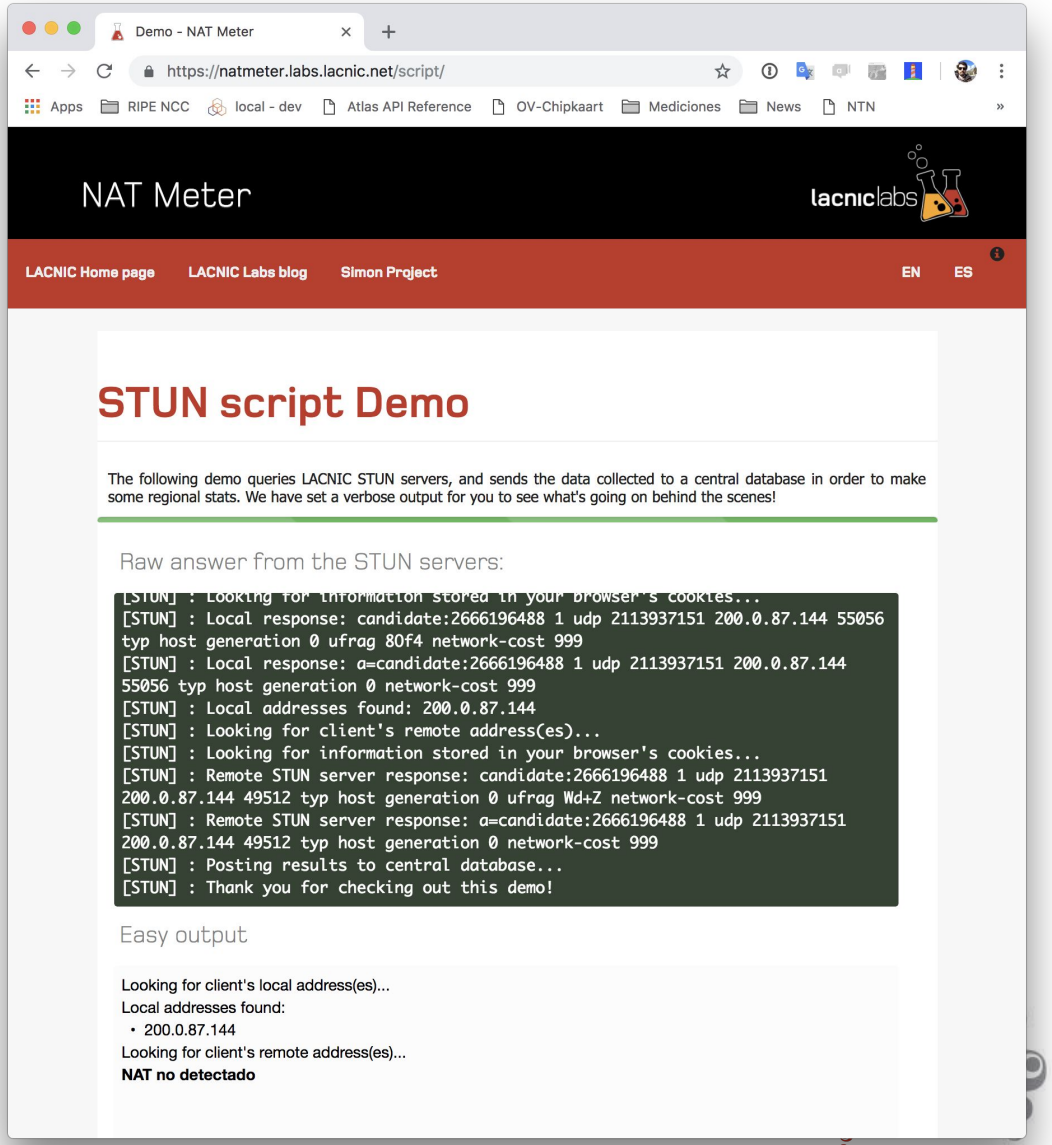
lacnic
lacnic NATmeter

Unas notas finales

- Los datos
  - Colectados parcialmente apoyado con visitantes de www.lacnic.net y otros blogs regionales
  - Tenemos algunos filtros de redes: por ejemplo, prefijos de la casa de Internet.
  - La recolección de datos comenzó el 9 de Septiembre de 2016. Aún continúa
  - Actualmente, aproximadamente 50 K registros
  - www.lacnic.net utilizado hasta Diciembre 2017
- Geolocation
  - Using Maxmind
- Code at github.com/LACNIC/natmeter, based on github.com/diafygi/webrtc-ips

https://natmeter.labs.lacnic.net/script/

- Funciona 100% en Chrome
- ¿Quieres contribuir?
  - Acércate a nosotros [1] y conversamos sobre colocar el script en tu sitio



[1] alejandro @ lacnic.net

Thanks! Questions?

natmeter.labs.lacnic.net

lacnic

www.lacnic.net