ROA deployment in the DNS Core

24 January 2021 Data Included

Edward Lewis

NANOG 81
8-10 February 2021

Purpose of the talk

- Is a new technology "ready for operations"?
- *Or perhaps:* How ready is a technology for operations?

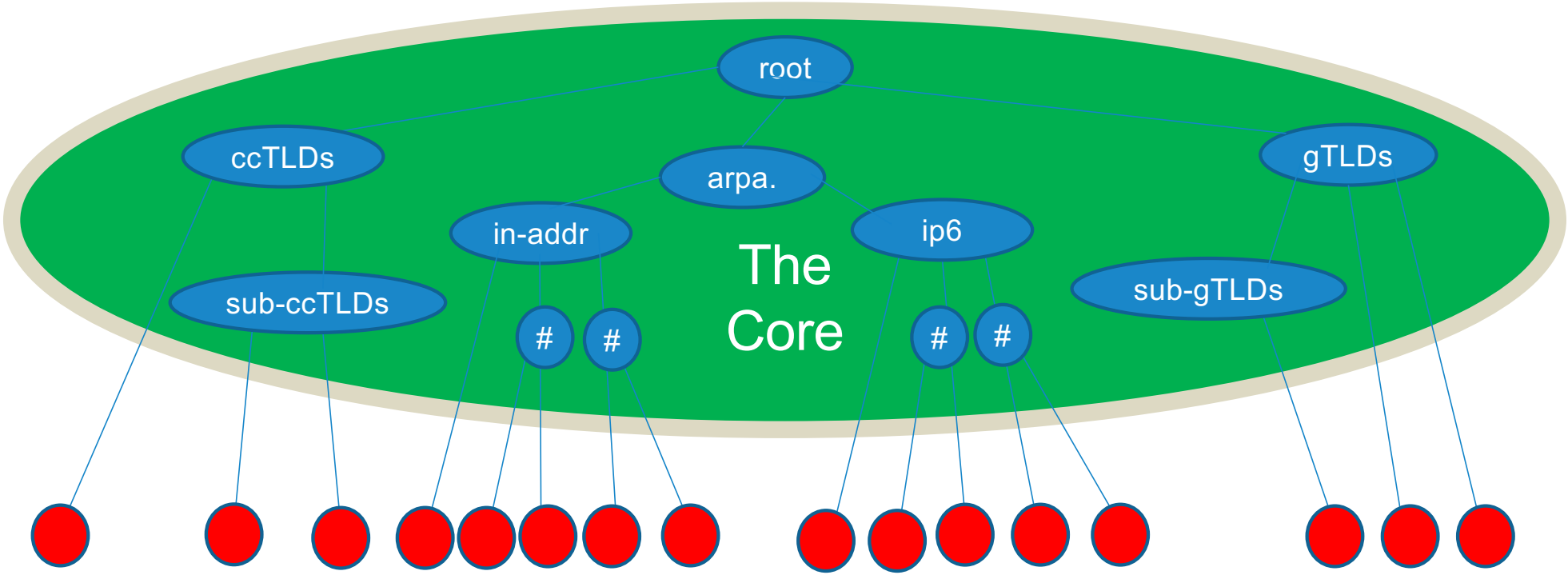
- It's not a "yes/no" question, it is a sliding scale
  - A way to discover whether further development is needed, adjustments are needed, etc., to achieve whatever goals (like "full deployment") exist

Measuring ROA Deployment in the DNS Core

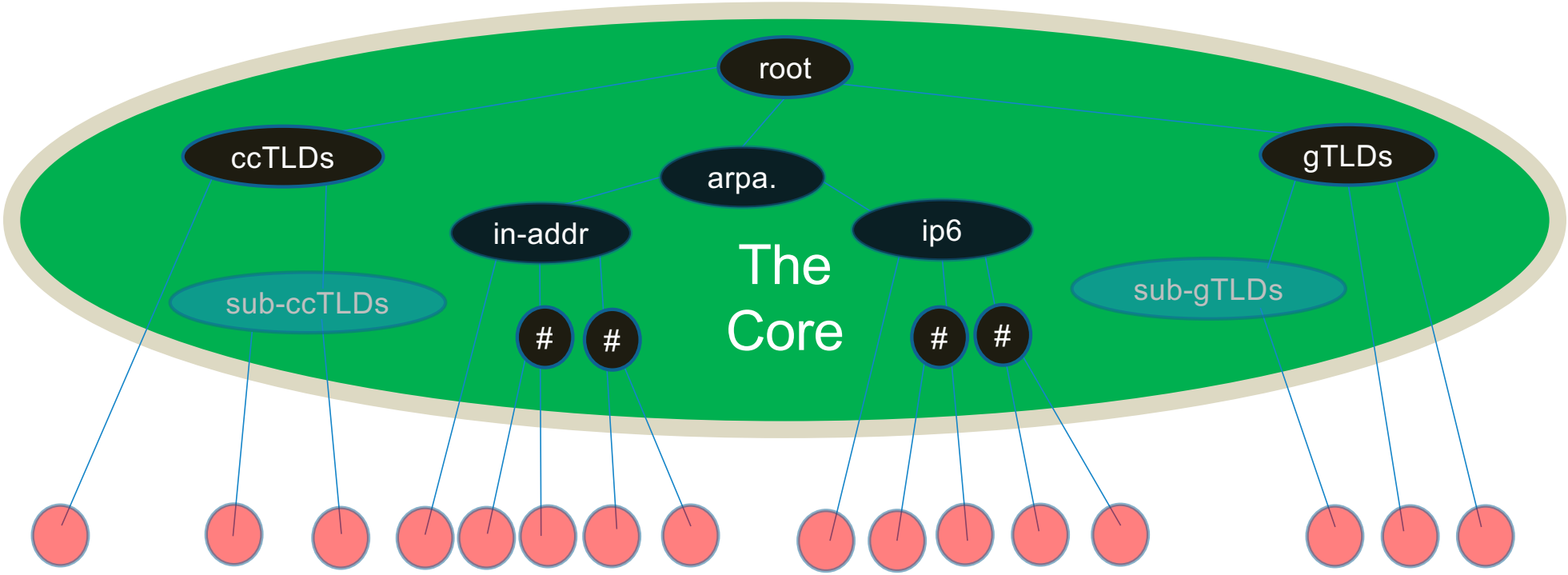
- This talk measures the adoption of Route Origin Attestations (part of the Routing Public Key Infrastructure) for routes leading to servers in the DNS Core

- What is the DNS Core?
- What are ROAs?

The DNS Core (in Cartoon Form)



I May "Slip Up" and talk about TLDs this way in the talk



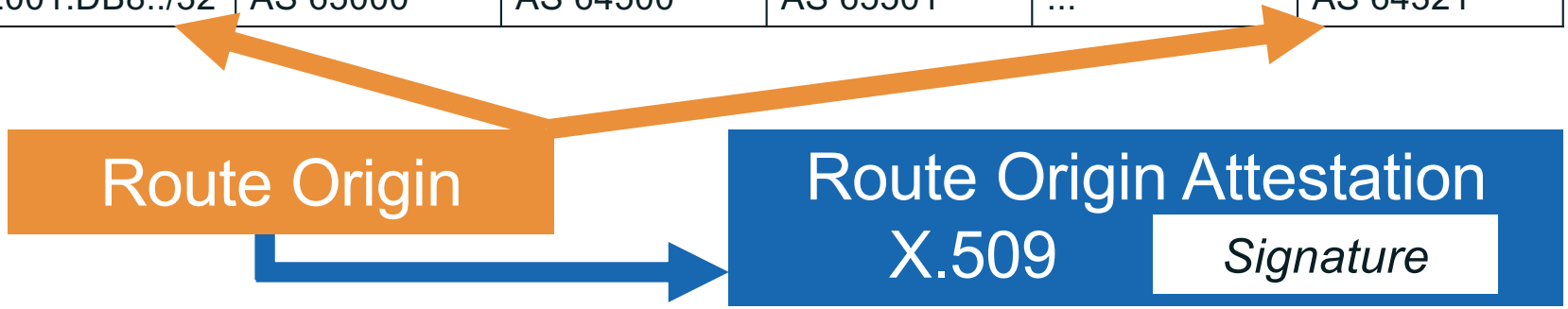
Caveats about defining the DNS Core

- The DNS Core covers the "upper reaches" of the DNS name space (root zone, top-level domains, etc.)
  - This space tends to be stable in membership
  - The operators have DNS as their primary mission
  - The protocol is at its "simplest" here
- Outside of this core there are:
  - Higher traffic zones (operationally meaningful)
  - Higher valued zones (financially meaningful)
  - Greater functionality (more complexity)
  - Well-engineered zones (DNS figures prominently in another mission)

ROAs = Route Origination Authorization

- RPKI is a Public Key Infrastructure framework deployed to secure BGP against invalid or unauthorized route announcements
  - ROA stands for Route Origination Authorization is a cryptographic attestation that the ASN is authorized to originate a network prefix

IP Prefix	Next ASN	Another ASN	Another ASN	...	Last Hop ASN
192.0.2.0/24	AS 65000	AS 64500	AS 64677		AS 64321
2001:DB8::/32	AS 65000	AS 64500	AS 65501	...	AS 64321



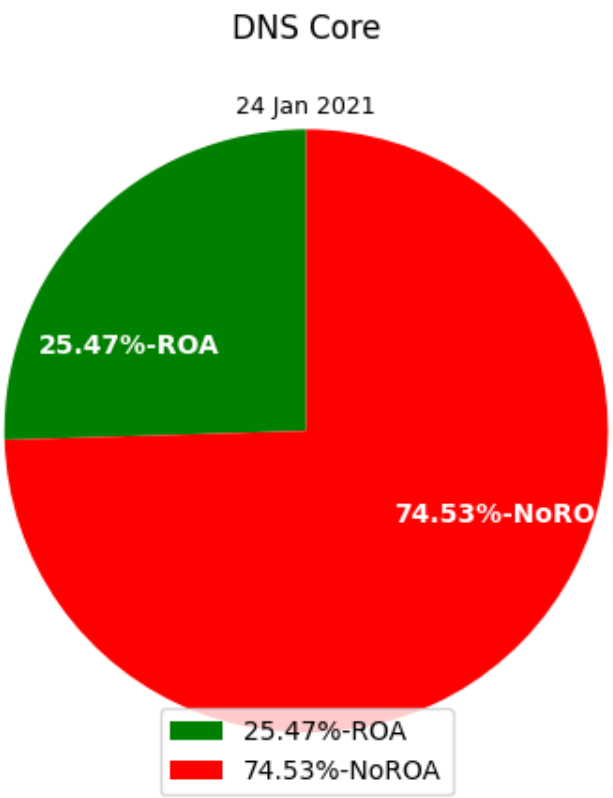
Is ROA Signing Happening In the DNS Core?

- With ROA a being a (relatively) "new" technology
- How far has it been deployed?
  - Low deployment would suggest it is a "hard sell"
  - High deployment would suggest it solves an "immediate need"
- Is there a pattern to the deployment?
  - Where should efforts to increase adoption be focused?
  - Where would studies discover needed improvement?
- Does work does not consider deployment of validation

Measurement Method

- Use a census (listing) of the the DNS core, looking at
  - zones
    - nameservers
      - addresses
        - route originations
  - Relying on Team Cymru's *IP to ASN mapping service*
- Does the route origination have a *validated-by-RIPE* ROA?
  - Yes or No, percentages are `"Yes"/("Yes"+"No")`

Overall ROA Coverage (Now = 24 January 2021)



Zones(+ subTLDs): 3114

TLDs(+ revmap): 1774

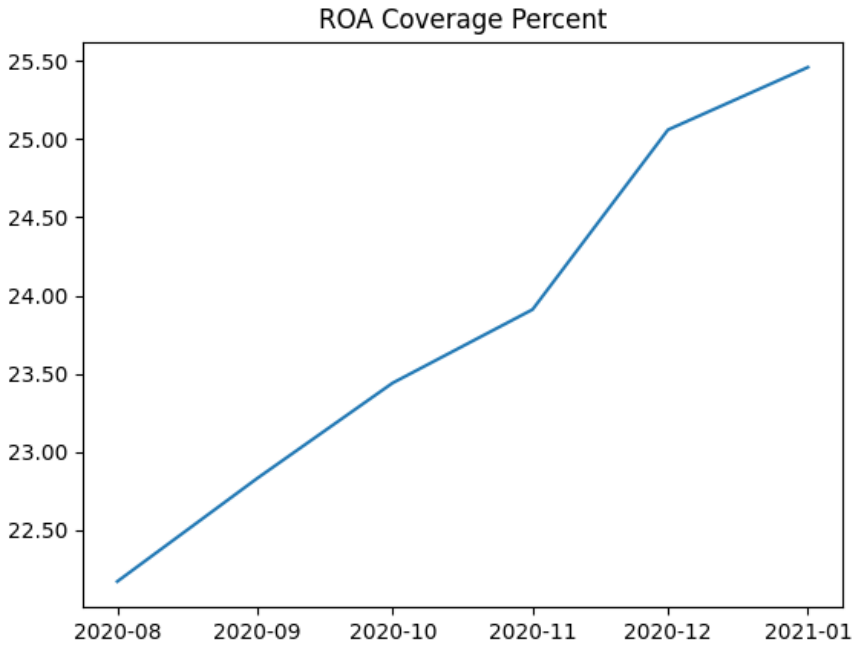
Nameservers: 4315

Addresses: 6917

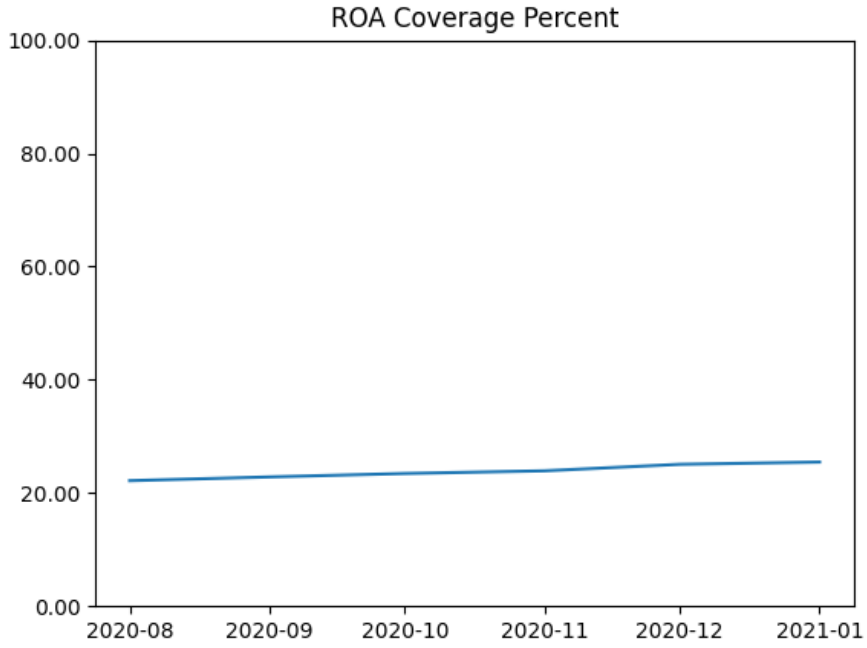
RouteOrigins: 2218

Overall ROA Coverage (Last 5 months)

- There's been steady upward measurements



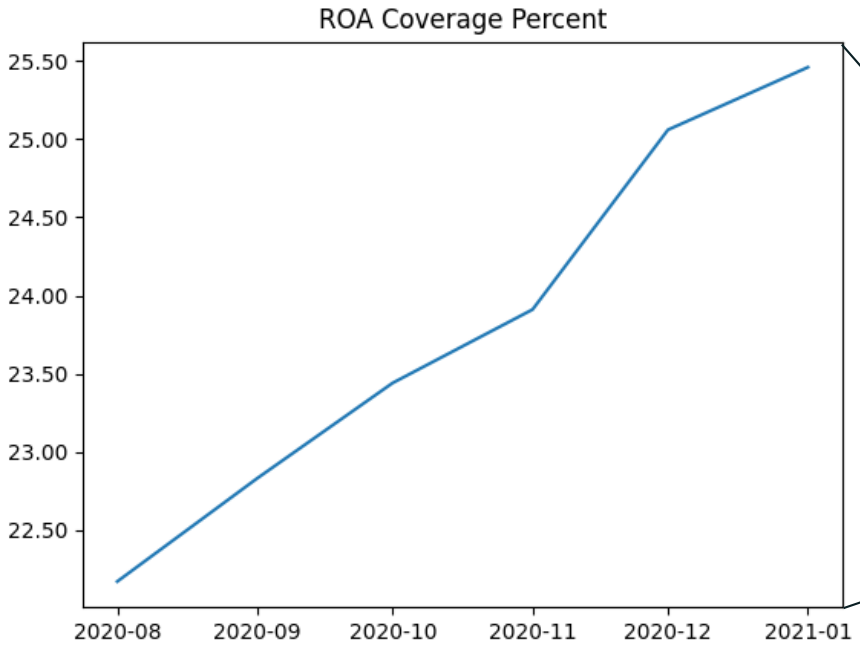
- It's a long way to 100%
- Linear fit: 9-10 more years

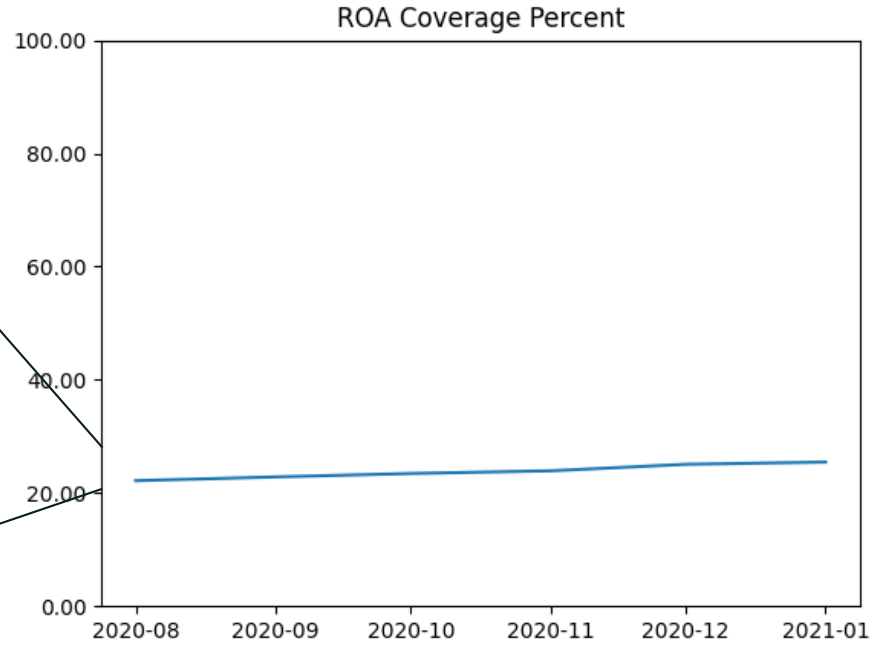


Overall ROA Coverage (Last 5 months)

- There's been steady upward measurements

- It's a long way to 100%
- At this rate: 9-10 more years



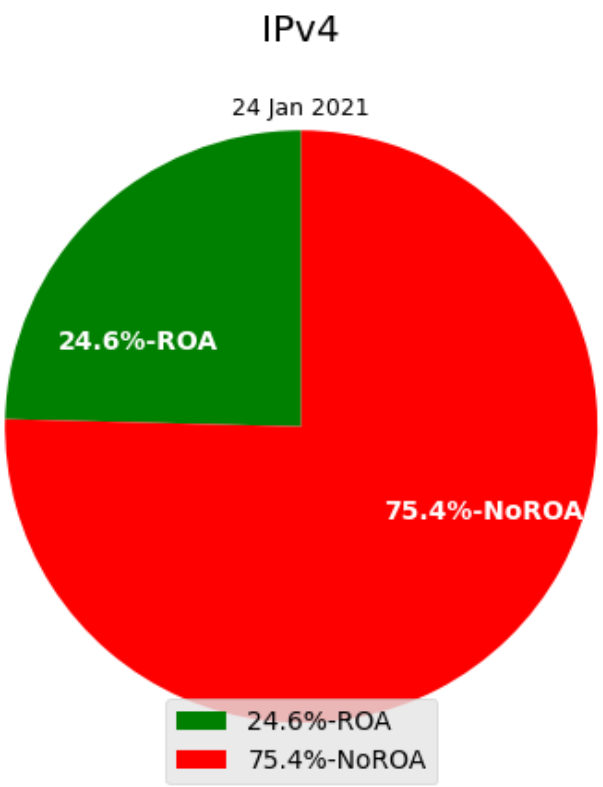


Digging Deeper

- One number is not enough...
- How about
  - IPv4 vs. IPv6?
  - Categories of the DNS Core?
    - Such as ccTLDs, gTLD, and reverse Map (RIRs)
- Or something else?

- A goal is to find "decision points"

IPv4 versus IPv6? (Note the difference in TLD counts)



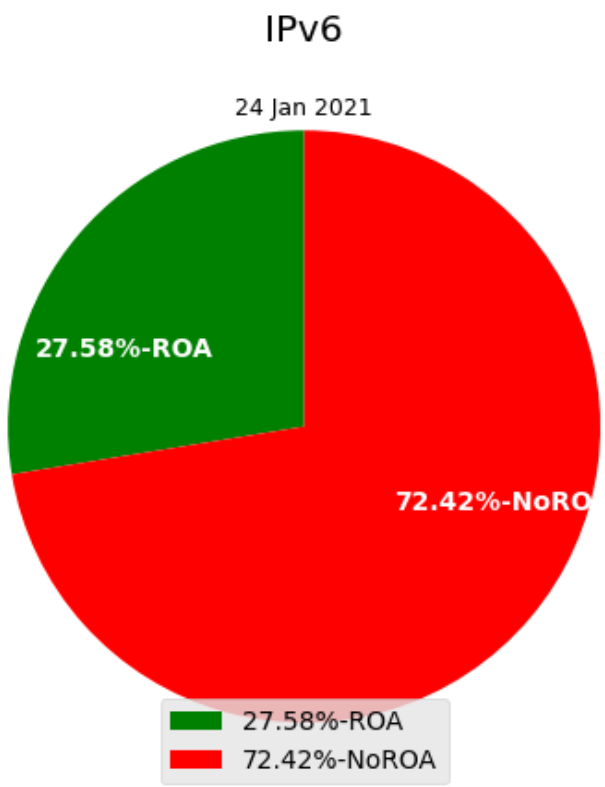
Zones(+ subTLDs): 3179

TLDs(+ revmap): 1774

Nameservers: 4434

Addresses: 3785

RouteOrigins: 1634



Zones(+ subTLDs): 3036

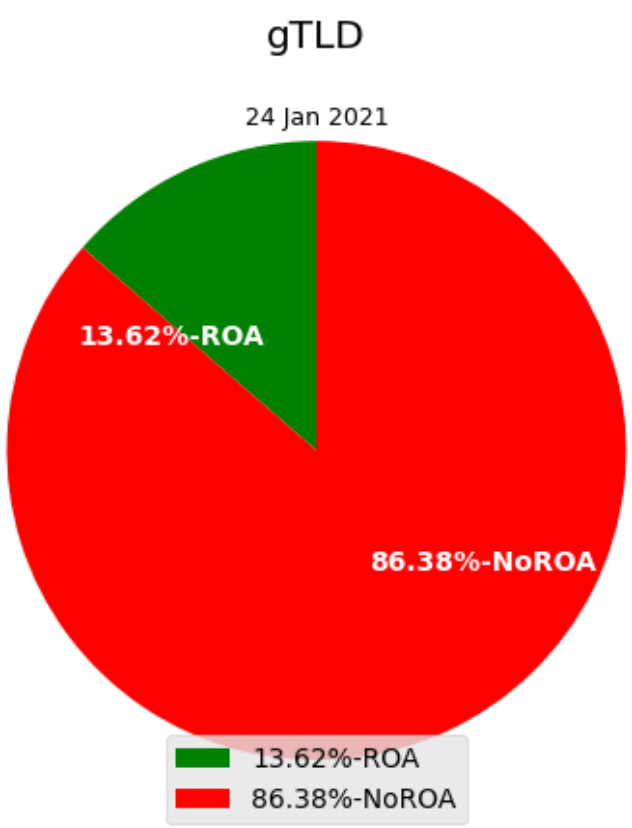
TLDs(+ revmap): 1753

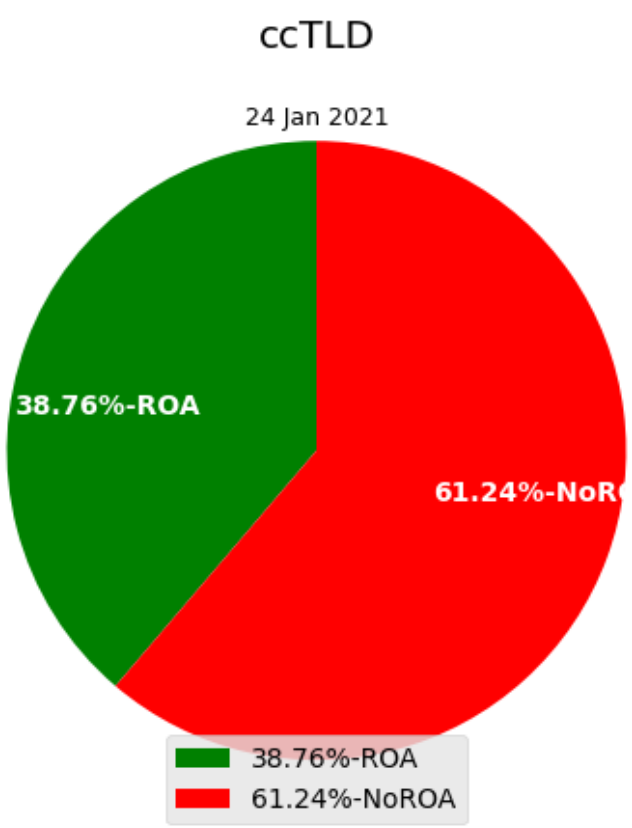
Nameservers: 3717

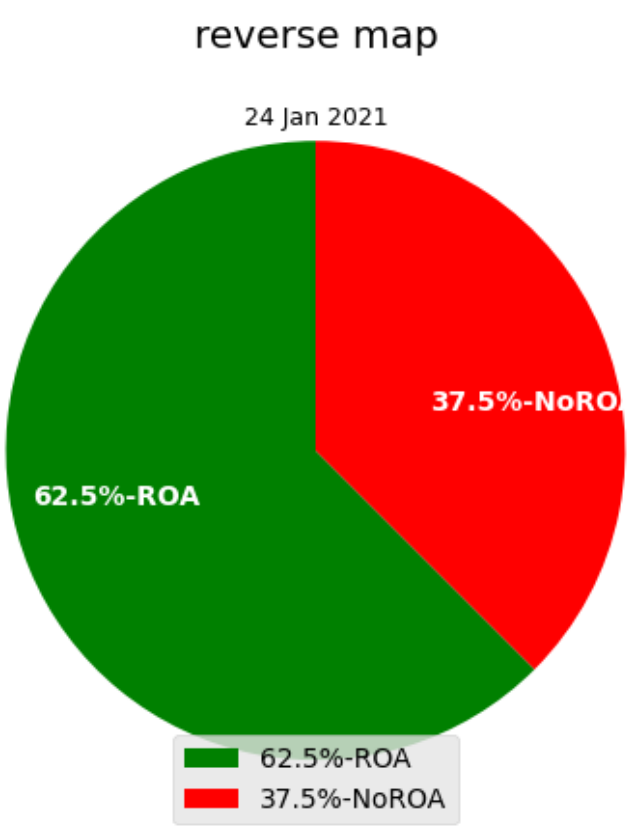
Addresses: 3330

RouteOrigins: 736

ccTLD / gTLD / Reverse Map





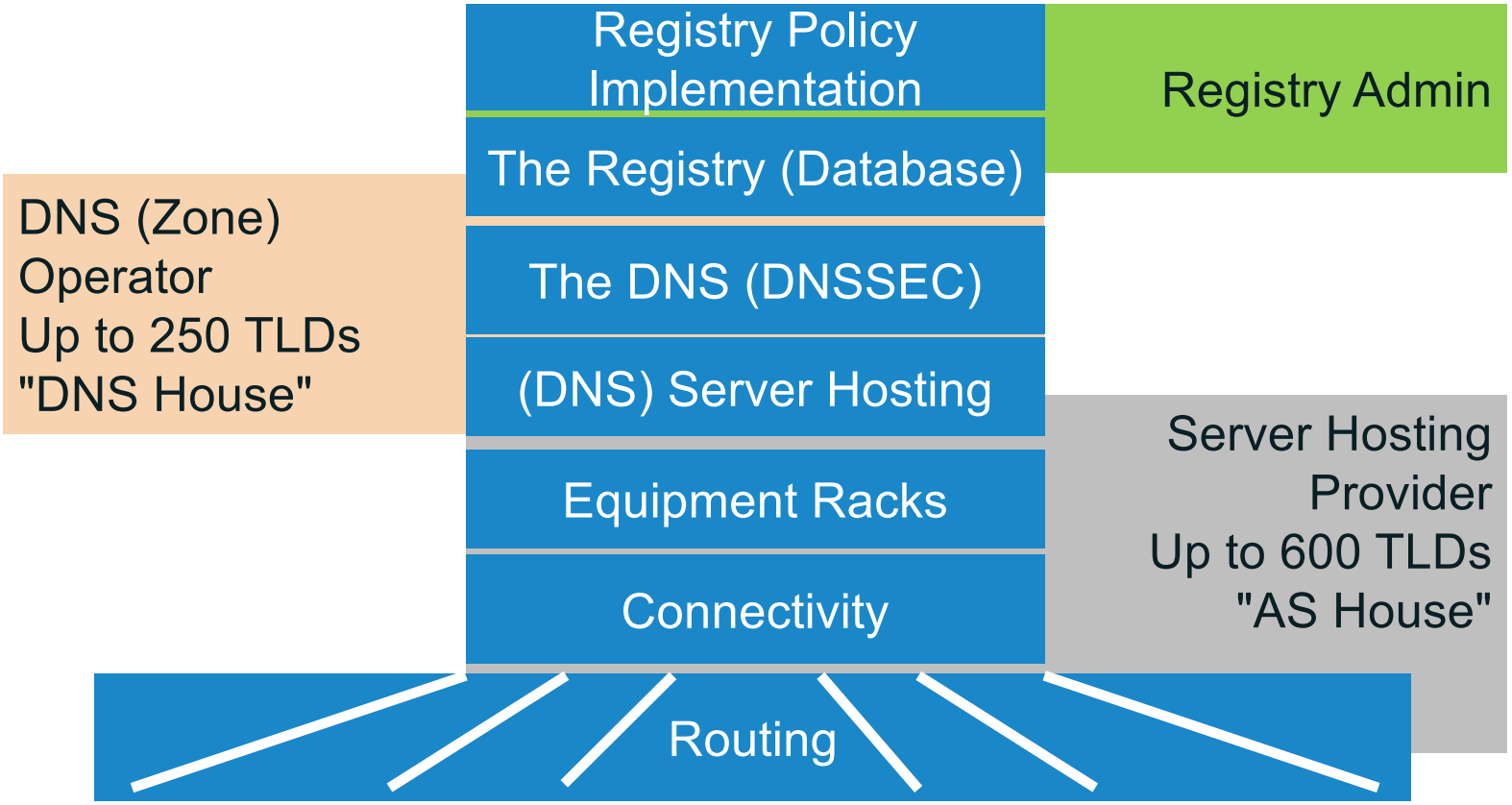


Looking for ROA Coverage Along Decision Points

- DNS Registries are highly layered
  - Many different configurations
  - Many different agreements (contracts)
  - Clusters of TLDs (gTLD/ccTLD/reverse map) share operating platforms

- Can the routing security policy decision points be discovered and examined?

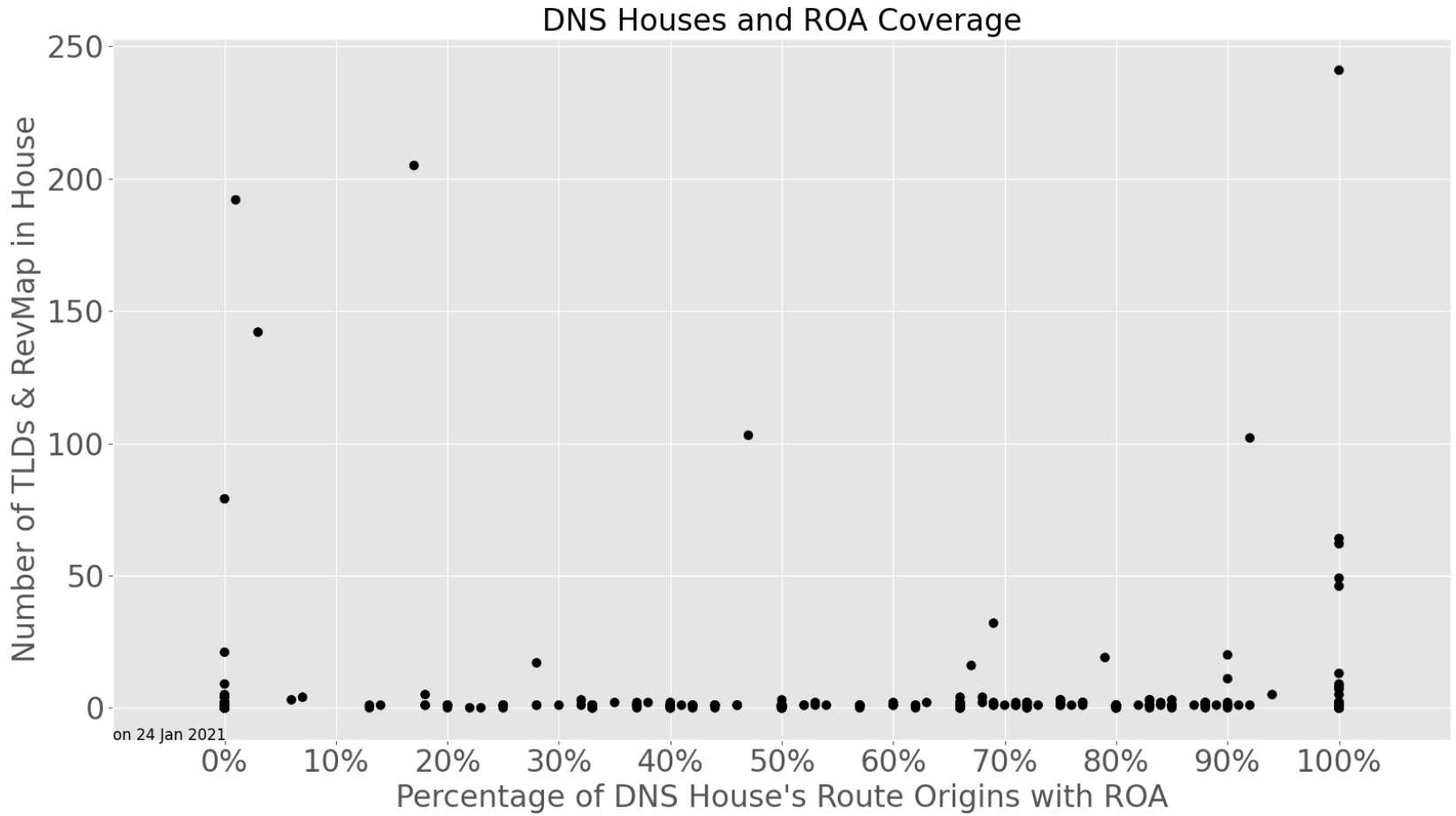
Registry Service Implementation Layers



DNS House

- Determined by
  - DNS SOA Resource Record "RNAME" field (R is for Responsible)
  - IANA function's DNS root registry *technical contact* field
- Using the contents of those fields, TLDs are bucketed
  - Highlighting one level of shared operating platforms
- There are a very few "large" houses (hundreds of TLDs) and many "single" houses (1 or 2 TLDs)

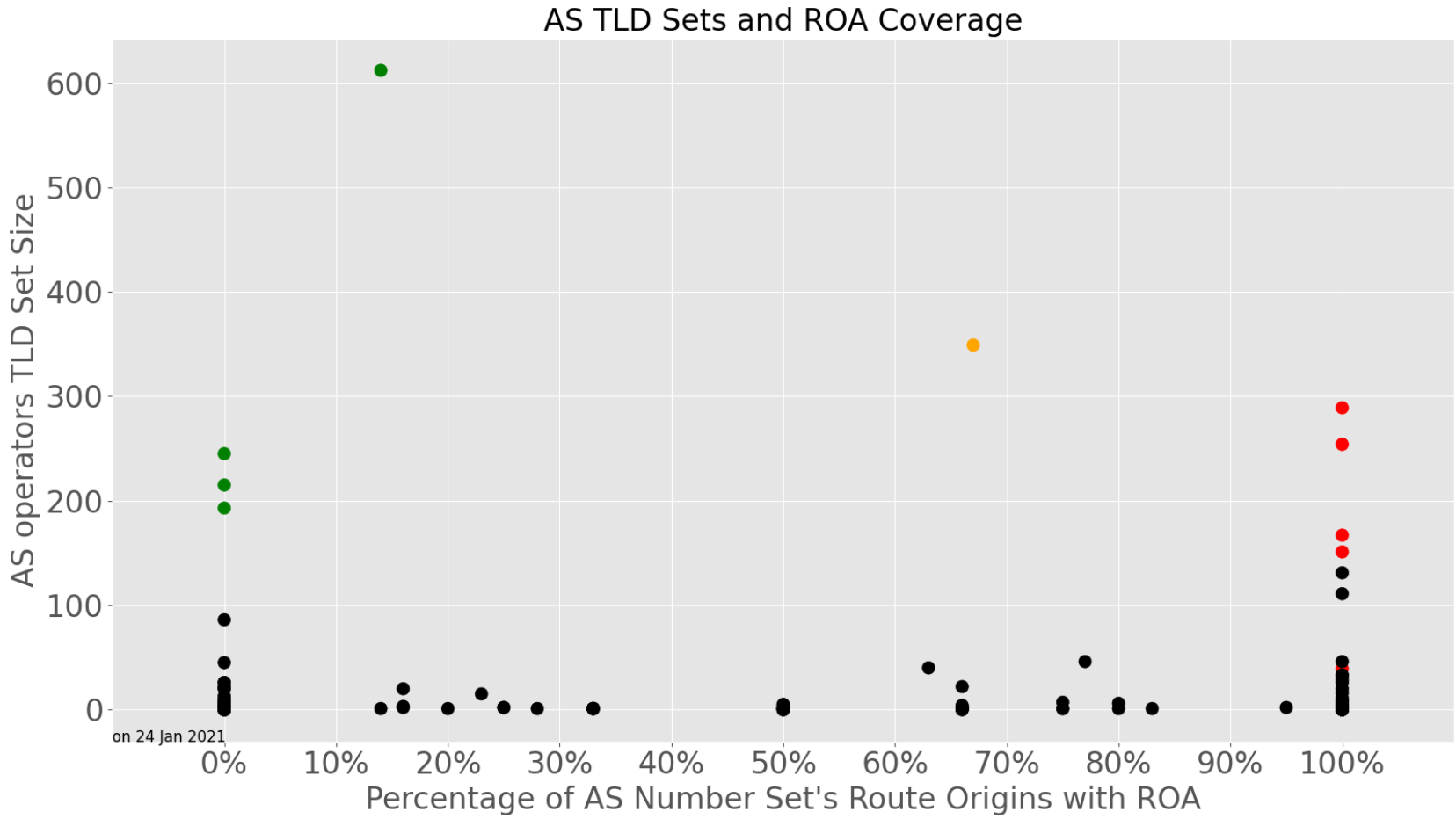
DNS House Chart



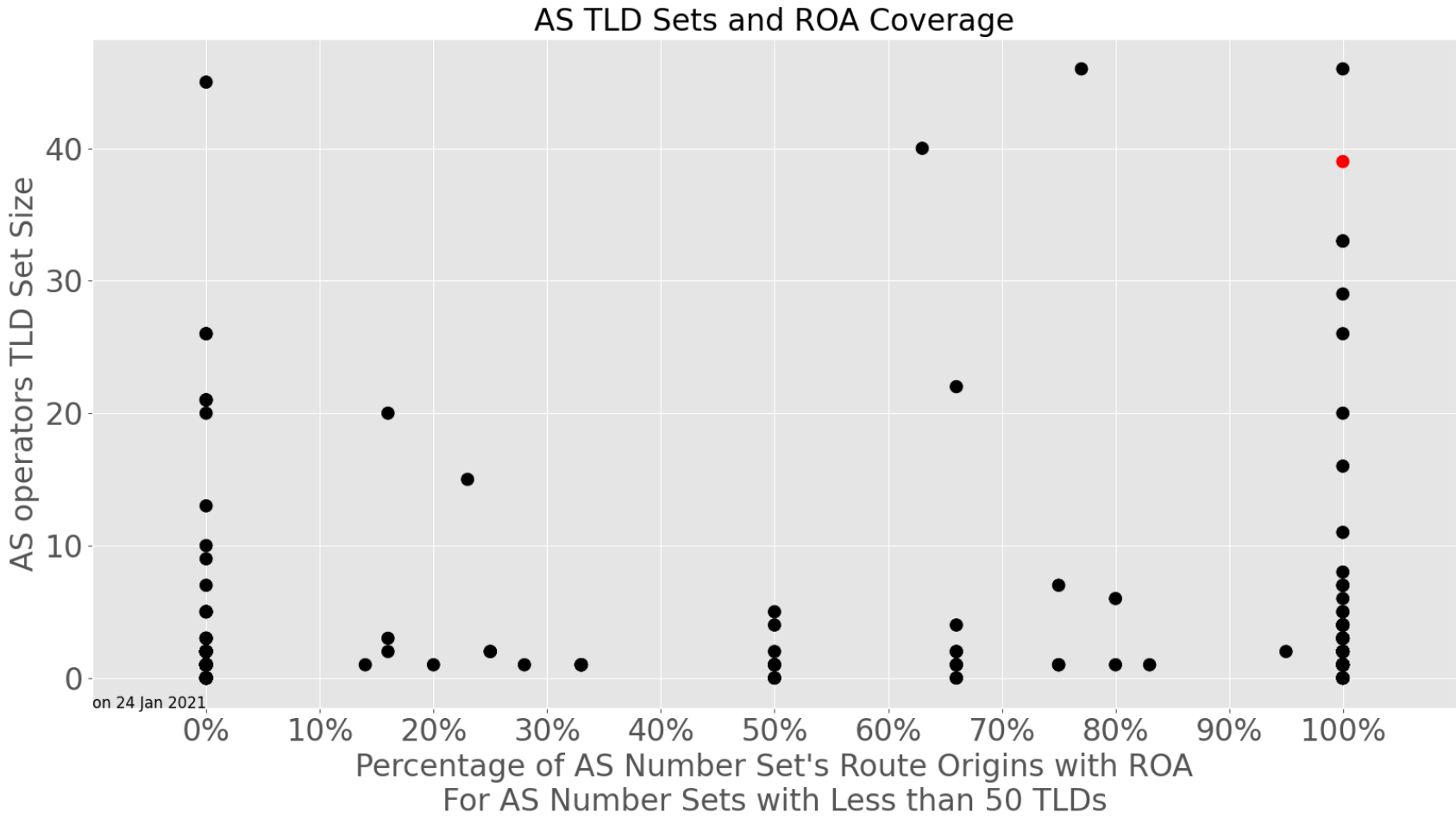
AS House

- More complicated/subjective
  - Shared "Network names"
  - Shared BGP prefixes
  - *Imaginative* parsing of the "Network names" and see what's shared
  - Other debatable rules
    - Such as - commonly serving the same, single zone
- Multiple AS numbers may be in one AS House
  - An AS House includes control over the routed address space
- A zone many be in multiple AS Houses

AS House Chart



AS House Chart for houses with < 50 TLDs served



Some Observations About ROA Deployment

- Overall deployment of ROAs is sparse in the DNS Core
- Judging from few data points, decisions related to deployment of ROA's rests with whomever is hosting the servers (the address space operators)
  - A routing thing and not a DNS thing

- The large, non-RIR hosters (AS Houses) have low deployment
- The large, RIR hosters (AS Houses) have high deployment

Concerns Related to Securing Critical Infrastructure

- There's inherent risk of adding security to an "in operations" system, especially if the system is depended upon by so much
  - While protecting routing is essential and would benefit the security of the DNS, if the protection backfires, there'll be chaos
- Given this observation, maybe it wouldn't be surprising to see deployment "go slow"
  - Are there mitigations to apply?

Contrasting with DNSSEC

- DNSSEC is another a post-operational-phase security mechanism significant in the DNS Core
  - Risking operational stability of an insecure system by imposing security mechanisms is shared by DNSSEC and RPKI/ROA
  - Adoption of DNSSEC has taken a very long time, it has grown only to perhaps "respectable"/"visible" after two decades
  - Currently DNSSEC sees a different adoption pattern (within the DNS Core)
    - Large operators have deployed, what remains are single-(cc)TLD operators

RPKI/ROAs: ready for deployment?

- I'm going to explicitly duck this question
  - I'm not an operator, I won't speak on behalf of the operations community
- If deployment ought to progress, what needs to be done to advance deployment?
  - This is a good question, again, I'll duck...

Wrap Up

- This work merely checks the "temperature of the room"
  - Rhetorical: Is 25% acceptable for now?
  - Are there possible improvements to RPKI and ROA to gain acceptance?
  - Is it a business case issue?

- Relying on my experience with DNSSEC adoption from 1998:
  - Slow adoption has advantages – outages have limited impact and "pioneers" are quick to address operational problems
  - Gaps exist and are filled with more to go
  - The value proposition may change over time

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: edward.lewis@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg