RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Debogonising 2a10::/12

Analysis of one week's visibility of a new /12

Stephen Strowes
René Wilhelm
Florian Obser
Riccardo Stagni
Agustín Formoso
Emile Aben

TMA 2020 | 2020-06-10

A new /12

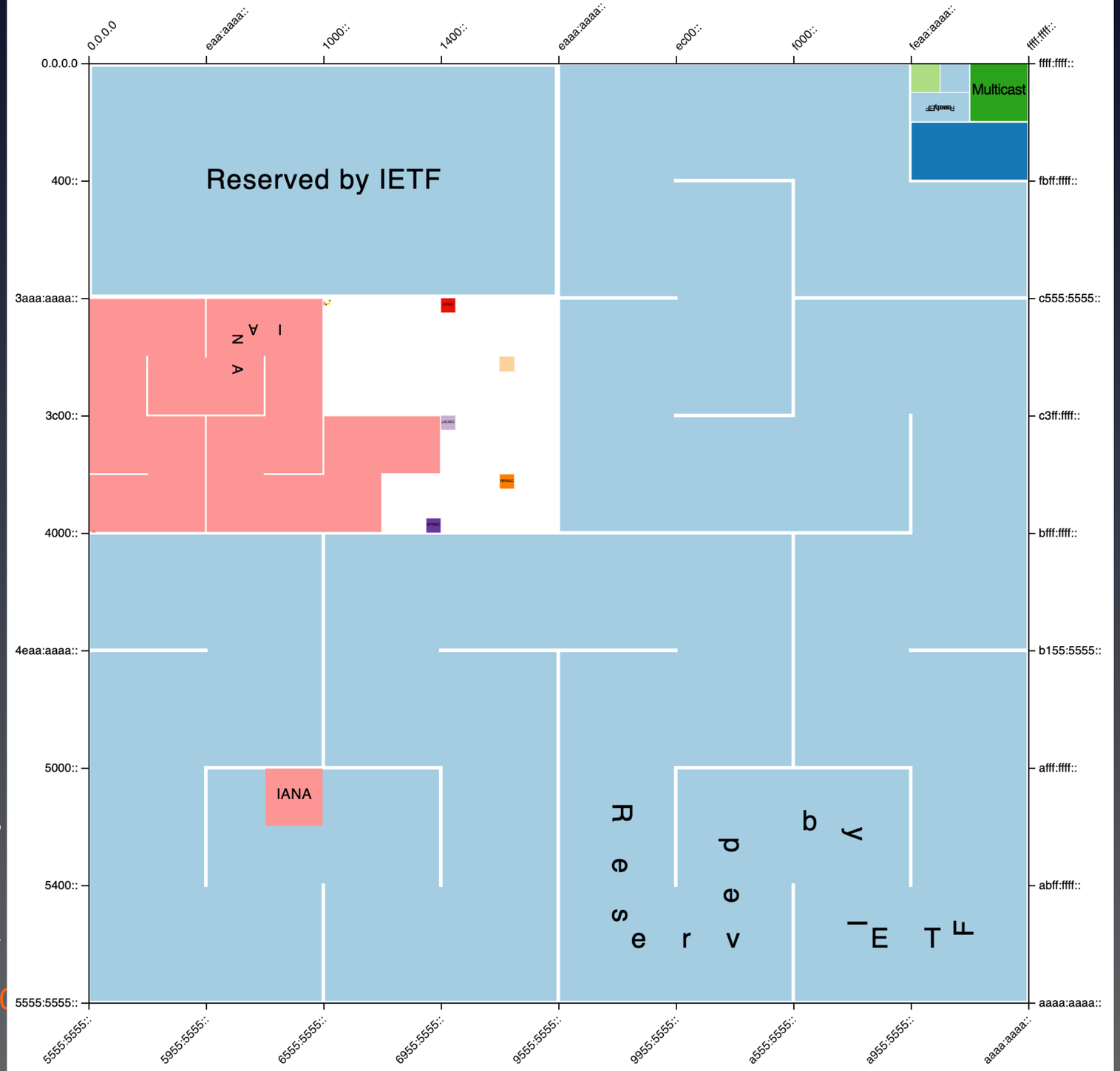
2400:0000::/12	APNIC	2006-10-03	whois.apnic.net	https://rdap.apnic.net/	ALLOCATED
2600:0000::/12	ARIN	2006-10-03	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2800:0000::/12	LACNIC	2006-10-03	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
2a00:0000::/12	RIPE NCC	2006-10-03	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED
2c00:0000::/12	AFRINIC	2006-10-03	whois.afrinic.net	https://rdap.afrinic.net/rdap/ http://rdap.afrinic.net/rdap/	ALLOCATED

2a10:0000::/12	RIPE NCC	2019-06-05	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED
2630:0000::/12	ARIN	2019-11-06	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED

https://www.iana.org/assignments/ipv6-unicast-address-assignments/

Motivating Questions

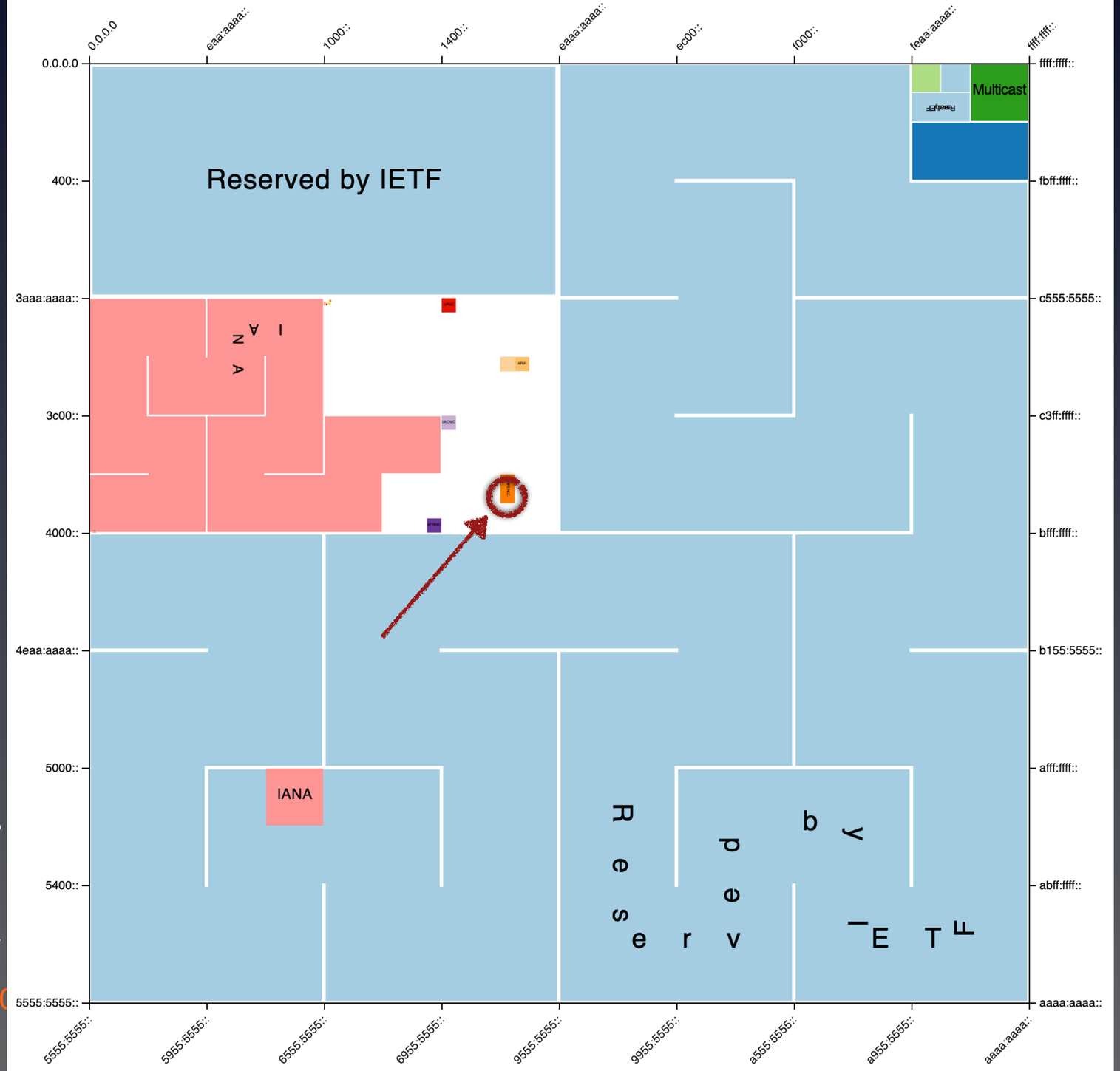
- Is it possible to use this address space?
- Is it safe to use this address space?



https://bl.ocks.org/vasturiano/ba0bdc27ddc2b13012e85b2a0b7a1c43

Prior Work

Study	Prefix	Period	Packets	Rate
Ford *et al.*, 2006 [4]	unspec. /48	16 mos.	12	0.025
APNIC, 2010 [5]	2400::/12	10 days	21.2K	2,210
Merit, 2013 [6]	2400::/12	3 mos.	1.3B	14.4M
	2600::/12	3 mos.	2.5B	27.8M
	2800::/12	3 mos.	504.8M	5.6M
	2c00::/12	3 mos.	20.3M	226K
	2a00::/12	5 days	25.5M	5.1M
	2a04::/14 2a08::/13	3 mos.	3K	33.3



https://bl.ocks.org/sdstrowes/f4190083a42fe6fbf33ef4e59128ff2b0

https://www.esa.int/Enabling_Support/Operations/Hubble_operations

Experimental Design

Experimental Design

- Announce the full /12
- Announce /32s and /48s
  - each configured slightly differently
- Set up one address responsive to echo requests in each
  - Run RIPE Atlas measurements to each
- Capture traffic sent into 2a10::/12

Prefix	IRR	ROA	Responsive address
2a10::/12	no	no	
2a10:4::/32	yes	yes	2a10:4::1
2a10:5::/32	no	yes	2a10:5::1
2a10:6::/32	yes	no	2a10:6::1
2a10:7::/32	no	no	2a10:7::1
2a10:3:4::/48	yes	yes	2a10:3:4::1
2a10:3:5::/48	no	yes	2a10:3:5::1
2a10:3:6::/48	yes	no	2a10:3:6::1
2a10:3:7::/48	no	no	2a10:3:7::1

Experimental Design

Experimental Design

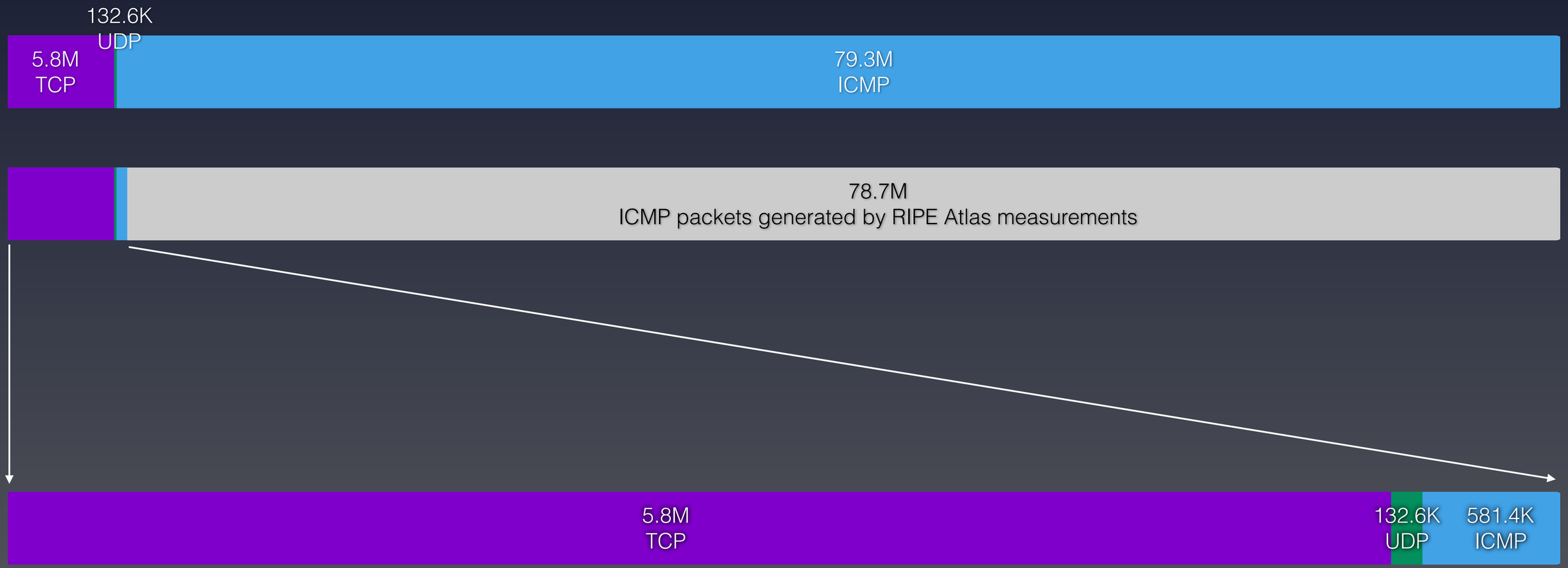
- RIS collects global routing state
- RIPE Atlas pings and traceroutes measure reachability
- Analyse traffic received by 2a10::/12

Captured Traffic

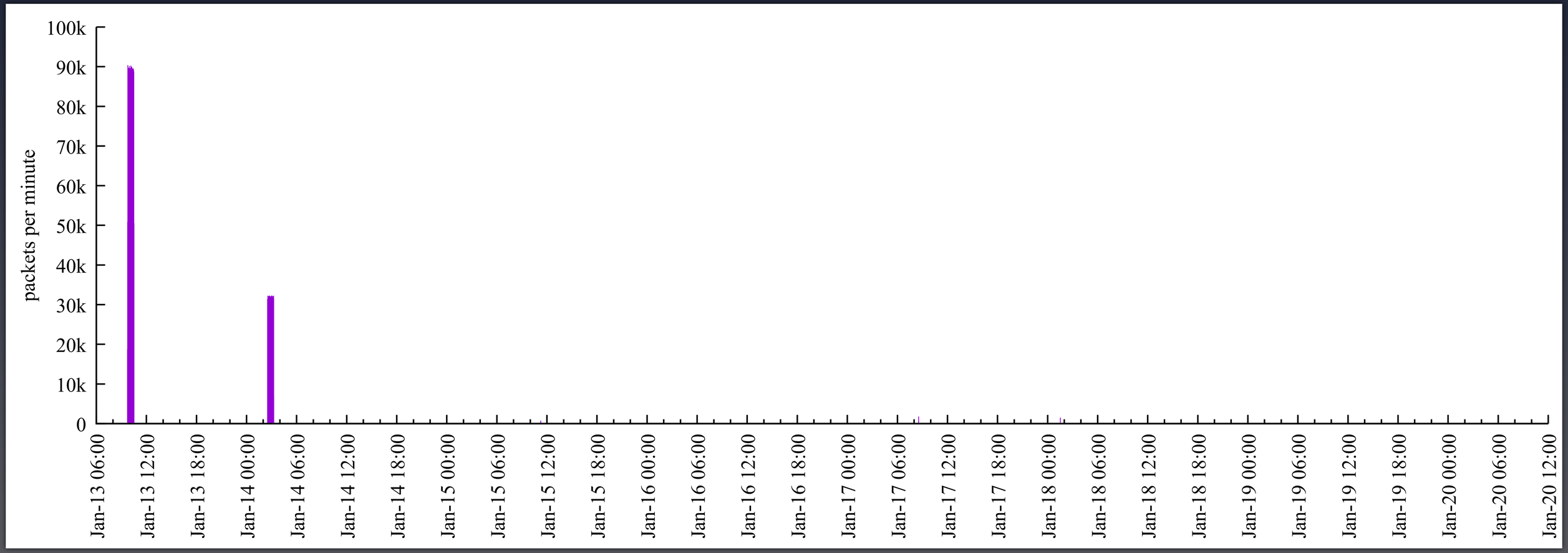
Overview

- Across one week, we captured 85.2M packets at 2a10::/12
  - 78.7M of these were generated by RIPE Atlas

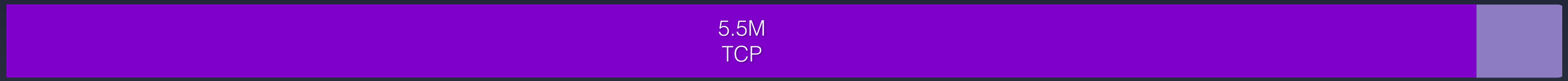
Traffic Overview



TCP

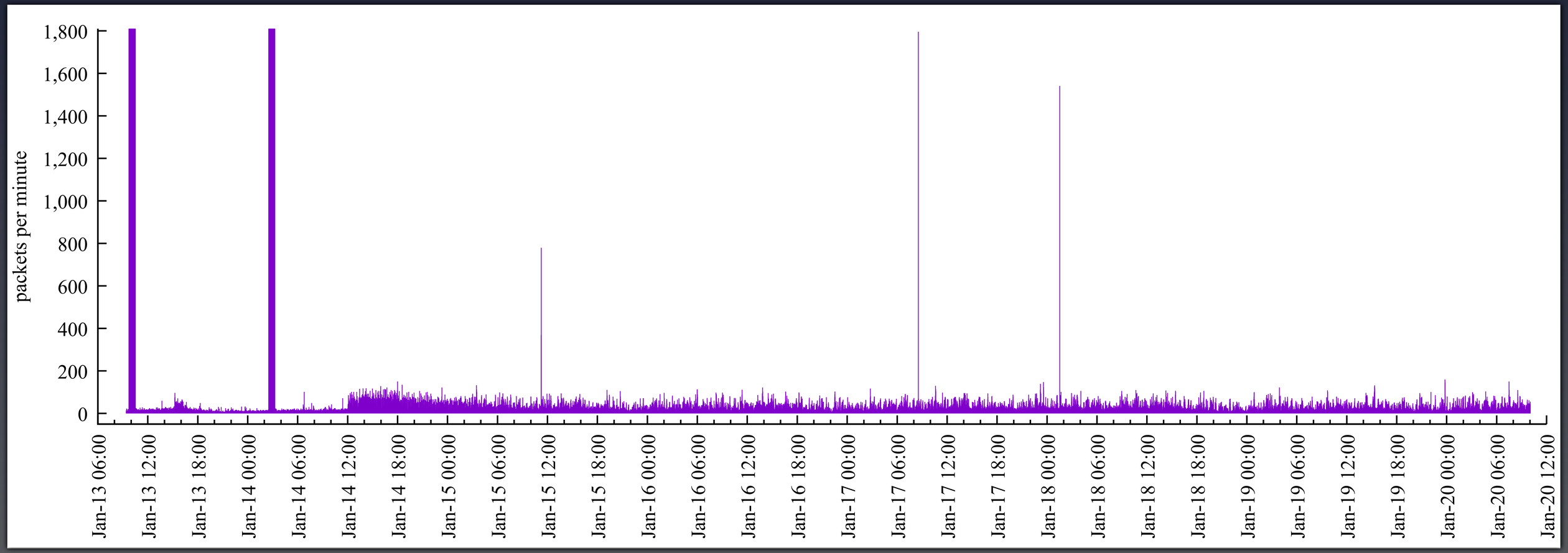

packets per minute
100k
90k
80k
70k
60k
50k
40k
30k
20k
10k
0
Jan-13 06:00
Jan-13 12:00
Jan-13 18:00
Jan-14 00:00
Jan-14 06:00
Jan-14 12:00
Jan-14 18:00
Jan-15 00:00
Jan-15 06:00
Jan-15 12:00
Jan-15 18:00
Jan-16 00:00
Jan-16 06:00
Jan-16 12:00
Jan-16 18:00
Jan-17 00:00
Jan-17 06:00
Jan-17 12:00
Jan-17 18:00
Jan-18 00:00
Jan-18 06:00
Jan-18 12:00
Jan-18 18:00
Jan-19 00:00
Jan-19 06:00
Jan-19 12:00
Jan-19 18:00
Jan-20 00:00
Jan-20 06:00
Jan-20 12:00

TCP



- Characteristics:
  - consistent source (49152) and destination (80) ports
  - no data in the segment
  - SYN flag set
  - increasing *hop-limit* (*i.e.*, TTL) in headers
  - over-sized MSS value
- Coordinated across more than one ASN

TCP


packets per minute
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
Jan-13 06:00
Jan-13 12:00
Jan-13 18:00
Jan-14 00:00
Jan-14 06:00
Jan-14 12:00
Jan-14 18:00
Jan-15 00:00
Jan-15 06:00
Jan-15 12:00
Jan-15 18:00
Jan-16 00:00
Jan-16 06:00
Jan-16 12:00
Jan-16 18:00
Jan-17 00:00
Jan-17 06:00
Jan-17 12:00
Jan-17 18:00
Jan-18 00:00
Jan-18 06:00
Jan-18 12:00
Jan-18 18:00
Jan-19 00:00
Jan-19 06:00
Jan-19 12:00
Jan-19 18:00
Jan-20 00:00
Jan-20 06:00
Jan-20 12:00

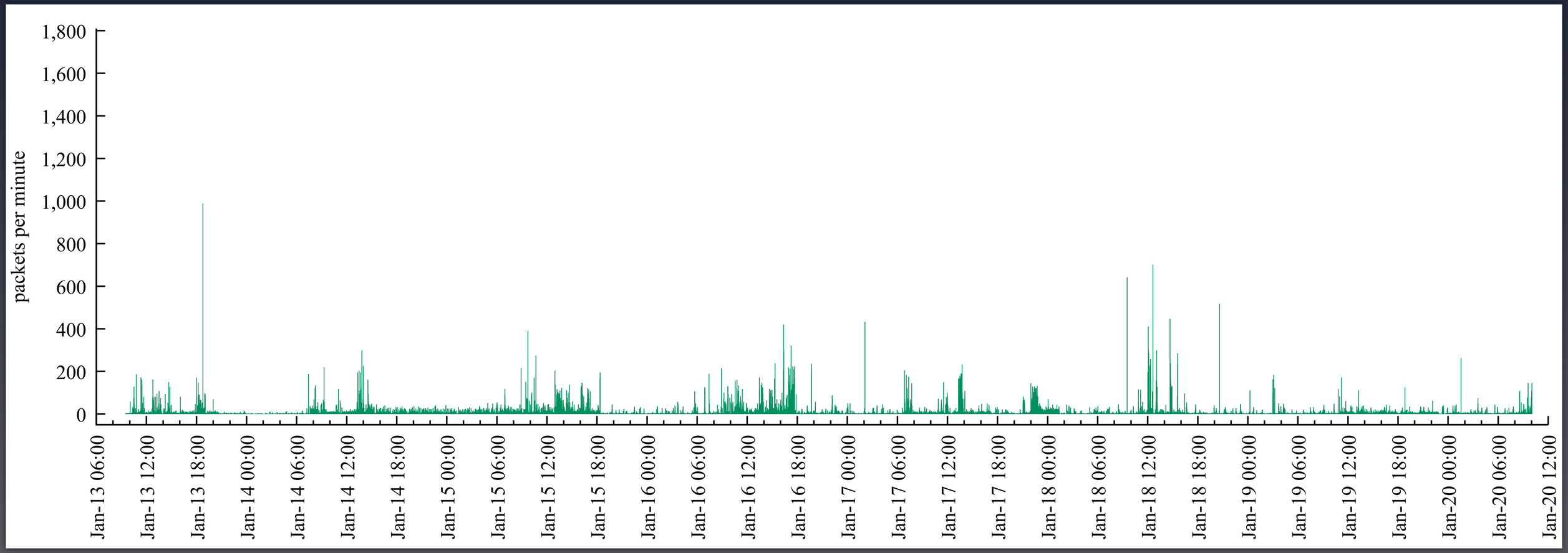
TCP

- Characteristics:
  - two origin IPs within one /64 in AS58461 (China Telecom)
  - SYN set, no data payload
  - targeting addresses within three /96s
  - targeting various TCP ports, such as 6379 (redis), port 6697 (IRC), HTTPS, POP3, IMAP, and various others
  - also an over-sized MSS value

TCP

- ~41k: dst port 443 + ACK flag
  - various source/destination IP pairs
- Other noise, including christmas tree packets

UDP


packets per minute
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
Jan-13 06:00
Jan-13 12:00
Jan-13 18:00
Jan-14 00:00
Jan-14 06:00
Jan-14 12:00
Jan-14 18:00
Jan-15 00:00
Jan-15 06:00
Jan-15 12:00
Jan-15 18:00
Jan-16 00:00
Jan-16 06:00
Jan-16 12:00
Jan-16 18:00
Jan-17 00:00
Jan-17 06:00
Jan-17 12:00
Jan-17 18:00
Jan-18 00:00
Jan-18 06:00
Jan-18 12:00
Jan-18 18:00
Jan-19 00:00
Jan-19 06:00
Jan-19 12:00
Jan-19 18:00
Jan-20 00:00
Jan-20 06:00
Jan-20 12:00

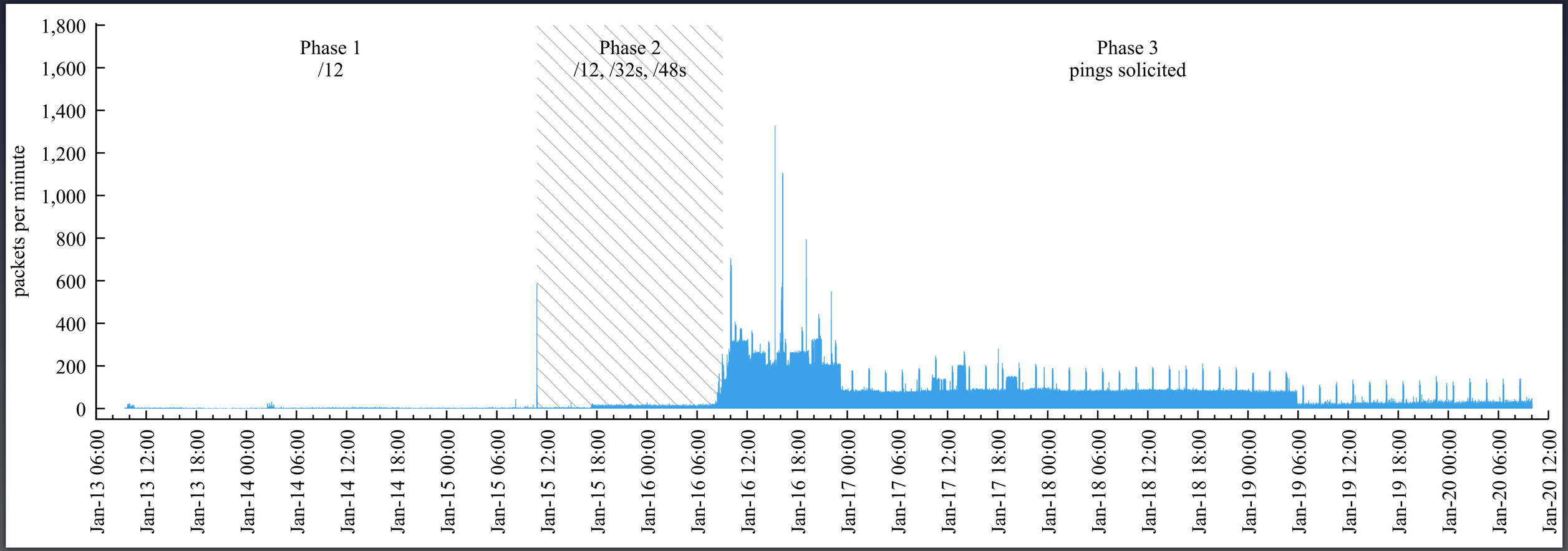
UDP

- DNS
  - over 60k were misconfiguration in one network
  - ~6.7k appear to be queries for *abuse.net*
  - ~500 are querying the *version.bind* string
  - few query A or AAAA records for names

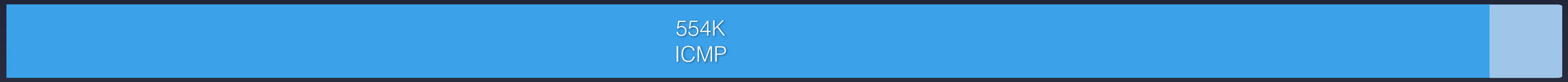
UDP

- Few standouts
  - some 10k target UDP port 1
  - another 1.5k have origin port 443

ICMP

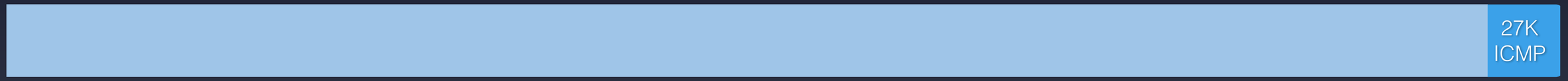

Phase 1
/12
Phase 2
/12, /32s, /48s
Phase 3
pings solicited
packets per minute
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
Jan-13 06:00
Jan-13 12:00
Jan-13 18:00
Jan-14 00:00
Jan-14 06:00
Jan-14 12:00
Jan-14 18:00
Jan-15 00:00
Jan-15 06:00
Jan-15 12:00
Jan-15 18:00
Jan-16 00:00
Jan-16 06:00
Jan-16 12:00
Jan-16 18:00
Jan-17 00:00
Jan-17 06:00
Jan-17 12:00
Jan-17 18:00
Jan-18 00:00
Jan-18 06:00
Jan-18 12:00
Jan-18 18:00
Jan-19 00:00
Jan-19 06:00
Jan-19 12:00
Jan-19 18:00
Jan-20 00:00
Jan-20 06:00
Jan-20 12:00

ICMP



- ICMP to responsive targets
  - the only traffic solicited for this study
  - echo requests originate from 892 separate /64s

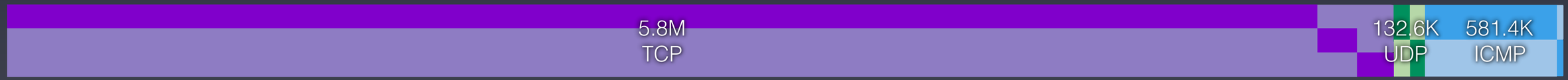
ICMP



- ICMP to other (unresponsive) destinations
  - includes “junk” traffic

Traffic Summary

- We captured 85.2M packets with destinations in 2a10::/12
  - 78.7M of these were generated by RIPE Atlas
- The remaining 6.5M falls into a few main categories



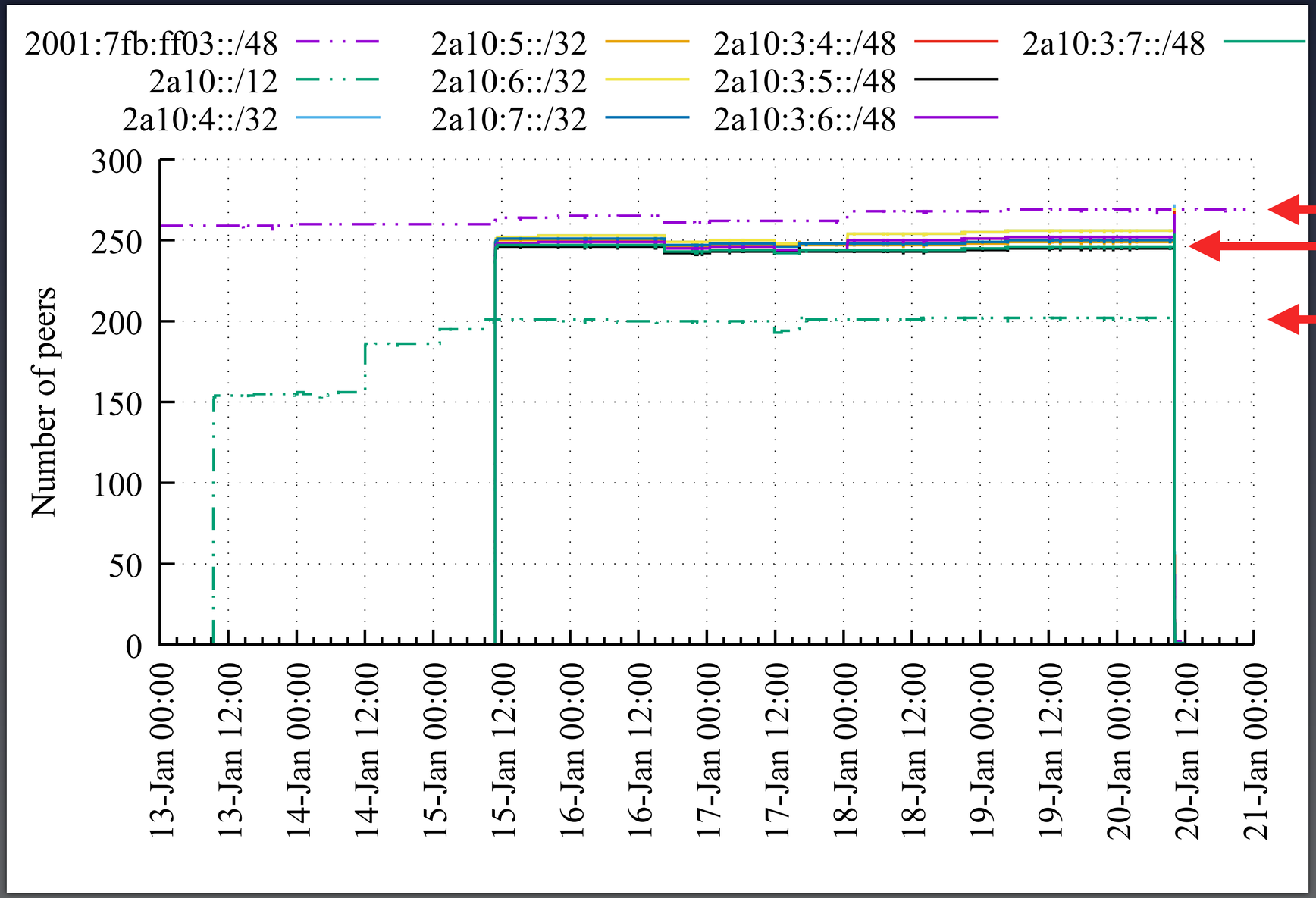
- TCP traceroute; some TCP port scanning
- Some DNS (misconfiguration)
- Echo requests (solicited)

Routing

Routing

- Key question: Are these prefixes visible?
  - All prefixes are visible at all 21 route collectors
- How widely visible are they?
  - We compare against a stable “anchor” prefix announced from the same origin
  - 2001:7FB:FF03::/48
    https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/current-ris-routing-beacons

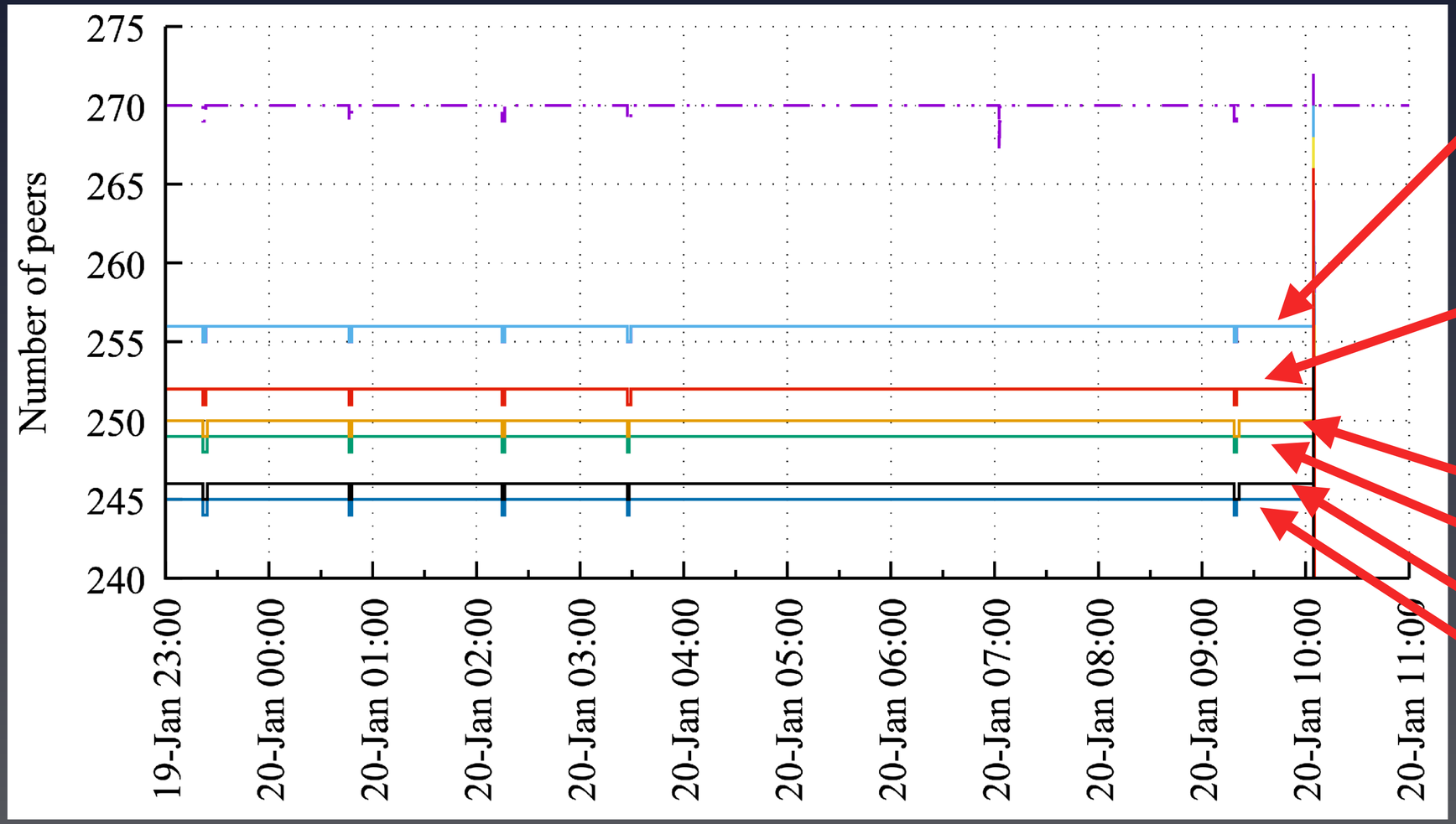
Routing



Stable anchor /32s and /48s

2a10::/12

Routing



2a10:4::/32 & 2a10:6::/32

2a10:3:4::/48 & 2a10:3:6::/48

2a10:3:7::/48

2a10:3:5::/48

2a10:3:7::/48

2a10:3:5::/48

RIPE Atlas

RIPE Atlas

Prefix	Responsive address	IRR	ROA	ping % response
2a10:4::/32	2a10:4::1	yes	yes	95.5%
2a10:5::/32	2a10:5::1	no	yes	94.8%
2a10:6::/32	2a10:6::1	yes	no	95.5%
2a10:7::/32	2a10:7::1	no	no	88.1%
2a10:3:4::/48	2a10:3:4::1	yes	yes	95.4%
2a10:3:5::/48	2a10:3:5::1	no	yes	95.5%
2a10:3:6::/48	2a10:3:6::1	yes	no	95.5%
2a10:3:7::/48	2a10:3:7::1	no	no	88.2%

Responsiveness

- Two patterns:

1. Probes with no response from any test address:

   Observed in 39 ASNs.

2. Probes with no response from the “:7:” addresses

   Observed primarily in AS3320 or ASNs that route via 3320.

Responsiveness

- Disregarding these two categories:
  - response rates to the test targets ~99.0% from 3,698 probes in 1,338 ASNs

In Summary

In Summary

- First new /12 in ~12 years
- Study on “background noise”
  - The traffic collected in this space is not onerous
  - Traffic is not concentrated in any particular subnet
- Routing visibility is generally good
- Reachability is generally good
  - Put your route objects in the database!

Questions?

slack, email, twitter