RIPE NCC
RIPE NETWORK COORDINATION CENTRE

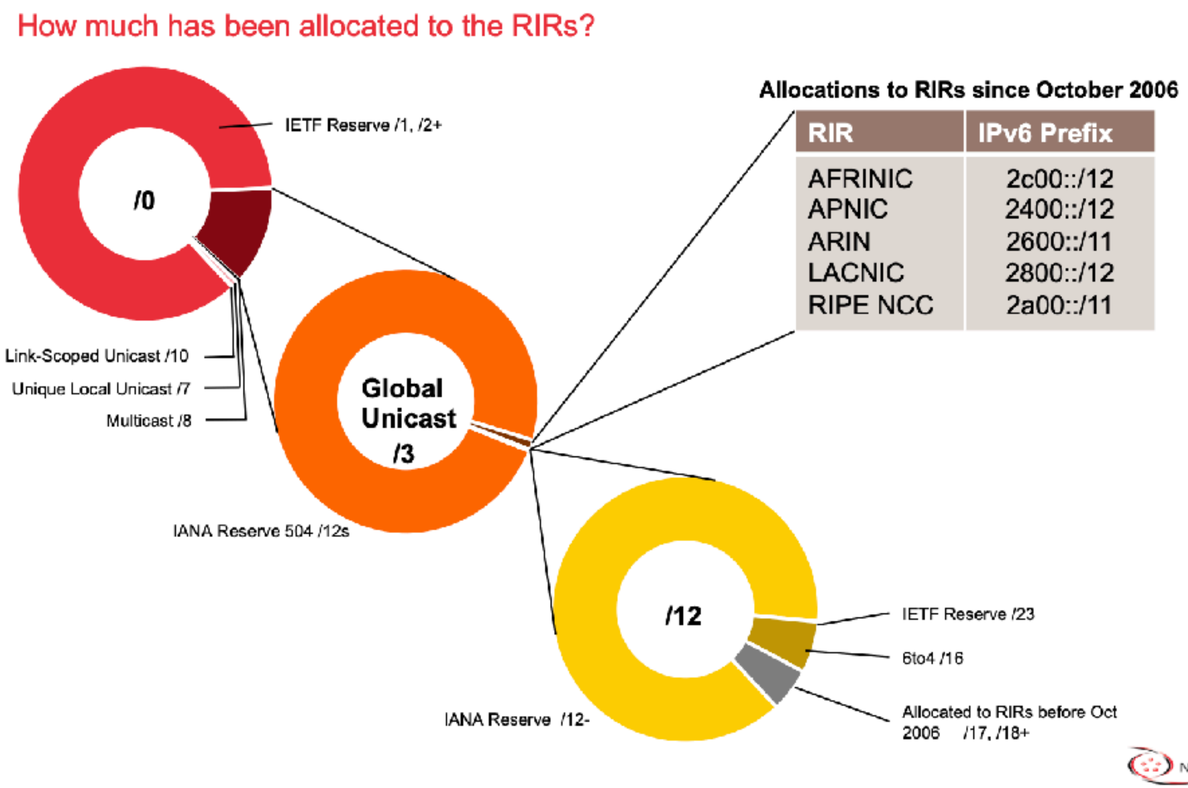
De-bogonizando 2a10::/12

Analizando la primera semana de un /12

Stephen D. Strowes, Emile Aben, Rene Wilhelm,
Florian Obser, Riccardo Stagni, Agustin Formoso

RIRs y asignaciones de recursos

- Nueva asignación IANA → RIPE NCC
  - `2a10::/12`
- ¿Por qué este momento es especial?
  - Nueva asignación IPv6 a un RIR desde 2006
  - Aún sin uso
  - *Bogon (Wikipedia)*



Motivación

- ¿Qué tan apto es el 2a10::/12 para ser utilizado por miembros de RIPE NCC? (RIPE Labs)
- ¿Podemos medir la usabilidad de este nuevo bloque?
  - *Captura de paquetes*
  - RIPE RIS
  - RIPE Atlas

RIPE RIS

- ris.ripe.net - Routing Information System
- Observatorio de rutas
  - Colectores: reciben tablas de sus peers
  - Peers: participan del proyecto para ofrecer visibilidad
- RRC24 @ LACNIC
  - Participar de RIS
- **¿Cómo vemos el `2a10::/12` desde RIS?**

RIPE Atlas

- atlas.ripe.net
- Red global de sondas
- +11000 sondas conectadas
- Permiten lanzar pings y traceroutes, entre otras mediciones
- **¿Qué sondas tienen conectividad con el `2a10::/12`?**

RIPE Atlas

- Sondas de software
  - Es un paquete de software que funciona igual que las sondas físicas.
  - Instala y corre en tus máquinas virtuales, router doméstico, servidores, etc.
  - Soporta CentOS 7 y 8; Debian (9 y 10) y Raspbian; Docker; Turris Routers
  - Más información
  - Aplicar a un software probe (requiere cuenta de RIPE Access)

Experiencias pasadas

- 2006 - Matt Ford: /48, 15 meses, 12 paquetes
- 2010 - Geoff Huston: /12, 9 días, 21k paquetes
- 2012 - Merit (y RIPE 66): 5 /12s ~100 pps, visibilidad mixta
- Trabajos realizados en los inicios de IPv6
- Poco tráfico era de esperarse
- ¿Con qué nos podemos encontrar en 2020?

Datos IPv6 de Google

El experimento

- Anuncios desde el RRC03 de RIS
- `2a10::/12`
- Prefijos `/32` y `/48`
  - Configuración IRR y ROA

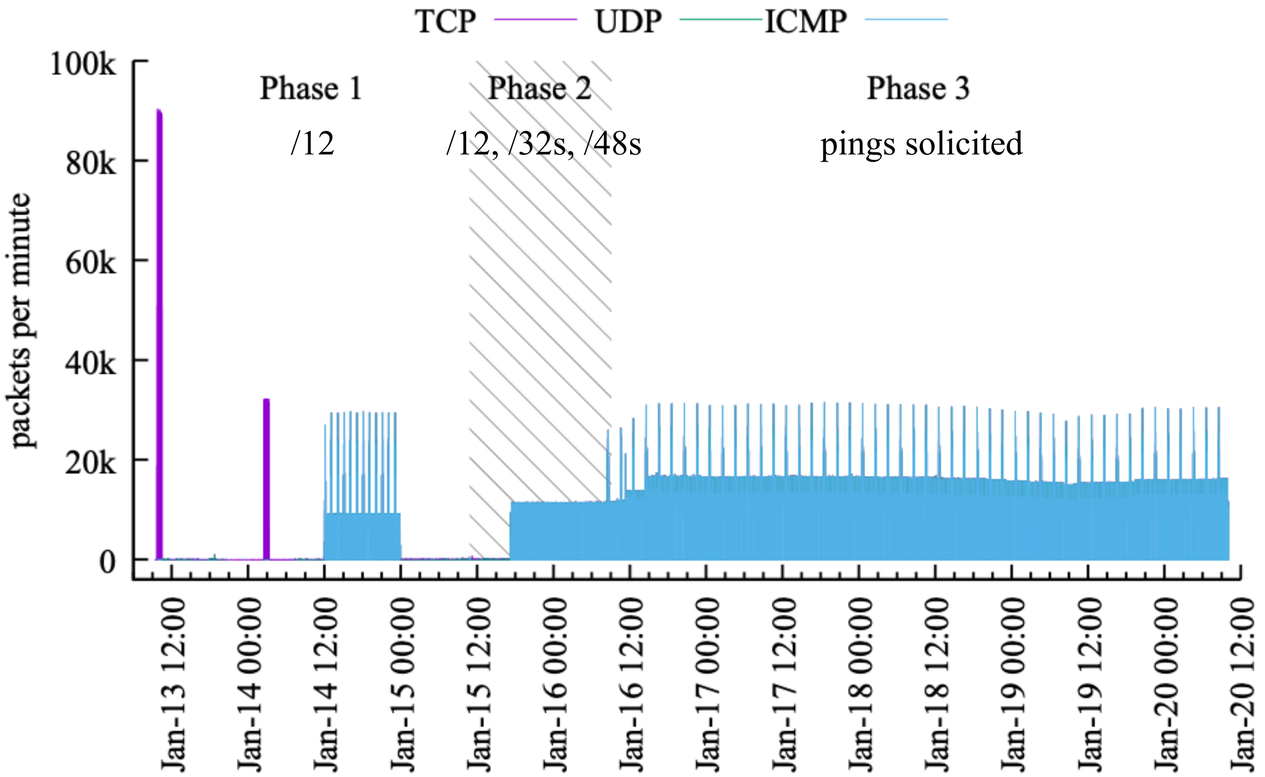
/32		ROA	
		✔	✘
IRR	✔	2a10:4::/32	2a10:6::/32
	✘	2a10:5::/32	2a10:7::/32

/48		ROA	
		✔	✘
IRR	✔	2a10:3:4::/48	2a10:3:6::/48
	✘	2a10:3:5::/48	2a10:3:7::/48

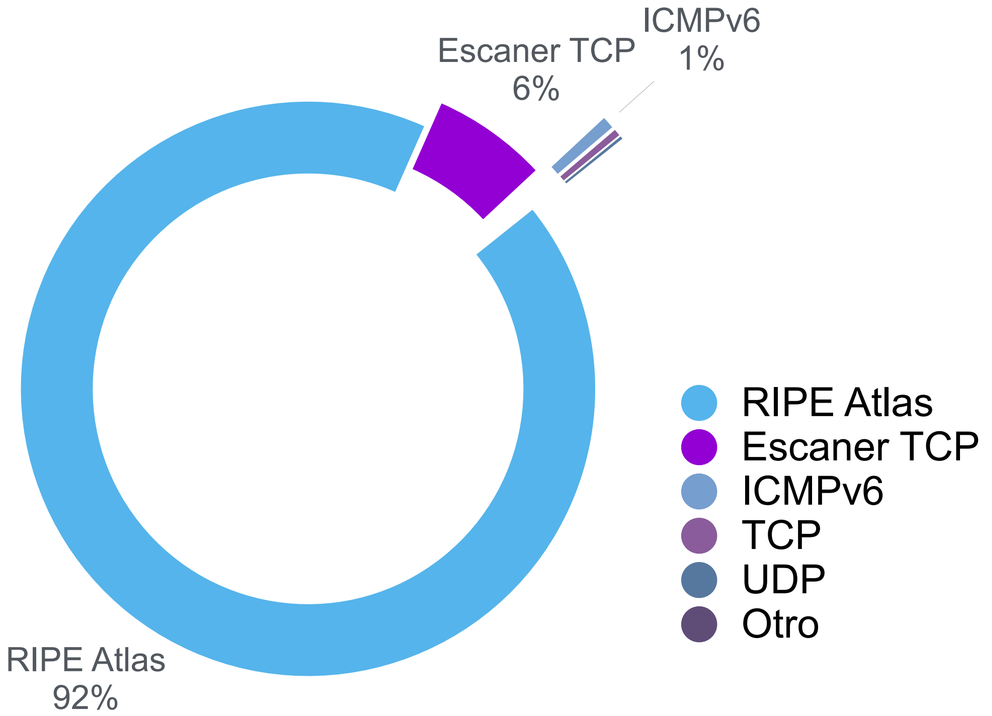
El experimento

- 1 semana (13 al 20 enero 2020)
- Eventos
  - Se crean hosts respondiendo en 8 direcciones ::1
  - Inicio de captura de paquetes (entrante al `/12`)
  - Anuncio del `/12` — Fase 1
  - Anuncio de más específicos `/32` y `/48` — Fase 2
  - Inicio de mediciones de RIPE Atlas (ping + traceroute) — Fase 2
  - Anuncio a listas de operadores — Fase 3
  - Withdrawal de todos los prefijos
  - Fin de las mediciones y período de cuarentena

Captura de paquetes



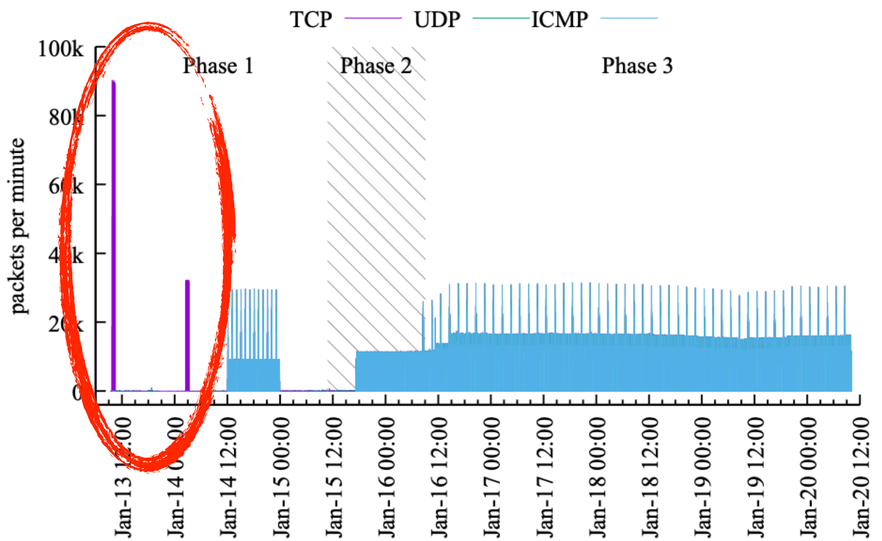
Paquetes por minuto capturados durante la duración del experimento

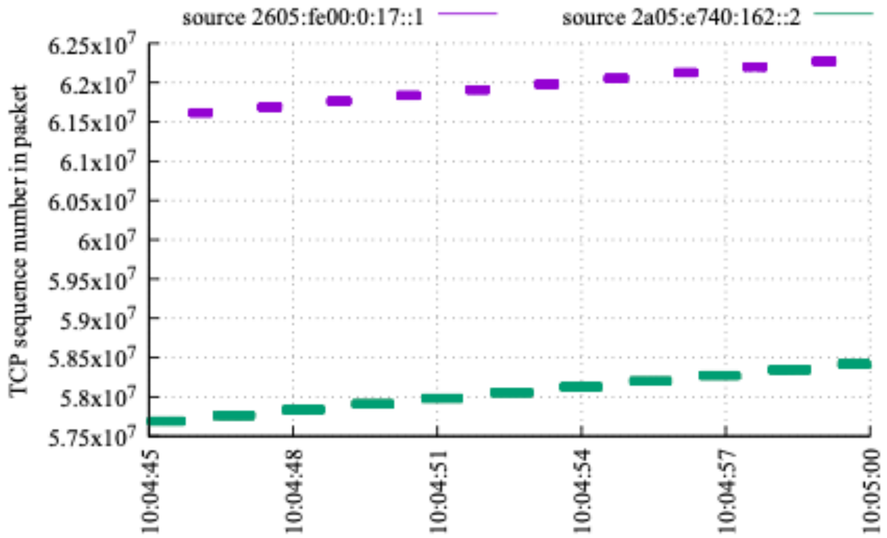


Porcentaje de paquetes capturados según fuente

Captura de paquetes

- Escaner TCP
  - Sólo SYN flag
  - src=49152 dst=80
  - Números de sequencia en batches
- Orígenes
  - Coordinado desde dos orígenes:
    `2a05:e740:162::2` (AS 39063)
    `2605:fe00:0:17::1` (AS 23033)
  - Cada `/64` se toca una única vez



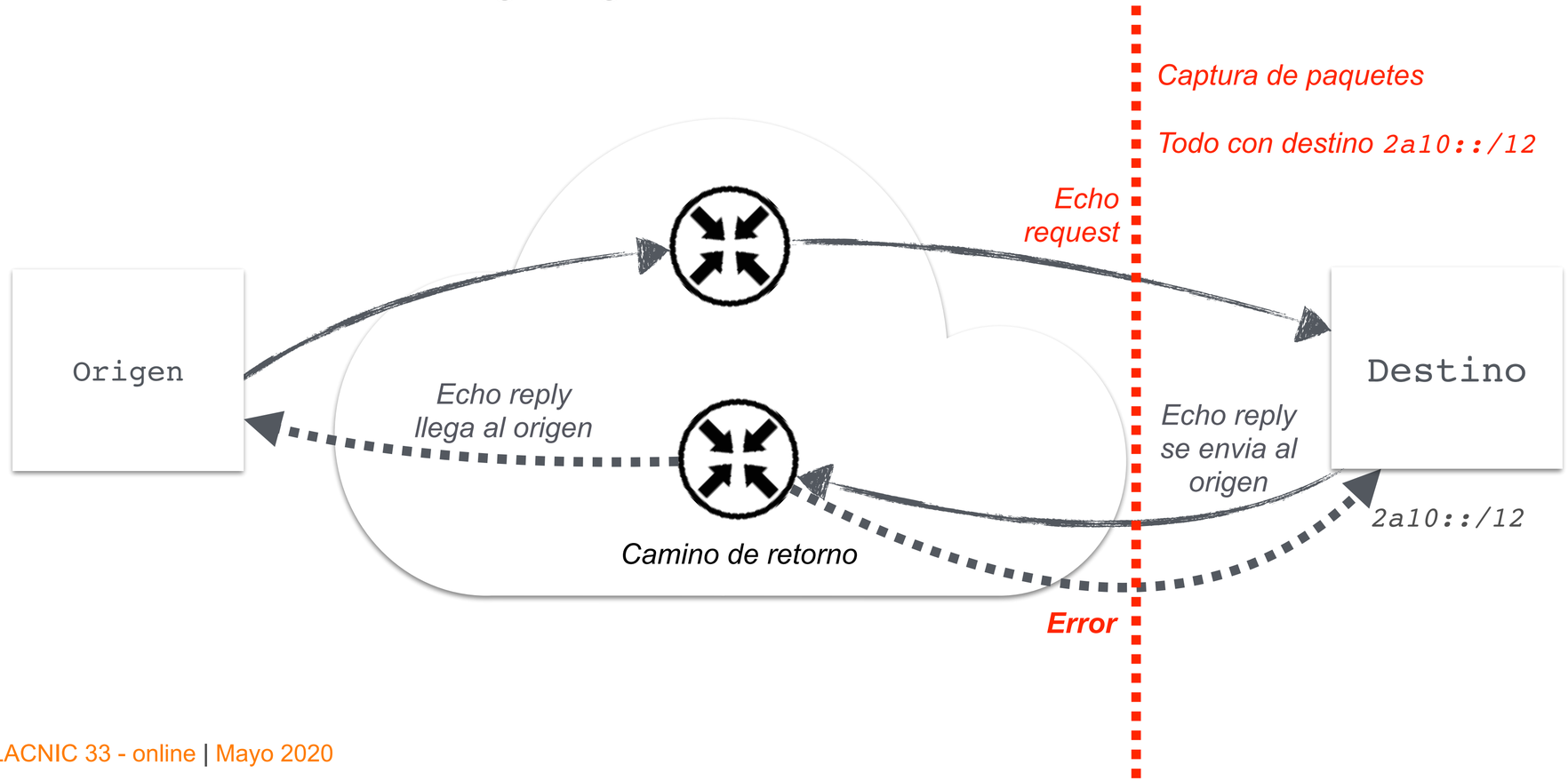


2^{52} `/64`s en un `/12`

"quadrillions"

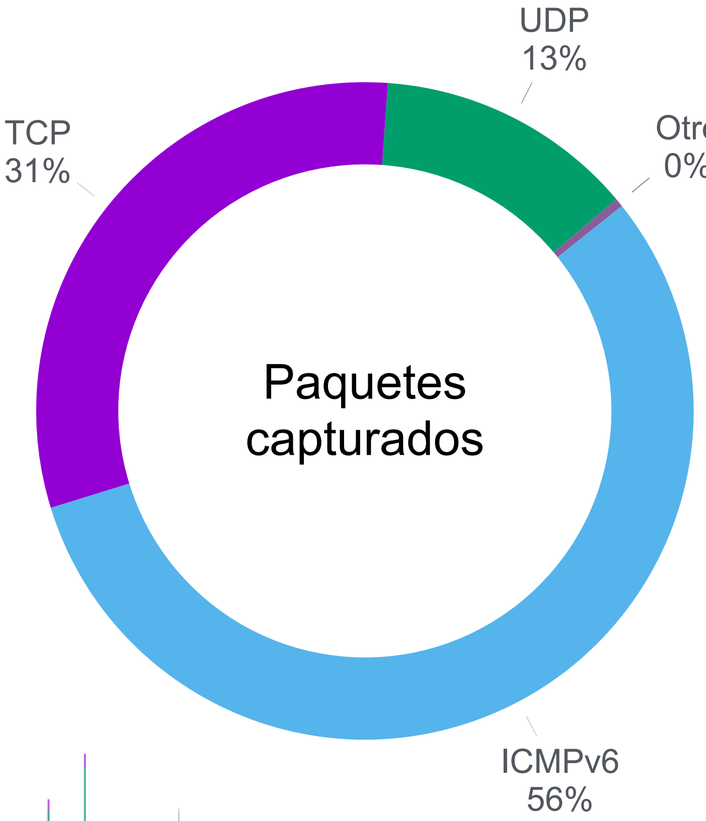
Captura de paquetes

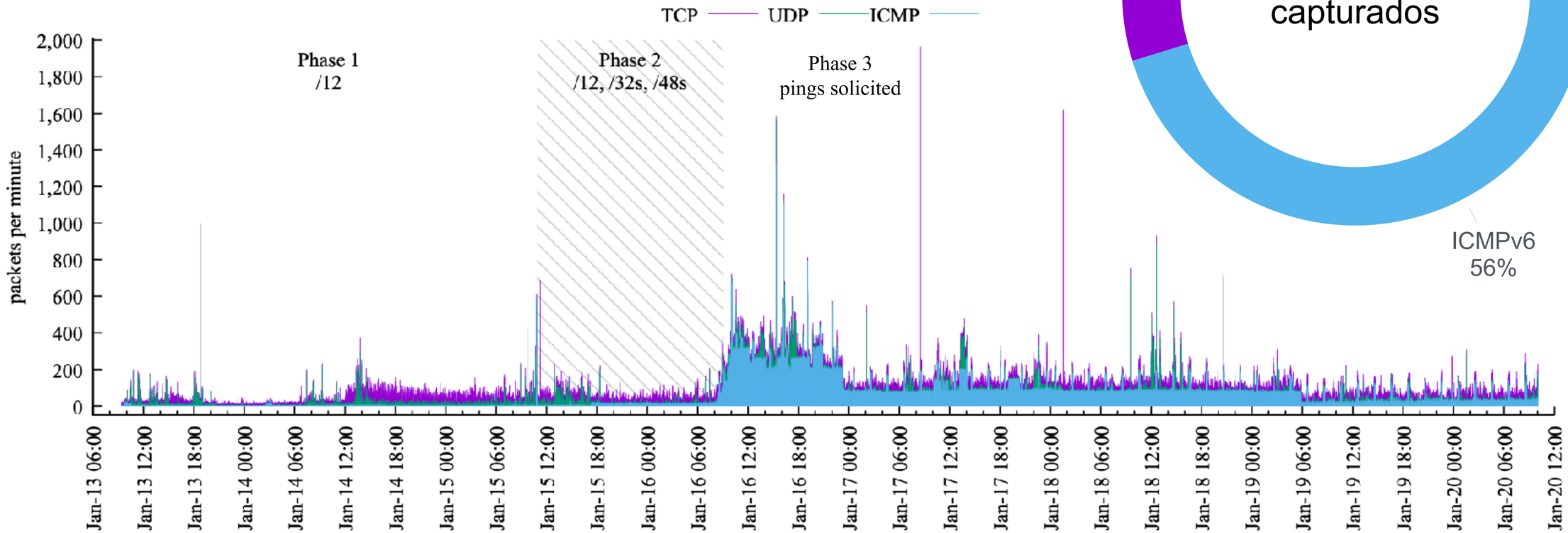
- 6613 direcciones IP de origen
- Camino de retorno ICMP
  - ~4% de direcciones de origen generaron error



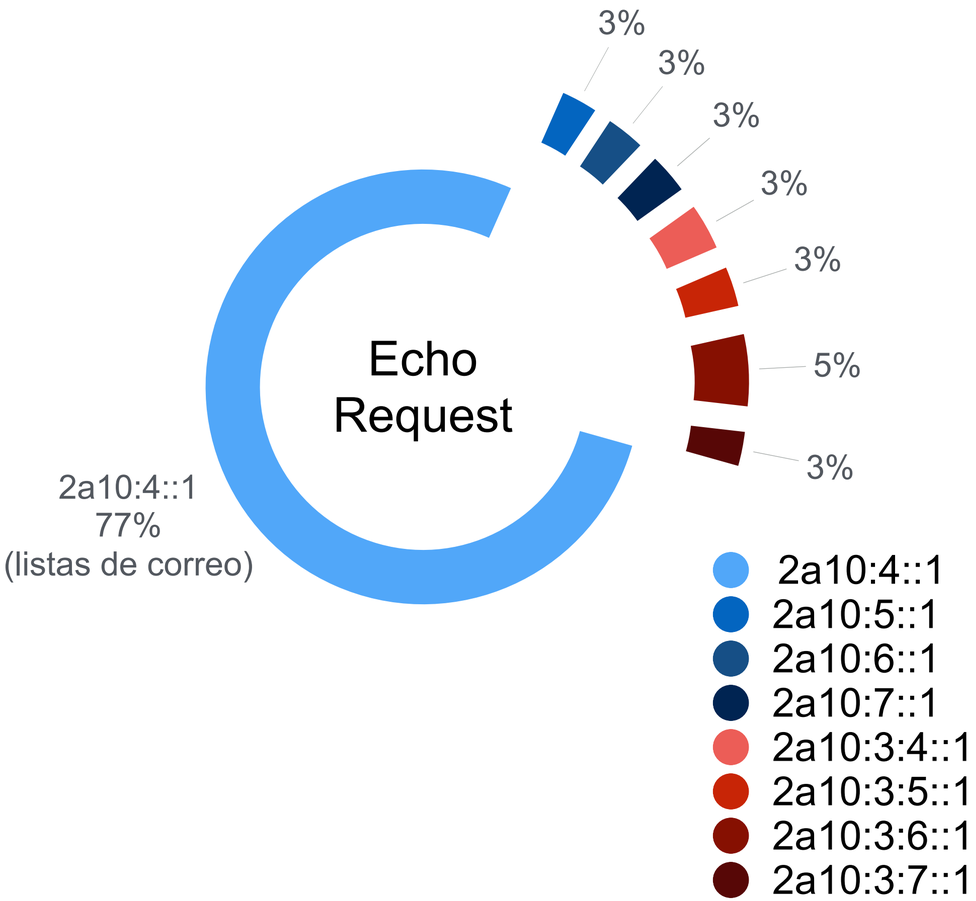
Captura de paquetes

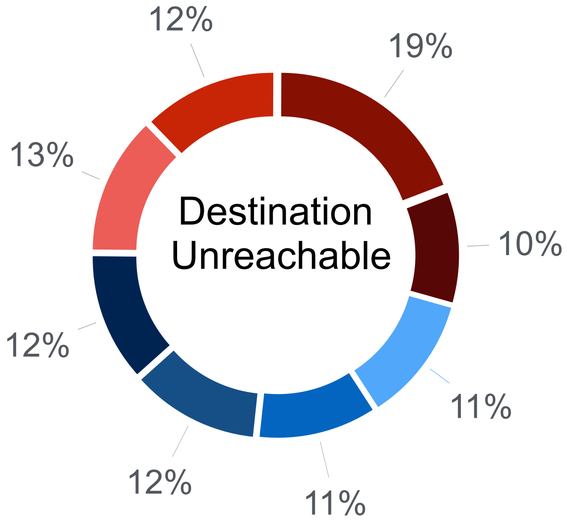
- Resto del tráfico, excluyendo:
  - Escaner TCP
  - Tráfico proveniente de RIPE Atlas

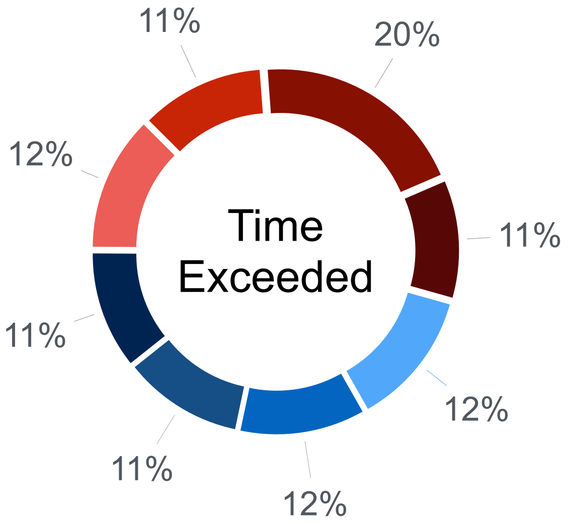




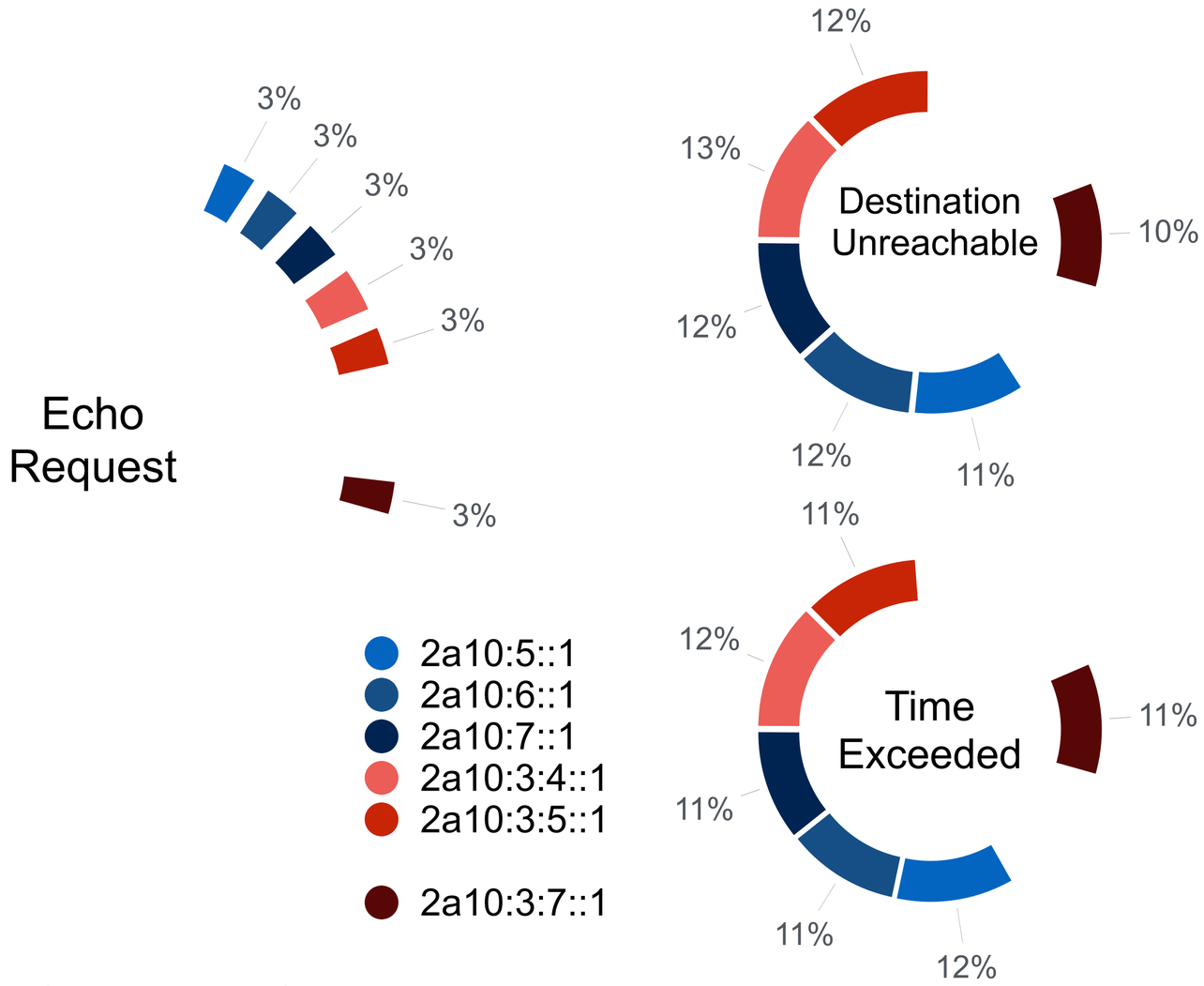
ICMPv6

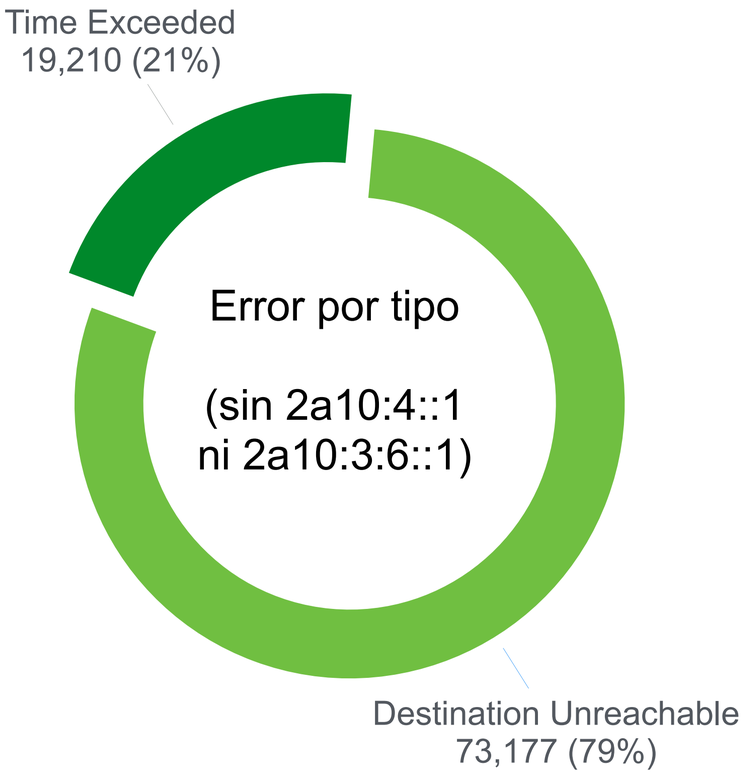

Echo Request
2a10:4::1
77%
(listas de correo)
3%
3%
3%
3%
3%
5%
3%
2a10:4::1
2a10:5::1
2a10:6::1
2a10:7::1
2a10:3:4::1
2a10:3:5::1
2a10:3:6::1
2a10:3:7::1


Destination Unreachable
12%
19%
13%
10%
12%
11%
12%
11%


Time Exceeded
11%
20%
12%
11%
11%
12%
11%
12%

ICMPv6


Echo Request
3%
3%
3%
3%
3%
3%
Destination Unreachable
12%
13%
10%
12%
12%
11%
Time Exceeded
11%
12%
11%
11%
11%
12%
2a10:5::1
2a10:6::1
2a10:7::1
2a10:3:4::1
2a10:3:5::1
2a10:3:7::1


Time Exceeded
19,210 (21%)
Error por tipo
(sin 2a10:4::1
ni 2a10:3:6::1)
Destination Unreachable
73,177 (79%)

TCP

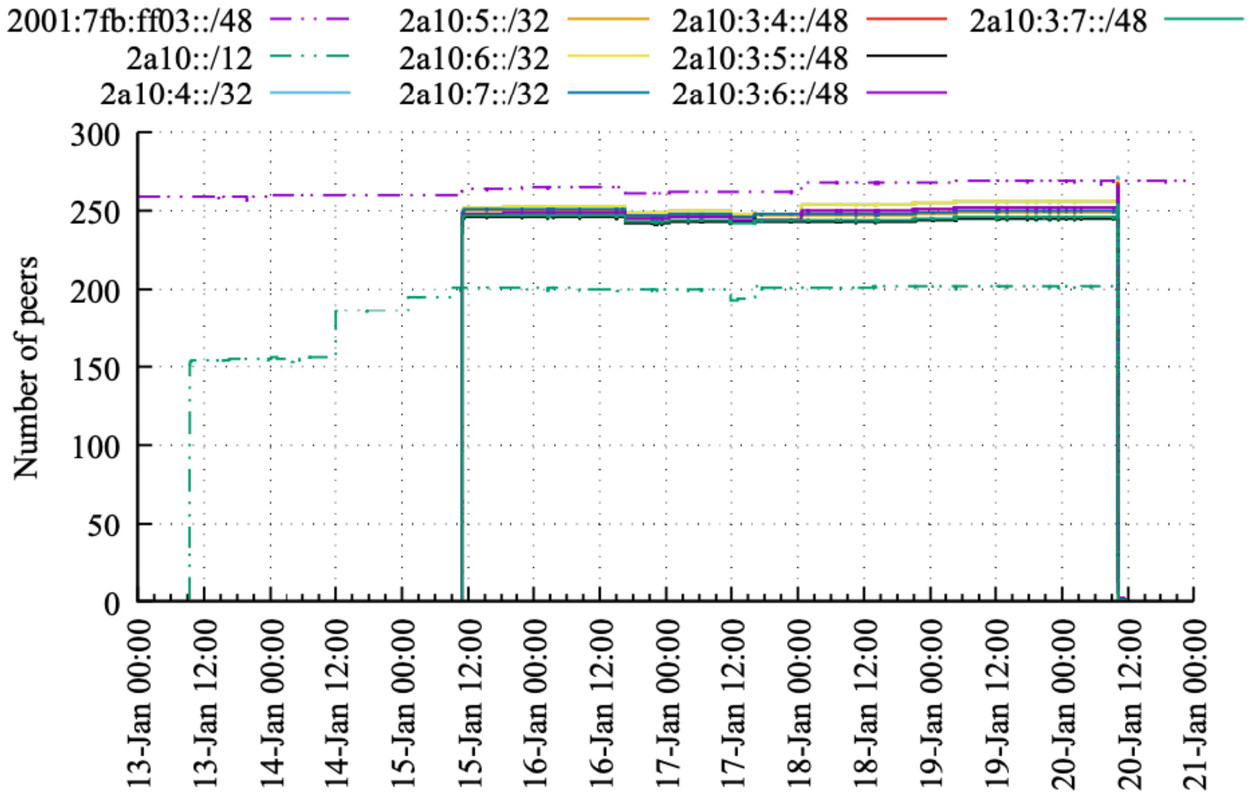
- src={5000..64999} dst=312 puertos
  - (redis, Tor, criptomonedas, HTTPS, POP3, IMAP)
  - Búsqueda de servicios vulnerables
  - Mayormente 3 `/96`s
- Patrones típicos en IPv4
  - Rotación de los últimos 16 bits de la dirección
  - MSS=1460 bytes

UDP

- DNS
  - Desde 530 `/64s`
  - 88% queries `A` o `AAAA`
  - 77% nombres en Cisco Umbrella 1 Million
  - Queries `HINFO` hacia abuse.net con string `"@<dominio>.contacts.abuse.net"`
- Algo de tráfico hacia el puerto 443
  - `src=2a02:2f00::/28 dst=2a12:2f00::/28`
- Mayoría errores en configuraciones

Visibilidad desde RIS

- Anunciado desde el RRC03 con conexión en AMS-IX y NL-IX
- ¿Cuántos peers ven el prefijo?
- Referencia:
  `2001:7fb:ff03::/48`
  (anunciado >10 años)
- `/12` baja propagación (esperado)



Visibilidad desde RIS

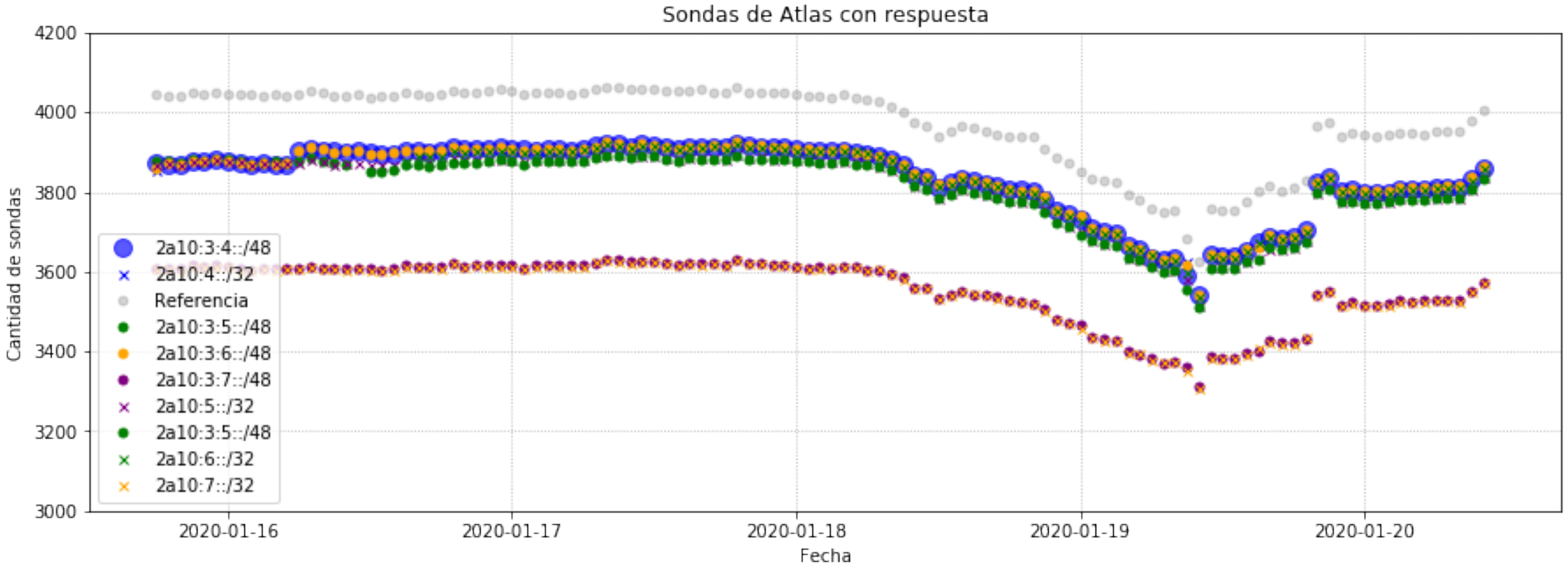
- Prefijo de referencia `2001:7fb:ff03::/48`
  - Visto por 262 peers

/32		ROA ✔	ROA ✘
IRR	✔	96.2%	96.2%
	✘	95.0%	95.4%

/48		ROA ✔	ROA ✘
IRR	✔	94.7%	94.7%
	✘	93.5%	93.9%

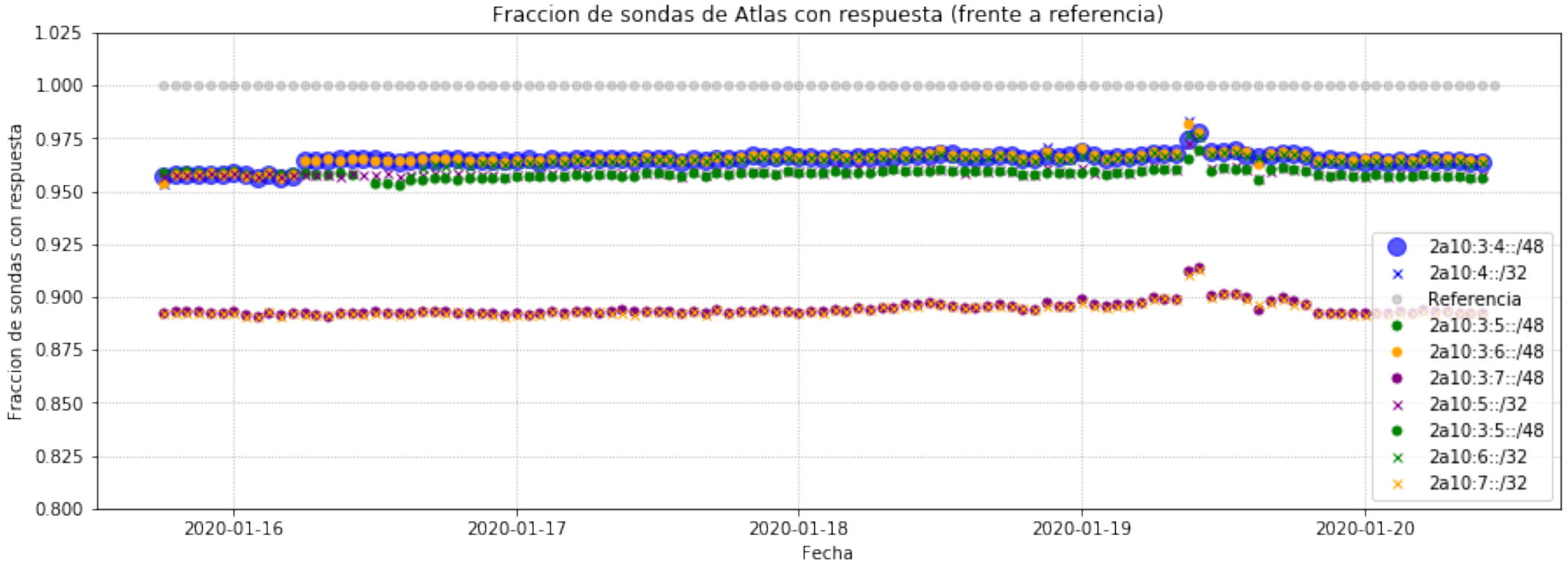
Visibilidad desde sondas de Atlas

- Envío de traceroutes a partir de la Fase 2
- Comparación frente a un prefijo de referencia (`2001:7fb:ff03::/48`)
- ¿Cuántas sondas reciban respuesta alguna?



Visibilidad desde sondas de Atlas

- Envío de traceroutes a partir de la Fase 2
- Comparación frente a un prefijo de referencia (`2001:7fb:ff03::/48`)
- ¿Cuántas sondas reciban respuesta alguna?



Visibilidad desde sondas de Atlas

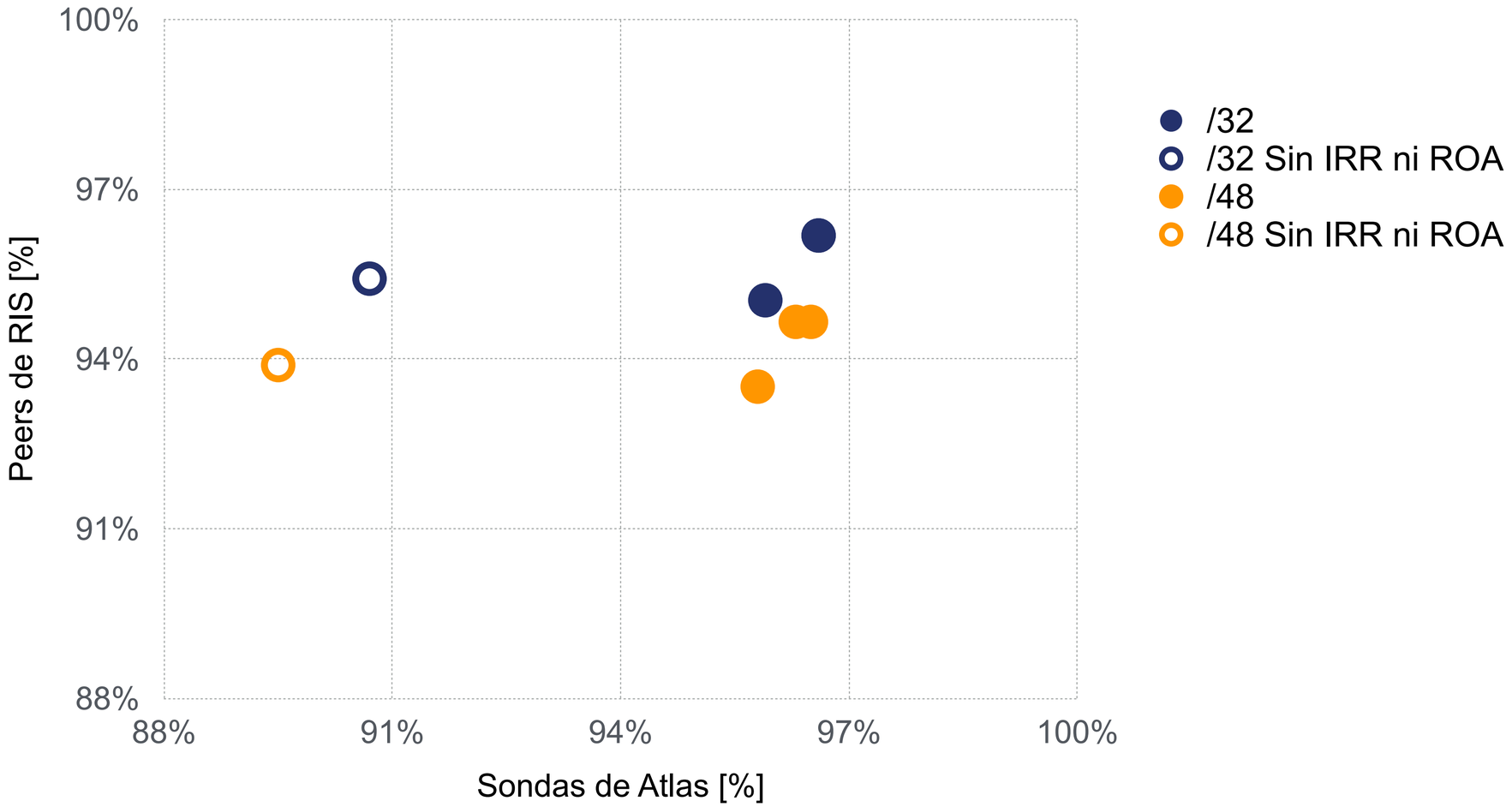
- Prefijo de referencia `2001:7fb:ff03::/48`
  - Alcanzable por +4000 sondas

/32		ROA	
		✔	✘
IRR	✔	96.6%	96.6%
	✘	95.9%	**90.7%**

/48		ROA	
		✔	✘
IRR	✔	96.3%	96.5%
	✘	95.8%	**89.5%**

Visibilidad desde Atlas y RIS

Porcentaje de peers de RIS que ven un prefijo, en relación al prefijo de referencia `2001:7fb:ff03::/48`



Porcentaje de sondas de Atlas que pueden hacer traceroute a un prefijo, en relación al prefijo de referencia `2001:7fb:ff03::/48`

Conclusiones

- Espacio apto para ser asignado a miembros de RIPE NCC ✔
- Tráfico bajo
- Observaciones
  - Escaner TCP coordinado
  - Errores en camino de retorno, sobre todo hacia Atlas
  - Resto del tráfico: poco y desde muchos orígenes
  - Tráfico DNS: accidental, errores en configuraciones
  - Similares comportamientos que cuando se escanea el espacio IPv4
- RIS y Atlas mayormente alineados

¡Gracias!

aformoso@ripe.net
@aguformoso