Measuring ROA deployment at the top of the DNS

Or, Taking a Simple Number and Really, Really, Really, Over Thinking It

Edward Lewis

RIPE WG Interim Session
9 December 2020

Origin of This Work

- CENTR Jamboree 2019
  - Job Snijders on the agenda to talk to Registry Operators
  - The Topic: RPKI for ccTLD Peers
    - Why the ccTLDs ought to validate routing information
  - Expected a talk on how RPKI could protect routes to name servers
    - So, I began to work on a talk related to that (route information signing)

Setting Expectations

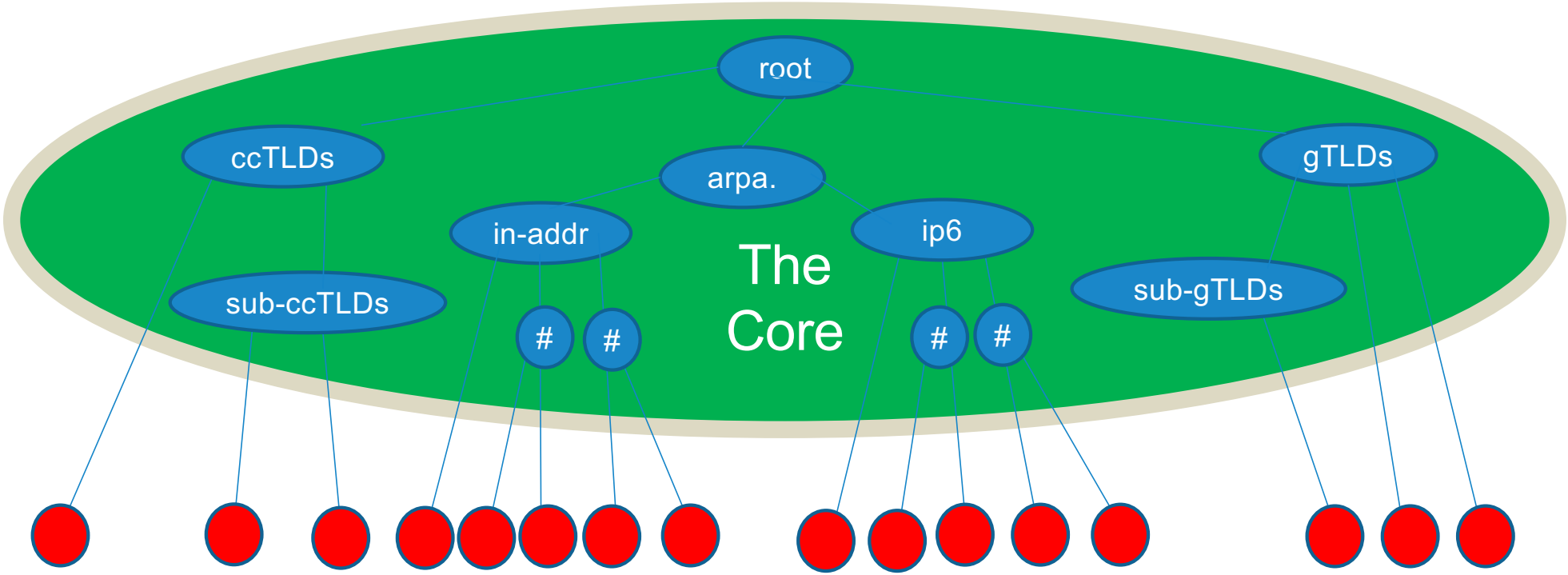
- The central theme of this talk is the methodology
  - What is covered in the assessment
  - How the experiment space is divided
- There's not much detail on RPKI and ROA's progress
  - Not enough time has elapsed to see penetration
  - No consideration of whether obstacles exist

Measuring ROA Deployment in the DNS Core

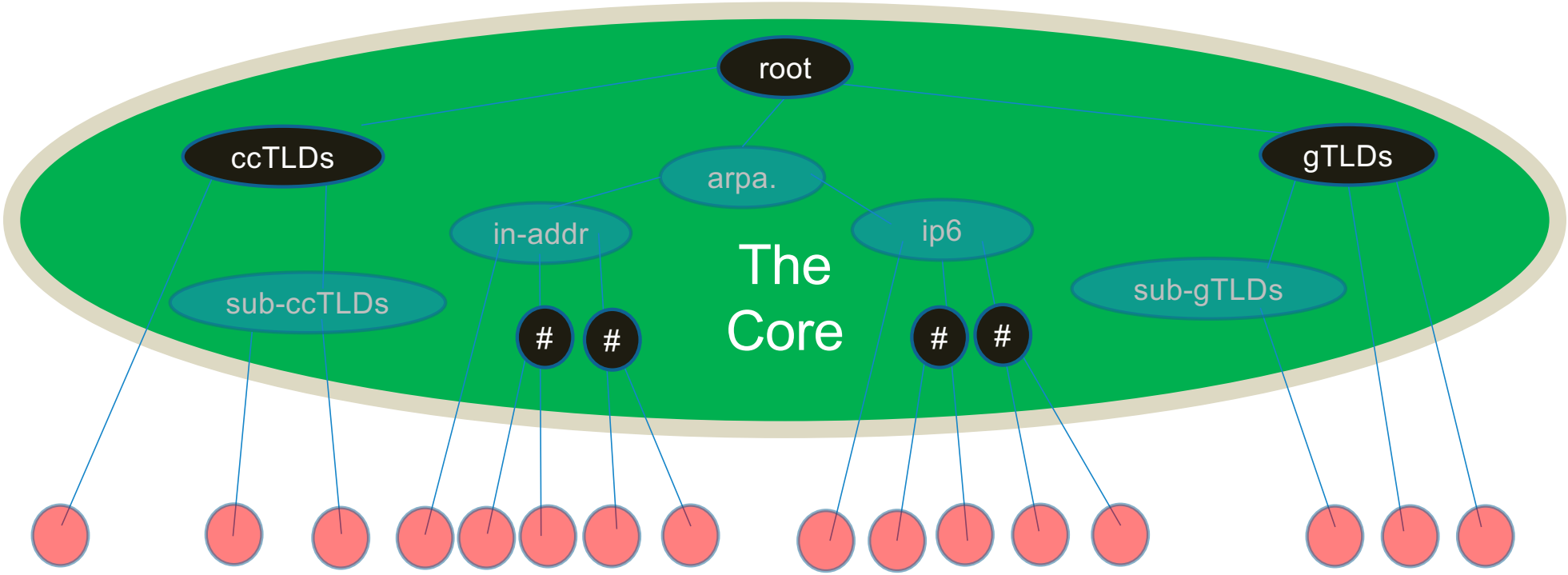
- This talk is not promoting "ROA adoption", just measuring it
  - An application/service-specific look at adoption
    - The DNS service, particularly the authoritative core

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

The DNS Core (in Cartoon Form)



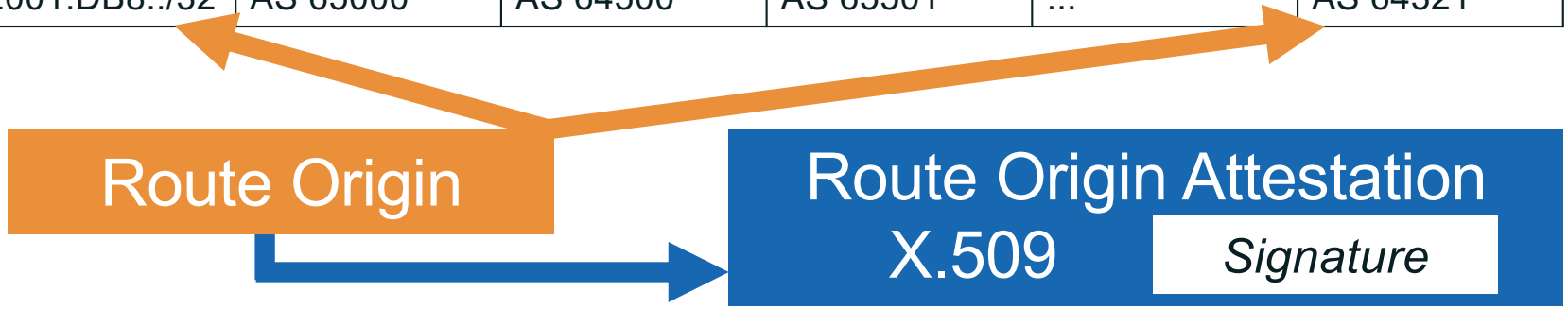
I May "Slip Up" and talk about TLDs this way in the talk



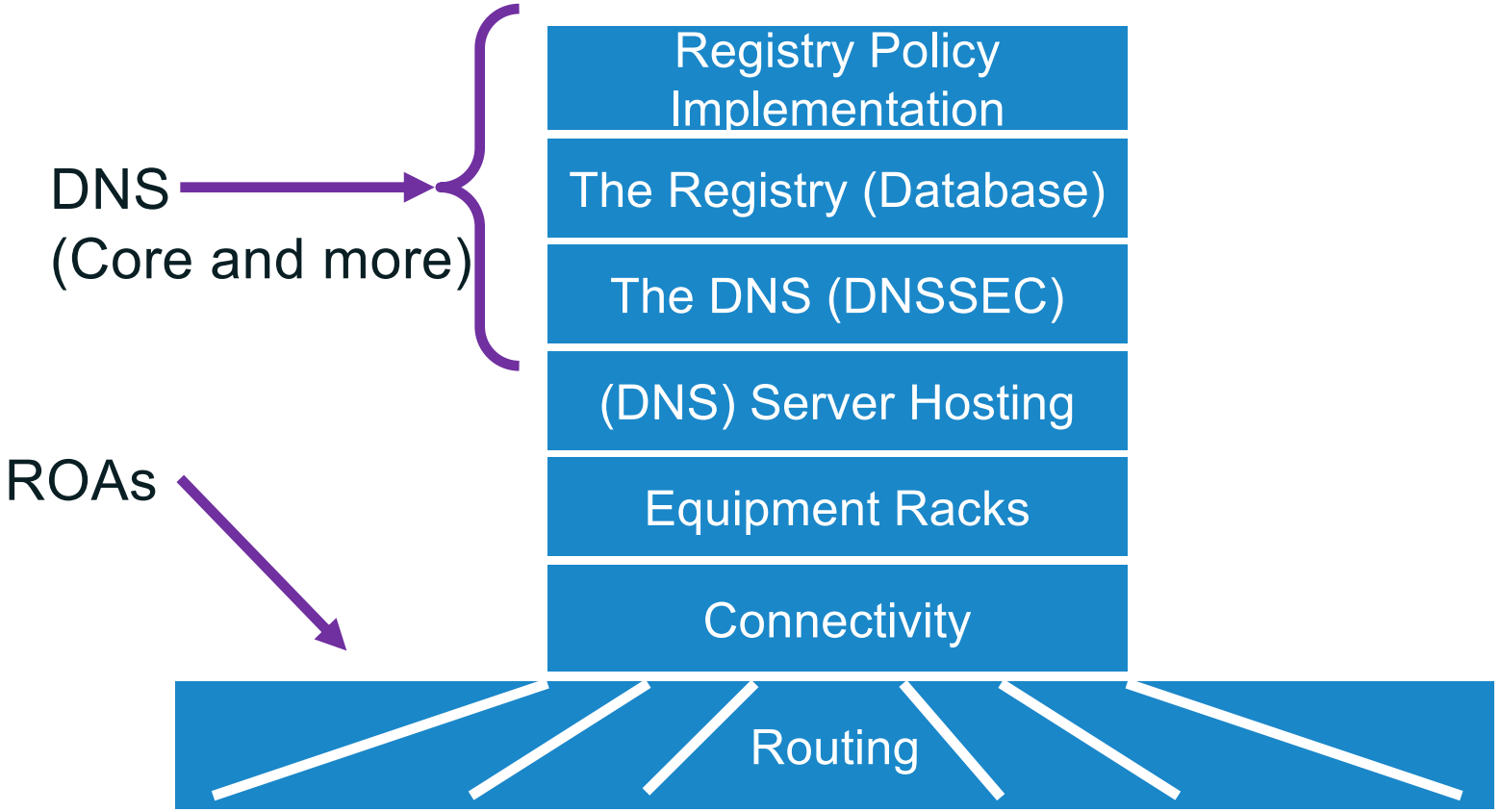
ROAs = Route Origination Authorization

- 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



The DNS Core Versus ROAs



Relationship of RPKI, ROAs and DNSSEC

- DNSSEC is a set of extensions assisting security of DNS
  - Allows recipient to verify that data received is genuine
  - Does not guarantee a response is delivered
- RPKI and ROA are meta-data about routes
  - Allows recipient of a BGP route advertisement to assess validity
  - Does not guarantee data arrives
- The intersection for DNS registries
  - DNSSEC helps protect responses, routing security helps protect queries

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"

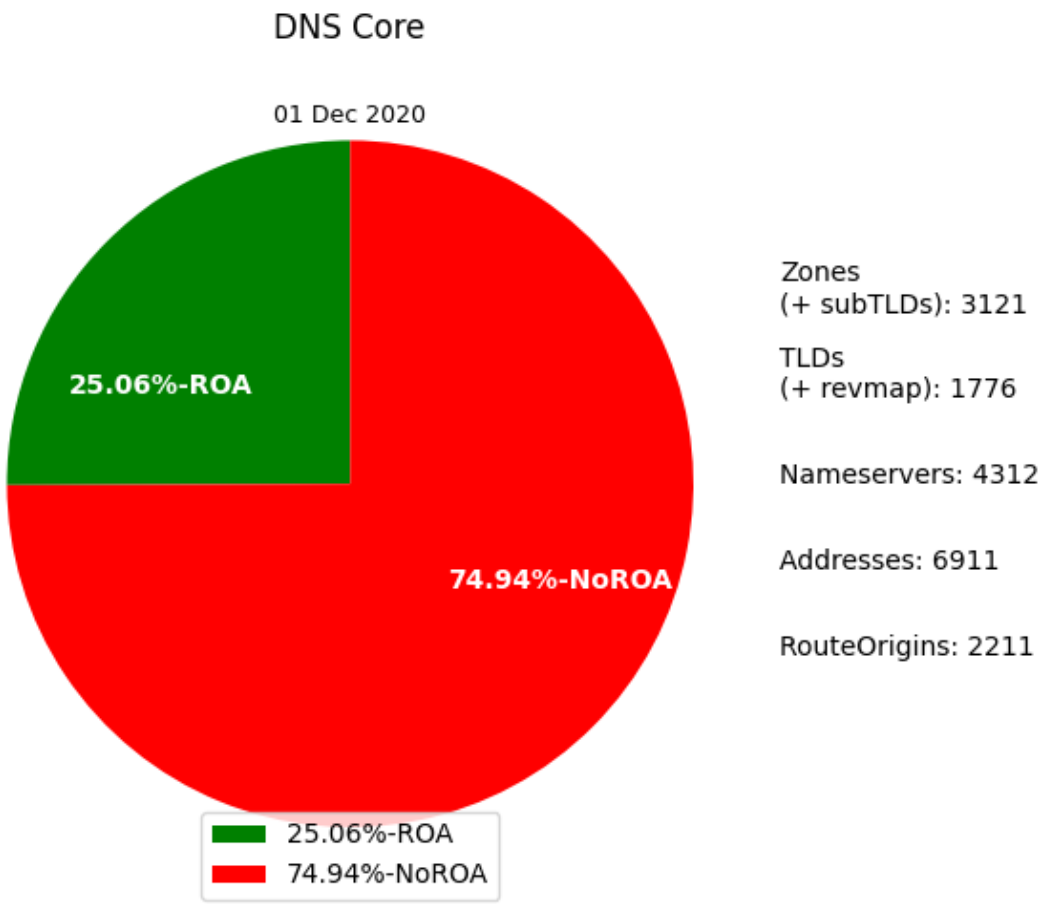
- Is there a pattern to the deployment?
  - Where should efforts to increase adoption be focused?
  - Where would studies discover needed improvement?

Measurement Method

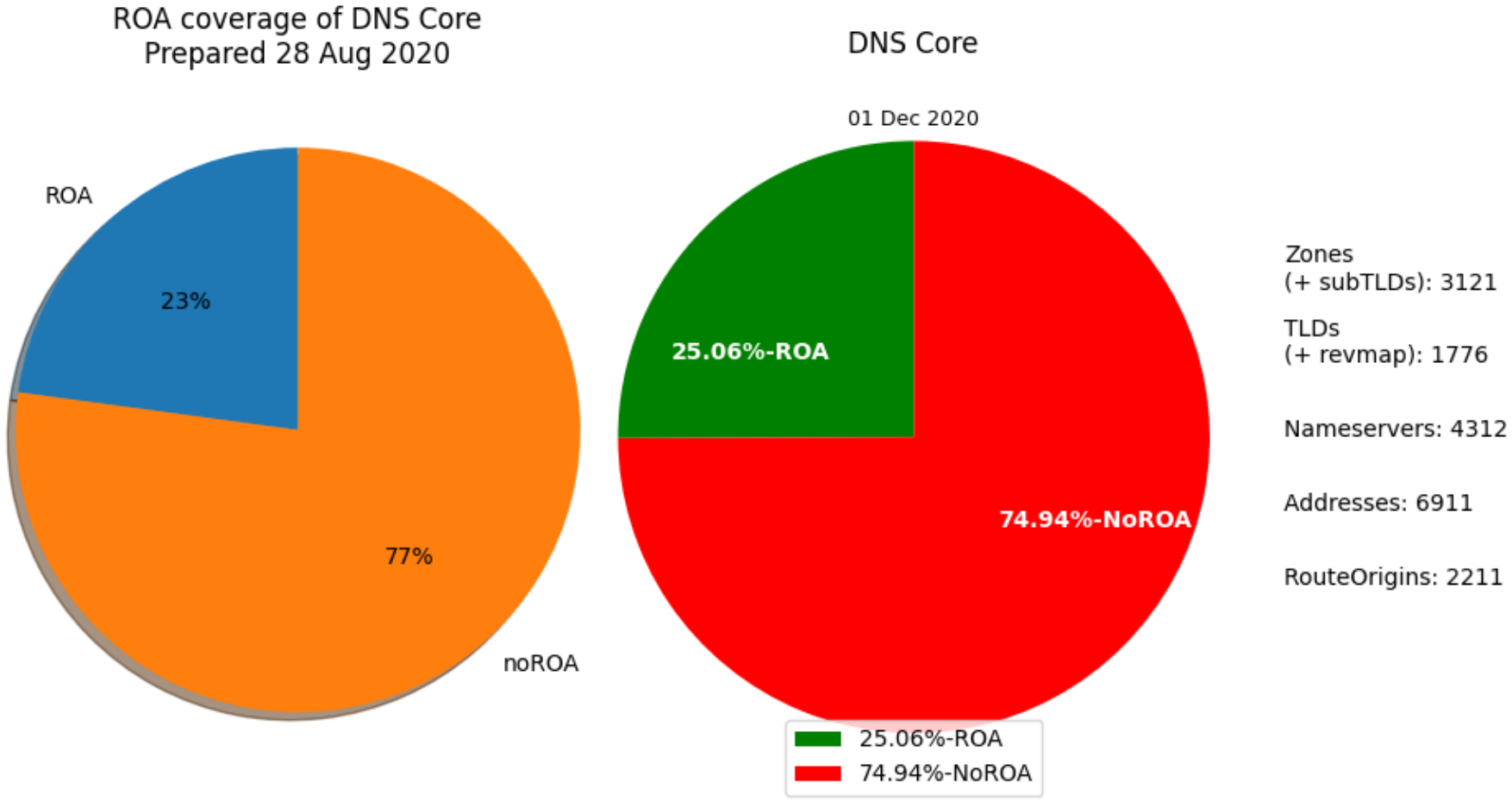
- Use a census (listing) of the the DNS core
- Looked at
  - zones
    - nameservers
      - addresses
        - route originations
  - Relying on Team Cymru's *IP to ASN mapping service*

- Does the route origination have a *validated-by-RIPE* ROA?
  - Yes or No, percentages are `"Yes"/("Yes"+"No")`

Overall ROA Coverage (Now = 1 December 2020)



Overall ROA Coverage (~3 months to now)

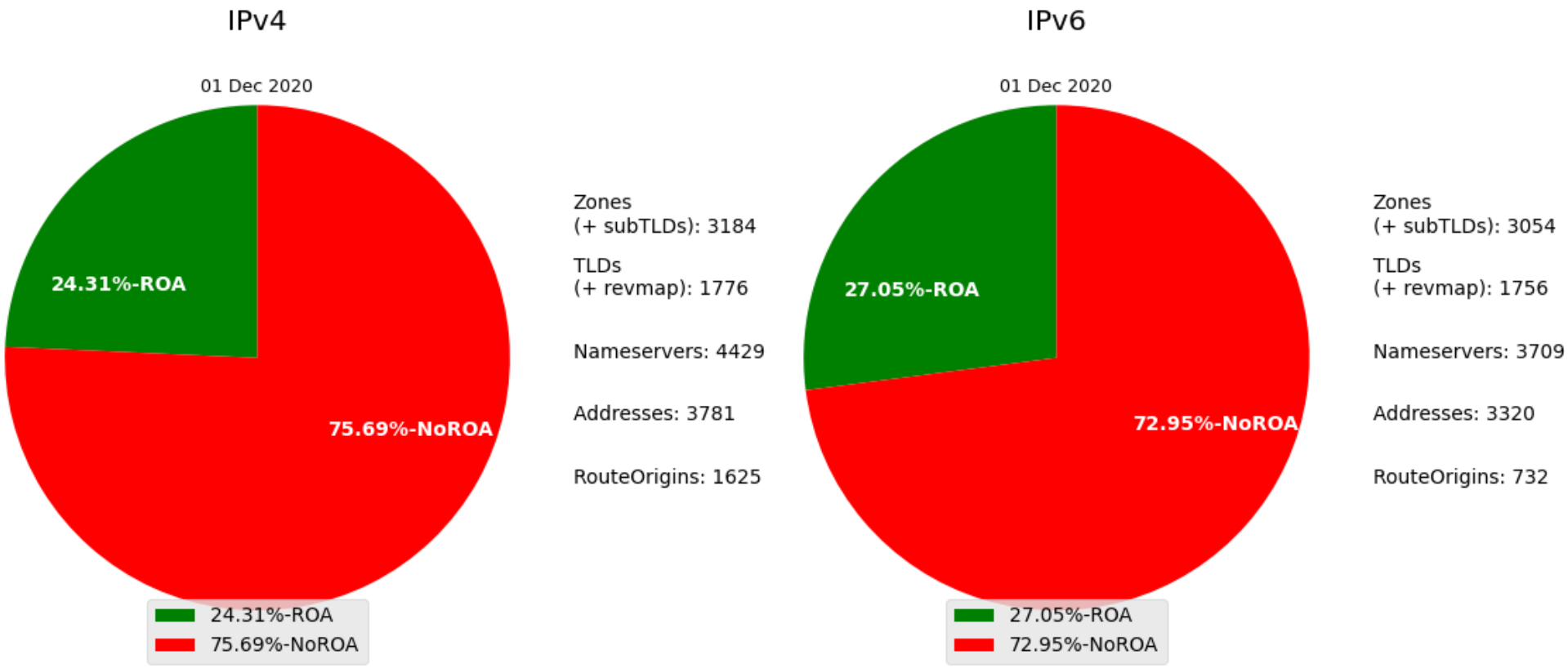


Digging Deeper

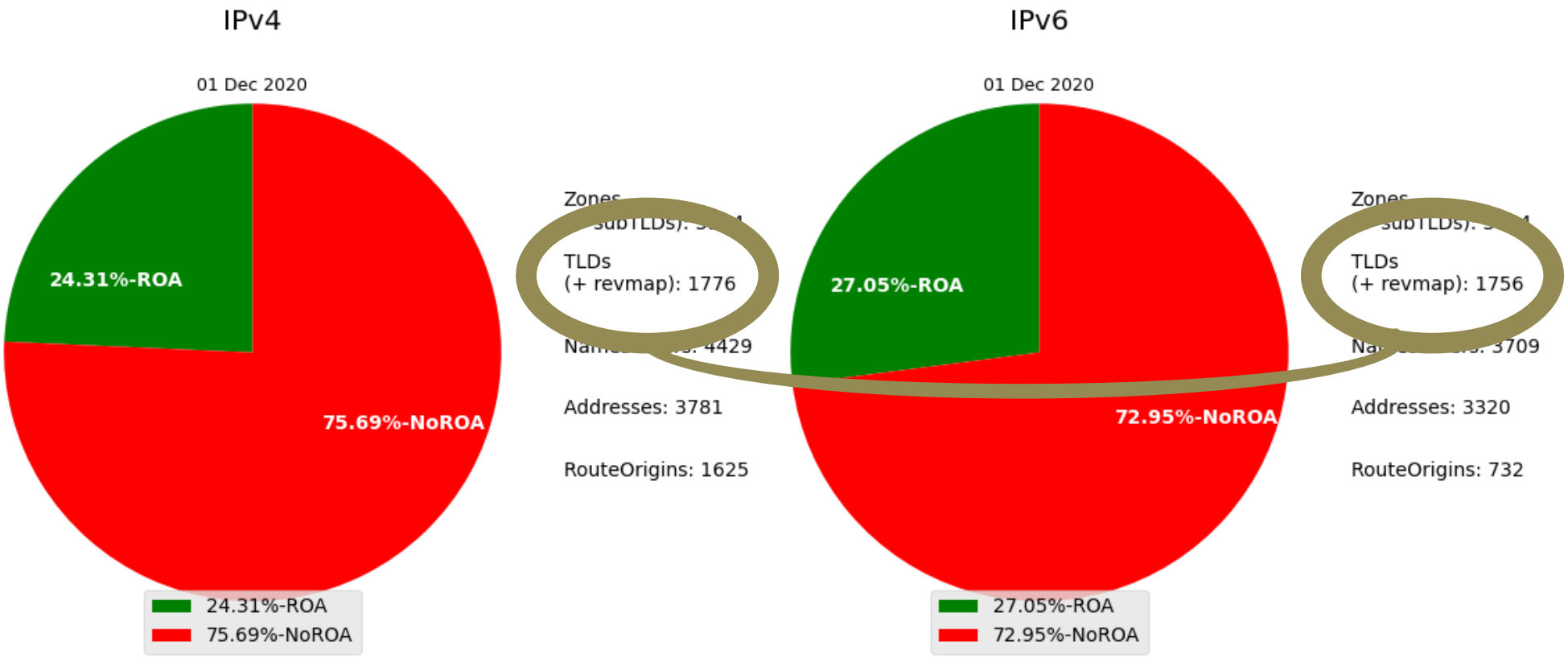
- One number is not enough...
- How about
  - IPv4 vs. IPv6?
  - Categories of the DNS Core?
    - Such as ccTLDs, gTLD, and reverse Map (RIRs)
- Or something else?

- A goal is to find "decision points"

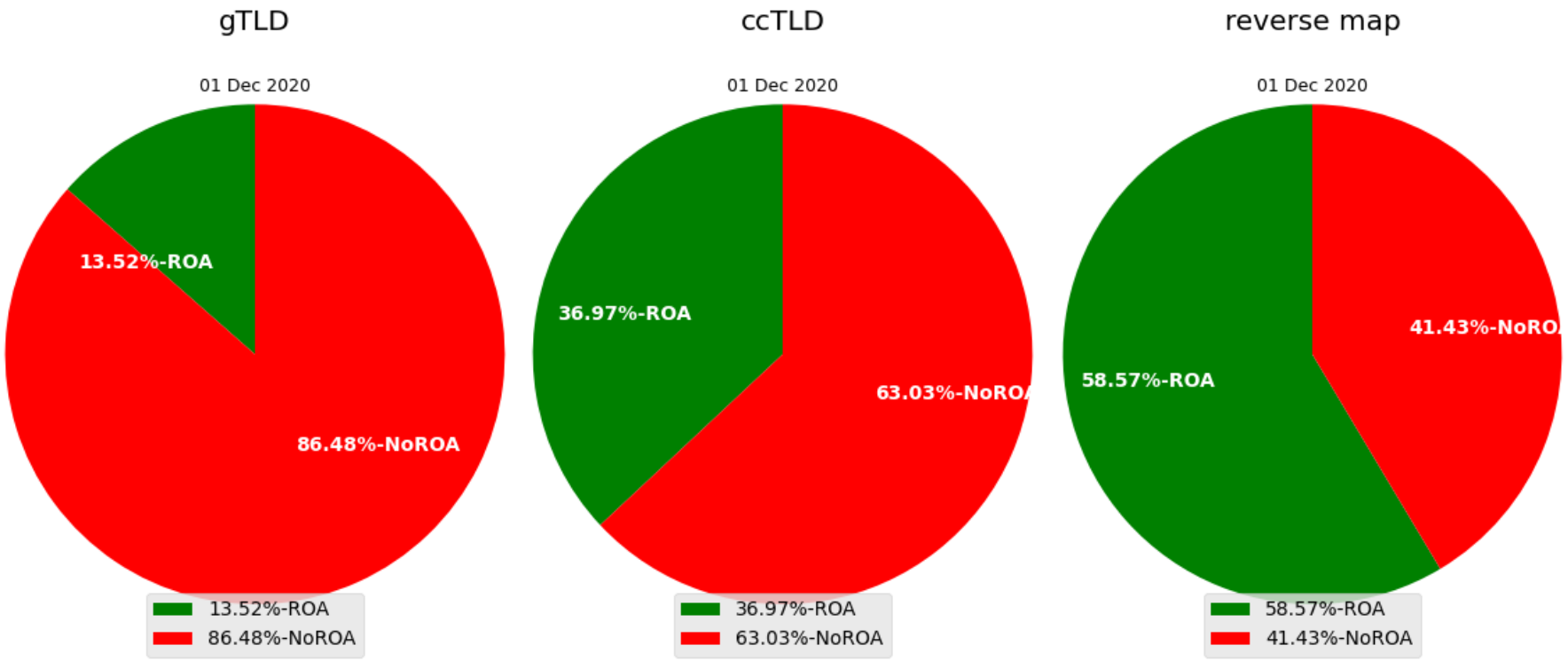
IPv4 versus IPv6?



IPv4 versus IPv6 – What, 20 TLDs fewer in IPv6?



ccTLD / gTLD / Reverse Map



Very Different Results

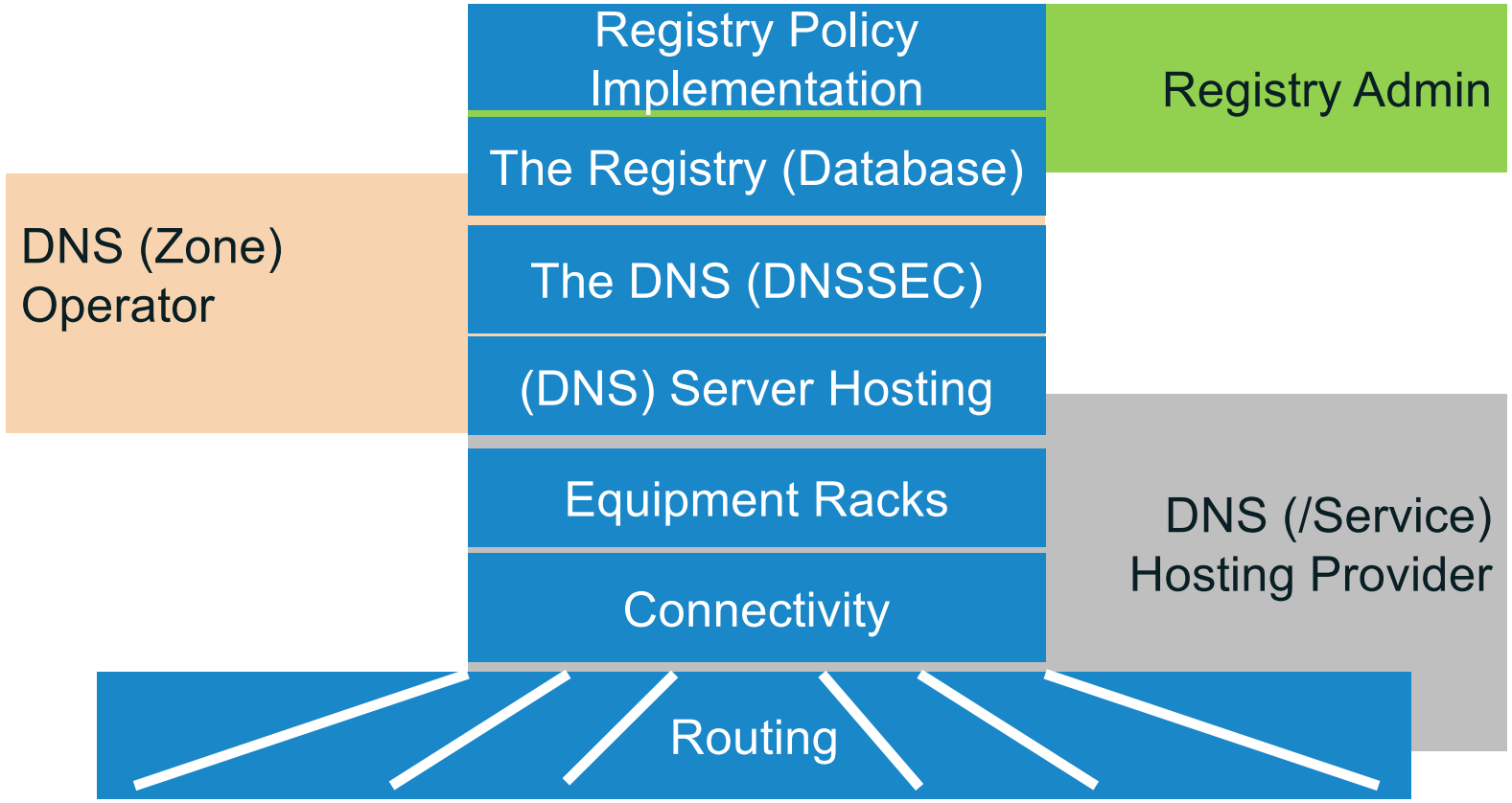
- Does this show a "true" divide?
  - Some gTLD and ccTLD operations overlap (same operators, same platforms)
  - What role does scale-of-operations play? Many TLDs are jointly operated in one way or another
- The RIR adoption rate seems low against expectations
  - Digging deeper, a lot of the "lowness" can be attributed to one server's IPv4 address and the numerous, un-ROA'd anycast origins it has
  - This hints that there is some "substructure" that begs investigation

Looking for ROA Coverage Along Decision Points

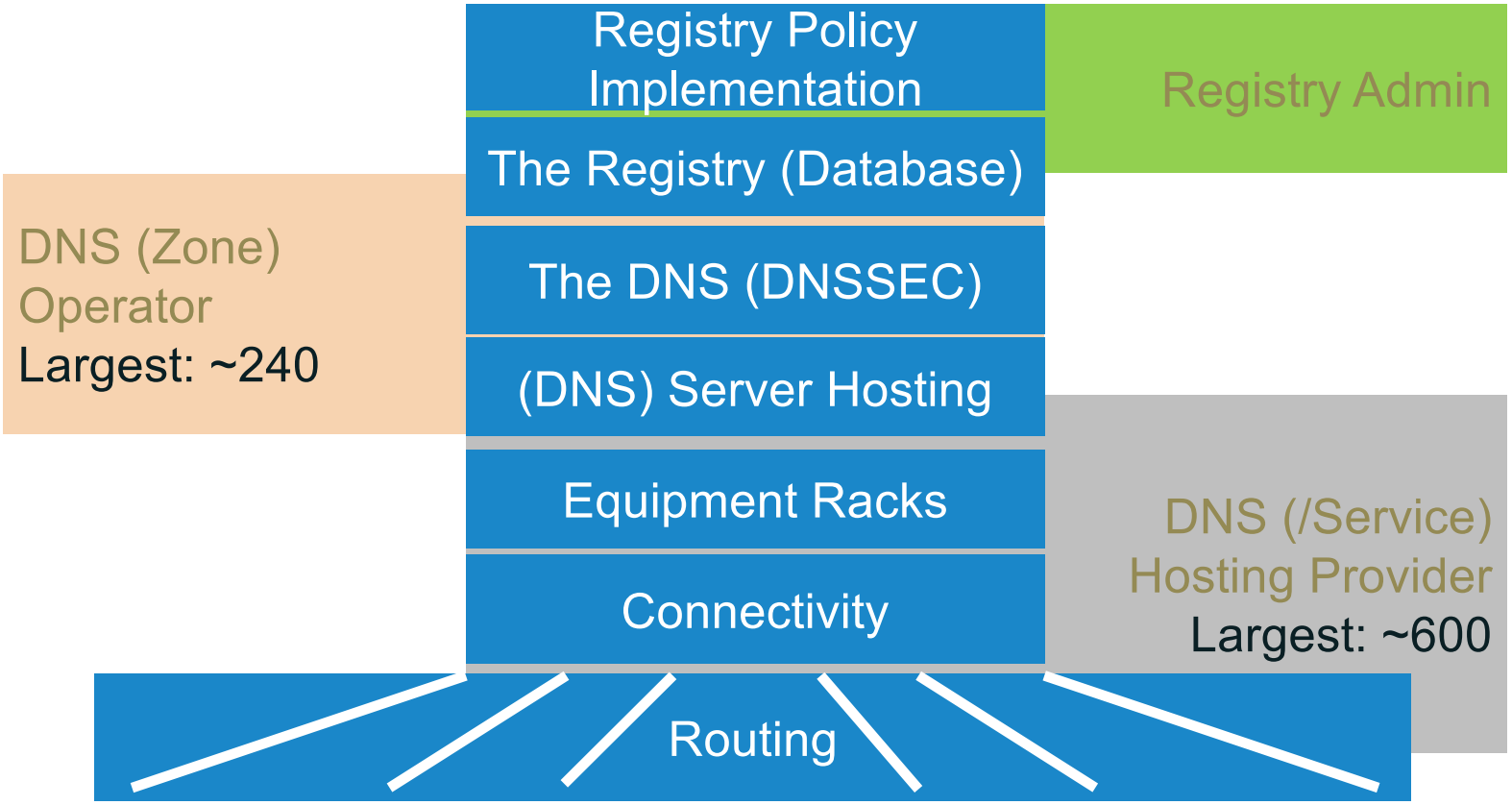
- DNS Registries are highly layered
  - Many different configurations
  - Many different agreements (contracts)

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

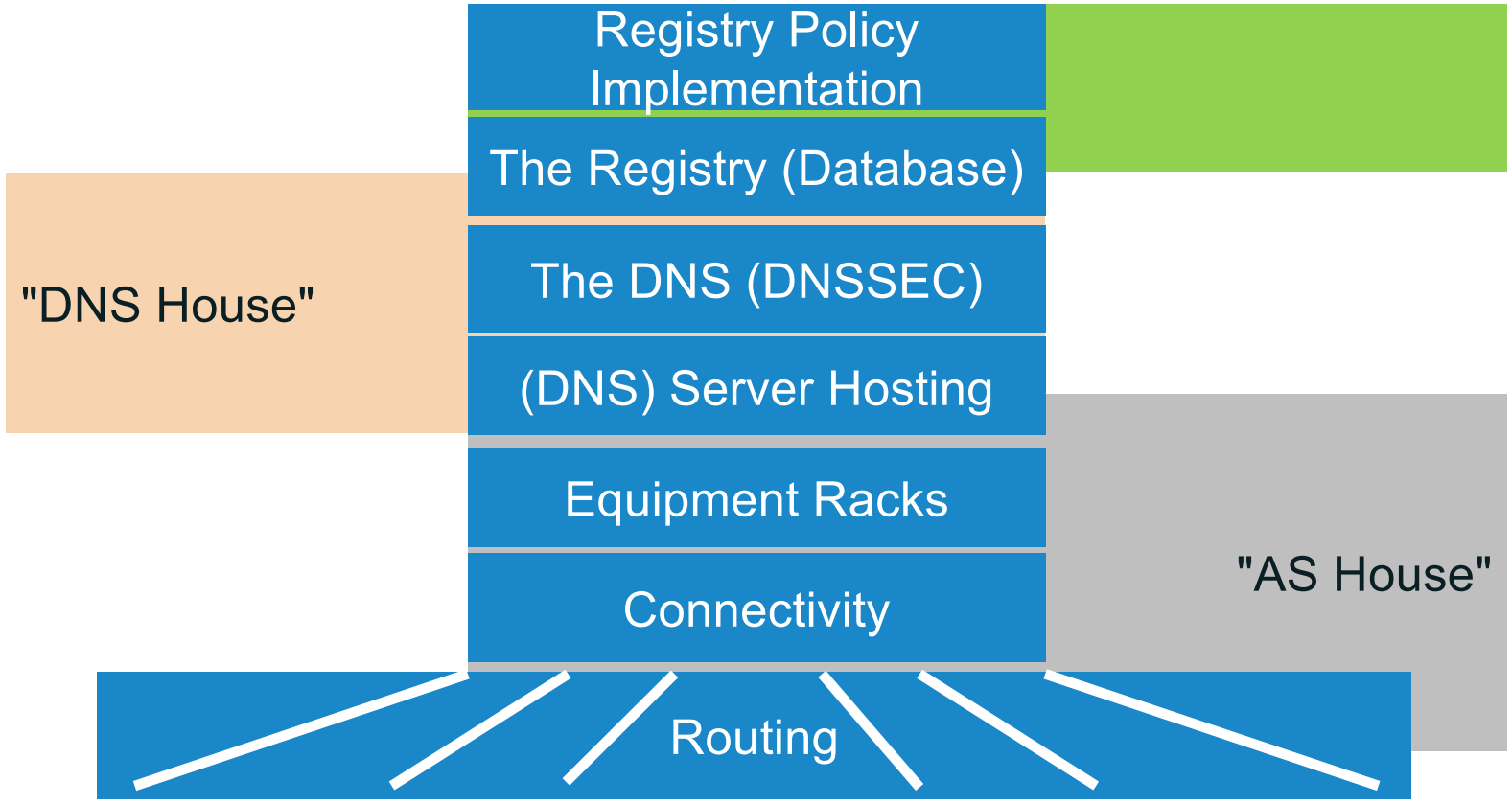
Registry Service Implementation Layers



Registry Service Implementation Layers



Registry Service Implementation Layers



Motivation

- Why try to discover, define, or quantify these "houses"?
  - Discard this: finding "Market Shares"
    - Not a goal, besides, this work is not sufficiently accurate
  - Protocol "Health" and "Deployment Progress"
    - To capture how many decision makers have adopted a protocol (feature)
    - To capture "operator demographics" related to decisions to go/no go
    - To capture, over time, growth milestones
  - Discover leading practices
    - What do operators do?
  - Find places where deeper study could be interesting

DNS House

- DNS SOA Resource Record "RNAME" field
  - Many backend operators use a common RNAME field
- IANA registry Technical Contact
  - A few use custom RNAME fields, but same Tech Contact

- Using the contents of those two fields, find all TLDs that fall into "buckets" based on those

DNS House Table (Part of it)

TLD/Rev	ccTLDs	gTLDs	revMap	House
241	0	241	0	hostmaster.donuts.co.
206	3	203	0	hostmaster.neustar.biz./support.ariservices.com.
193	13	180	0	noc.afilias-nst.info.
150	2	148	0	info.verisign-grs.com./nstld.verisign-grs.com.
103	0	0	103	dns-ops.arin.net.
94	6	88	0	hostmaster.centralnic.net.
79	0	79	0	hostmaster.nominet.org.uk.
64	0	0	64	dns.ripe.net.
62	0	0	62	read-txt-record-of-zone-first-dns-admin.apnic.net.
49	0	49	0	noc.gmoregistry.net.
46	0	46	0	cloud-dns-hostmaster.google.com.
32	1	31	0	regops.uniregistry.link./ops.uniregistry.net.
21	0	21	0	td_dns_gtld.knet.cn.
20	0	20	0	dnsmaster.corenic.org.
19	6	13	0	A.F.N.I.C.
...				
5	1	3	1	JAPAN REGISTRY SERVICES CO. LTD.
...				

AS House

- More complicated/subjective because autonomous systems are routing objects, not DNS objects
  - Shared "Network names"
  - Shared BGP prefixes
  - *Imaginative* parsing of the "Network names" and see what's shared
  - Other debatable rules
    - Commonly serving the same, single zone
- Multiple AS numbers may be in one AS House

AS House Table (Part of it)

TLD/rev	Operator	Autnum(s)
615	{'ULTRADNS, US'}...	{'397242', '397235', '397233', '397215', '397232...
348	{'WOODYNET-1, US...	{'42'}...
288	{'RIPE-NCC-AUTHD...	{'197000'}...
254	{'ARIN-PFS-ANYCA...	{'53535', '393225'}...
247	{'VGRS-AC25, US'...	{'396574', '397209', '397198', '396547', '396546...
216	{'AS-AFILIAS1, U...	{'12041', '207266'}...
167	{'APNIC-ANYCAST-...	{'18368', '18366', '18369'}...
151	{'LACNIC - Latin...	{'28001', '52224'}...
131	{'NETNOD-NDS $Id...	{'56908', '39840', '39871', '8674'}...
119	{'NEUSTAR-AS6, U...	{'19905'}...
108	{'CENTRALNIC-ANY...	{'201303', '199330', '60890', '201304'}...
84	{'NOMINETANYCAST...	{'43519', '137502'}...
46	{'YOUTUBE YOUTUB...	{'43515'}...
46	{'GOOGLE, US'} ...	{'15169'}...
44	{'CIRA-REGISTRY,...	{'55195', '394354'}...
40	{'NIC-FR-SITES-S...	{'2486', '2484', '2485'}...
39	{'AFRINIC-ANYCAS...	{'37177', '37181', '33764'}...
33	{'KNIPPWORLDWI, ...	{'50611', '8561', '8391', '48519'}...
32	{'UNIREGISTRY-AN...	{'62831', '63363'}...

AS House "concept" is not completely settled

- The idea of AS Houses is just a few weeks old, far from "tried and tested" or discussed

- E.g., for a small collection of Autonomous Systems, all serving a single, same TLD, should they be considered acting-as-one?
  - These cases may have very different registered network names, possibly from being "contracted hosting services" but are run by the administration staff
  - It is not necessarily clear yet how to classify these

The Houses versus Changes in the Business

- Early in 2020, one company operating a large (TLD-count) registry back-end operator sold the unit to another company
  - People we know have changed business cards and email addresses
  - But this is not evident in the development of the DNS Houses
    - Back end transitions take time

- Some transitions have been seen
  - Sometimes the RNAME and the Technical Contact are changed at different times, resulting in "interesting" changes in the houses
  - A reminder: the houses are "heuristically" determined by the data

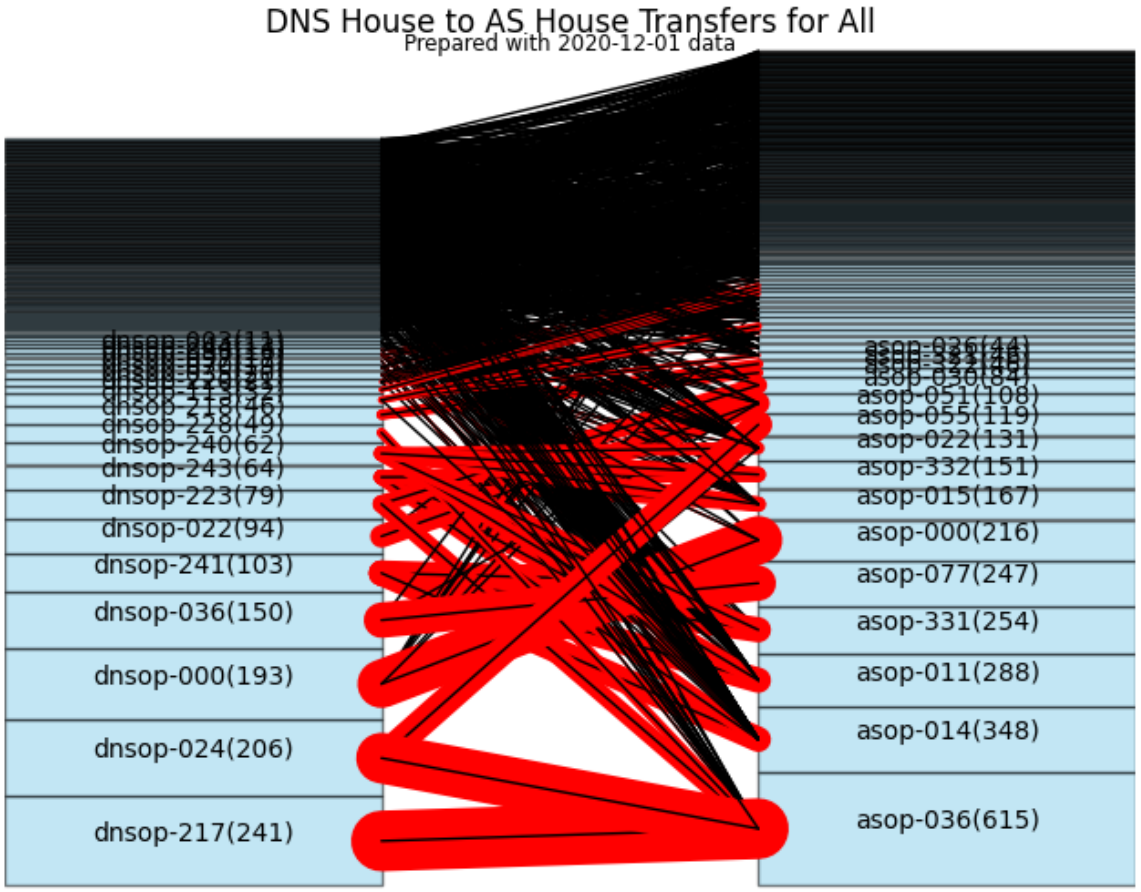
DNS Houses versus AS Houses

- A TLD can only be in one DNS House
  - Summing the TLD column adds to the number of TLDs
- A TLD can be in multiple AS Houses
  - Summing the TLD column will be greater than the TLDs

- A company may operate both a DNS House (or DNS Houses) and a AS House (or AS Houses)
  - Some may run everything "in house"

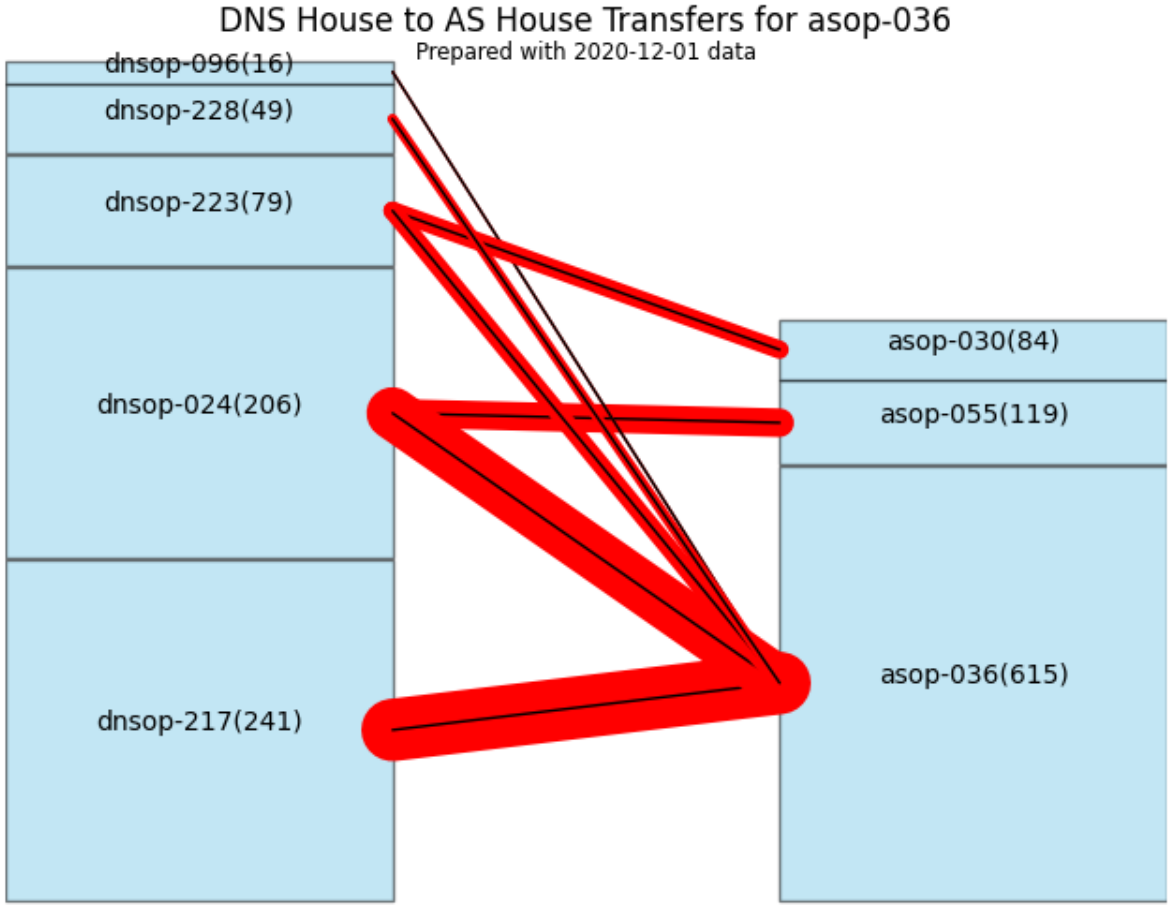
All DNS Houses feeding All AS Houses

- Left Column
  - DNS Houses Stacked
  - Box size proportional to TLDs
  - Names "masked"
- Right Column
  - AS Houses Stacked
  - Box size proportional to TLDs
  - Names "masked"
- Black Lines
  - 1+ TLD sent from DNS to AS house
  - The "long tail"
- Red Lines
  - Proportional to number of TLDs sent; high-volume visible
- Names are masked
  - TLD Count in parenthesis



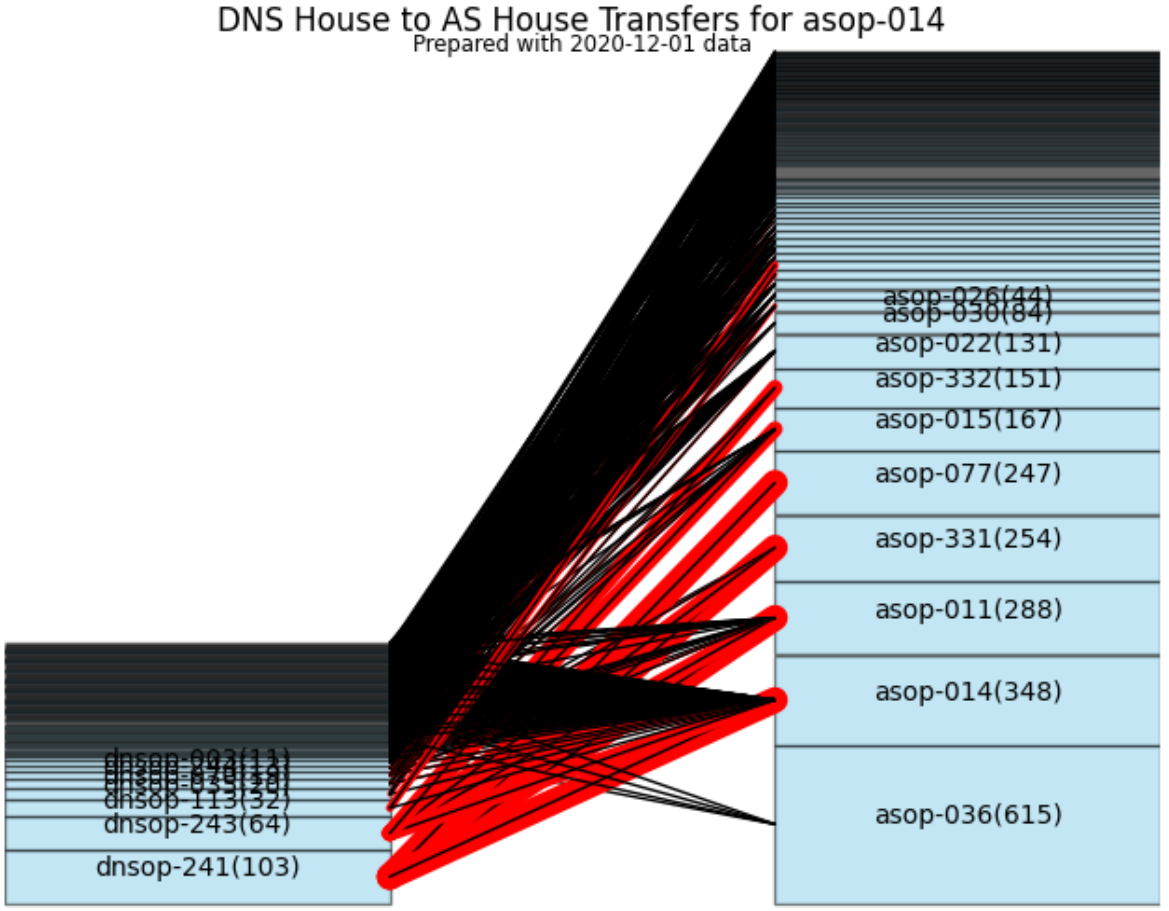
Largest AS Operator "High Volume" Relationships

- ASOP-036
  - Undergoing changes
  - ASOP-055 is a recent "fork"
- Three "large DNS Houses" fed all their zones exclusively to this AS House
- Another DNS House fed all zones to this house as well as another

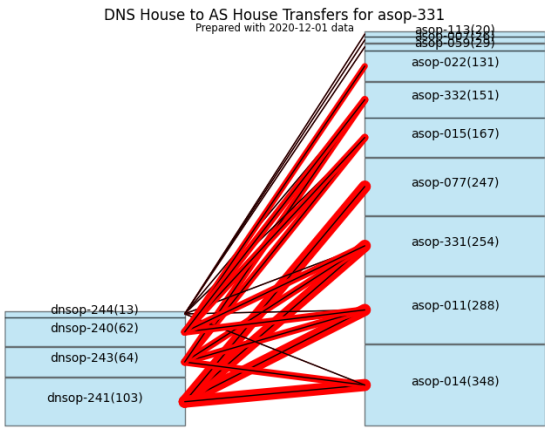


"Notable" Non-registry AS House

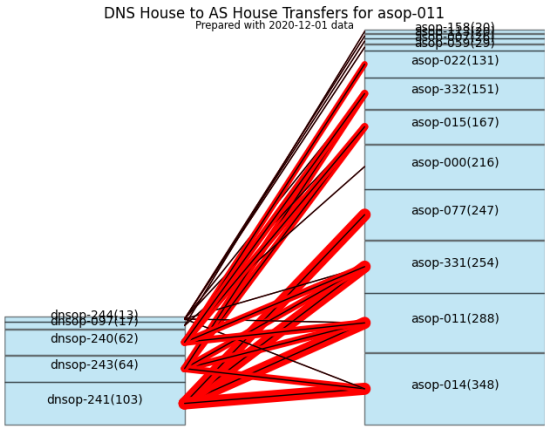
- AS operator 014
  - Only supplies DNS services
  - Does not operate a TLD
- Lots of relationships with small DNS Houses
- Provides services to RIRs
  - The "red lines"
- ASOP-036 appears because it also provides services to some of ASOP-014 customers

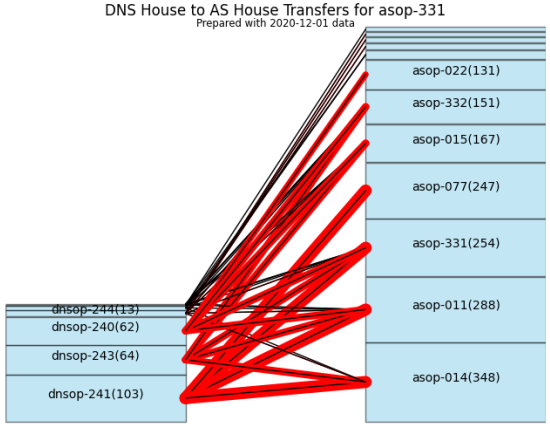


A Tale of Two RIRs

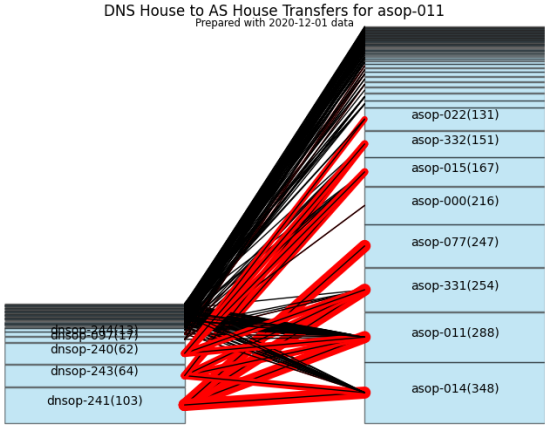


- High Volume Only
  - Meaning, over 10 reverse maps zones
  - The two RIRs look the same as each other





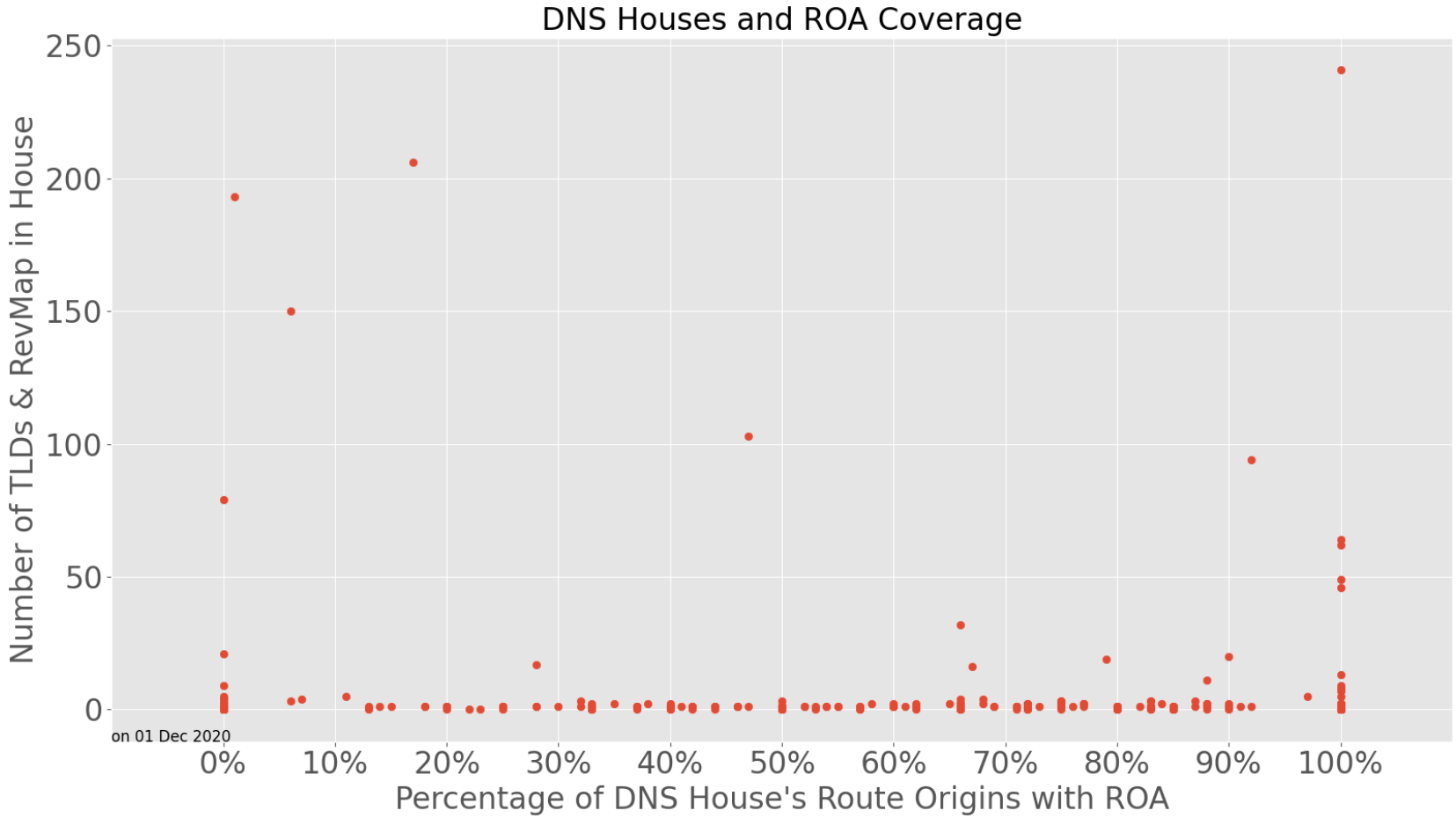
- All cases
  - The RIR on the right also secondaries many singleton TLD operators



Back to ROAs and (DNS/AS) Houses

- The idea was to plot ROA deployment per house
  - Looking for patterns...

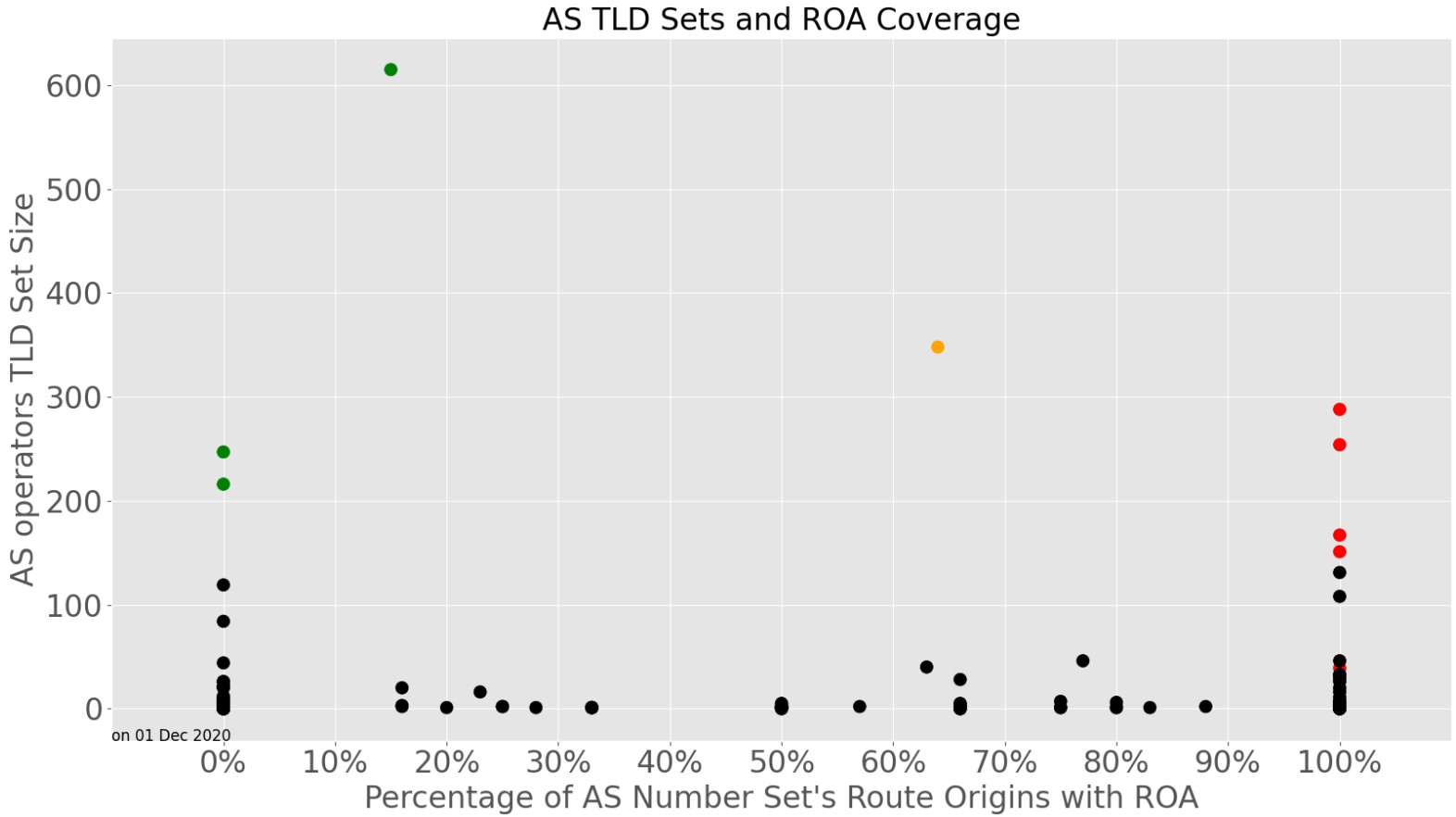
DNS House Chart



DNS Houses vs ROA Deployment

- Hmmm – nothing, really, maybe something...but, no
- (Why are the dots red? I don't recall. But the color does separate them from the dust on the screen. ;))

AS House Chart

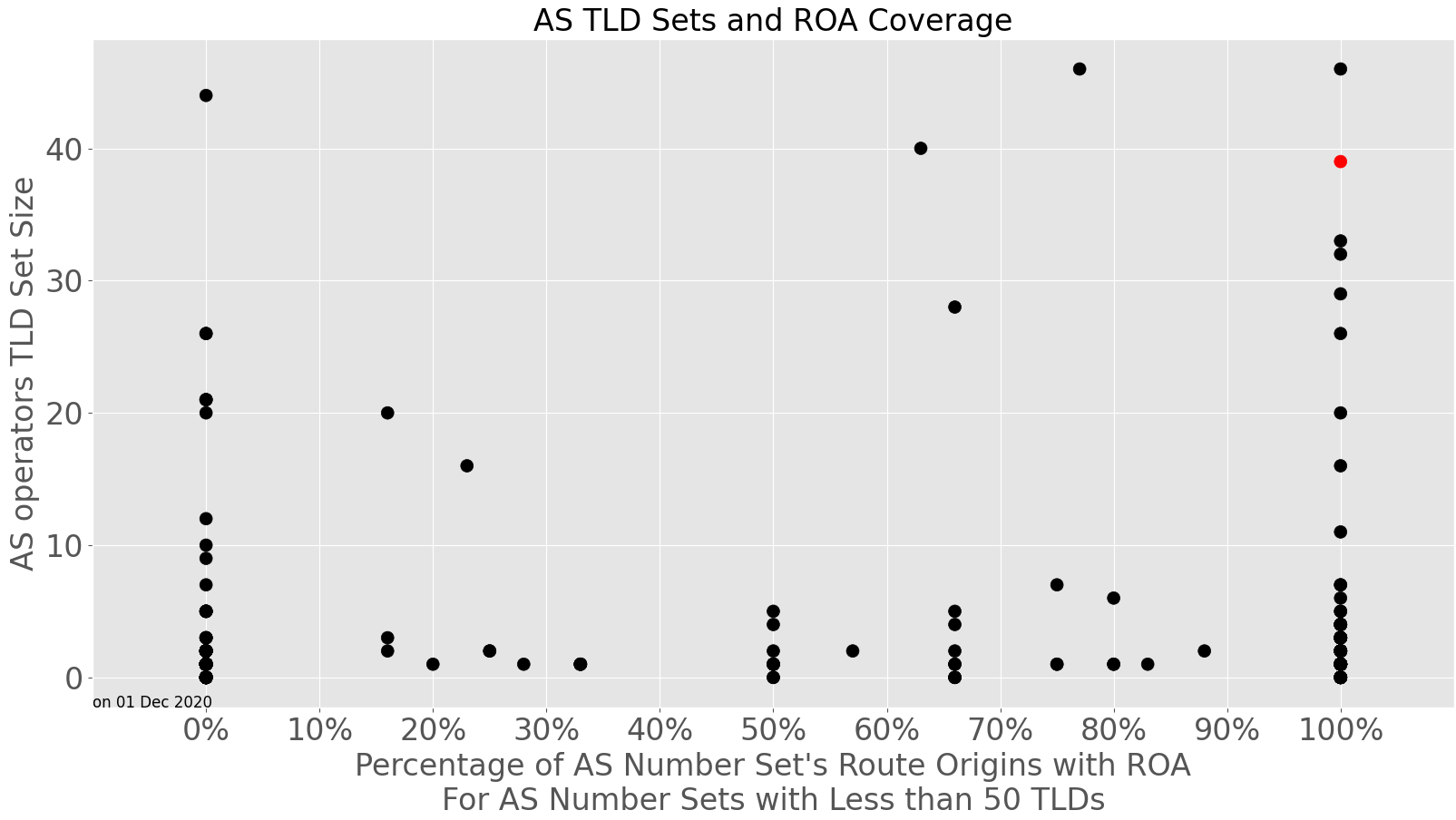


AS Houses vs ROA Deployment

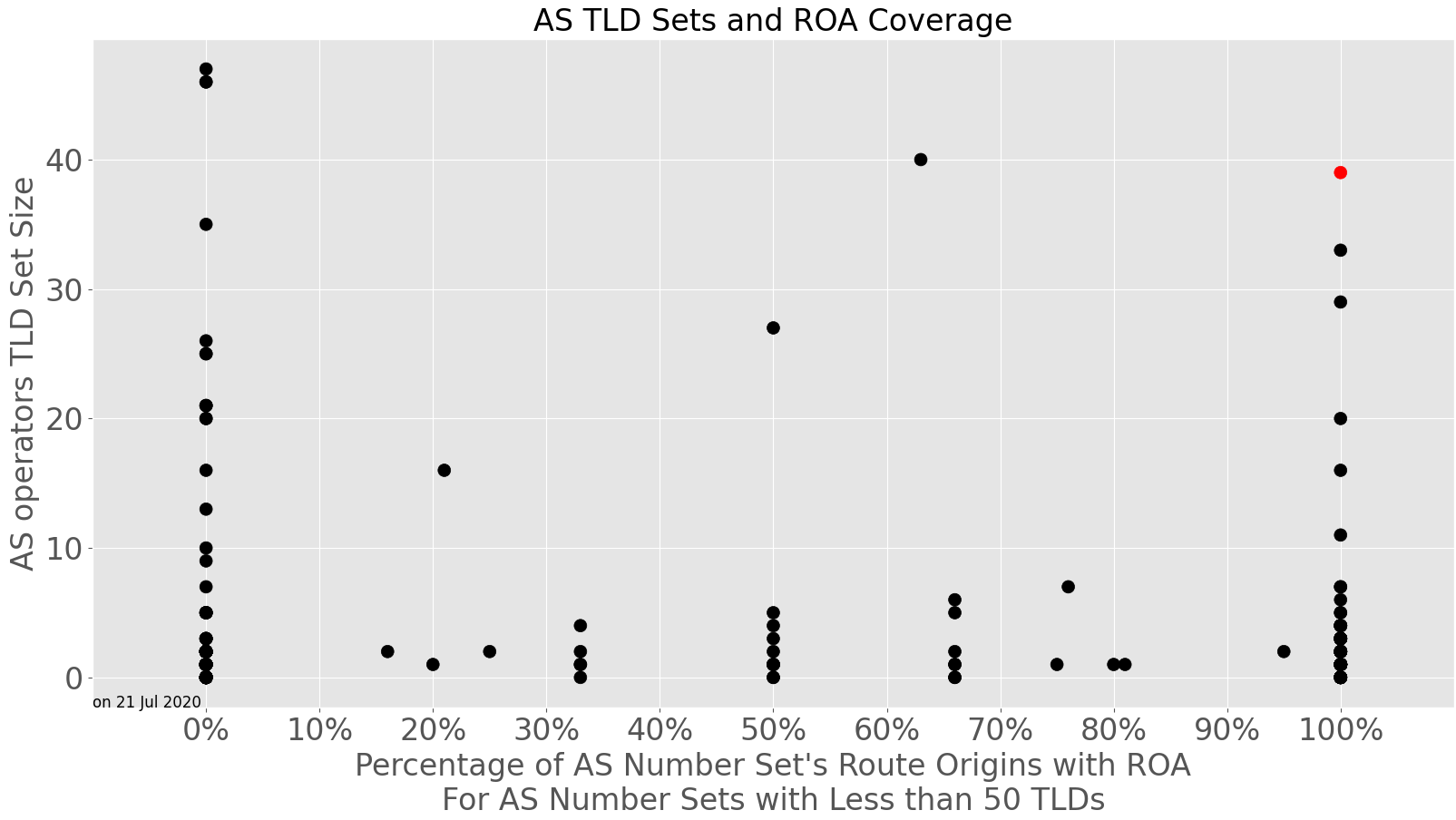
- A noticeable "U" shape with two outliers
  - Not so coincidently, those are ASOP-036 (green) and ASOP-014 (orange) from earlier
  - The other "green dots" are other operators
- The red dots are RIRs (4 of 5 visible here)

- The next slide is for 1 Dec 2020, the following is for 21 Jul 2020
  - An elementary attempt to show change over time

AS House Chart for houses with < 50 TLDs served



AS House Chart for houses with < 50 TLDs served



Smaller AS Houses vs ROA Deployment

- It looks like – the larger houses in this view are more likely to deploy ROAs
- Granted, the sample size is small for a scatter plot
- FWIW: The 5th RIR is visible here

Wrap Up

- The interesting part of this exercise is the analysis involved in developing the visualizations
  - The houses are based on heuristics which may fail over time
- Tracking ROA deployment over time
  - The data is available to run the snapshot any day back a few months
- The DNS Core isn't representative of the commercial DNS
  - But it is "closed environment" one can study over a long term

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