University of Glasgow

Internet Protocols Laboratory

Black Holes and Prisoners: Understanding AS112 Deployment Characteristics

Elizabeth Boswell, Xinyan Xian, Stephen McQuistin, Mingshu Wang, Colin Perkins

Junk

- The DNS translates domain names into IP addresses
- But not all queries have a meaningful response
  - “What domain name resolves to 192.168.0.1?” → private address, so no meaningful answer
  - Sent by misconfigured software
- **Where do those junk queries go?**
  - Are answered by **AS112**

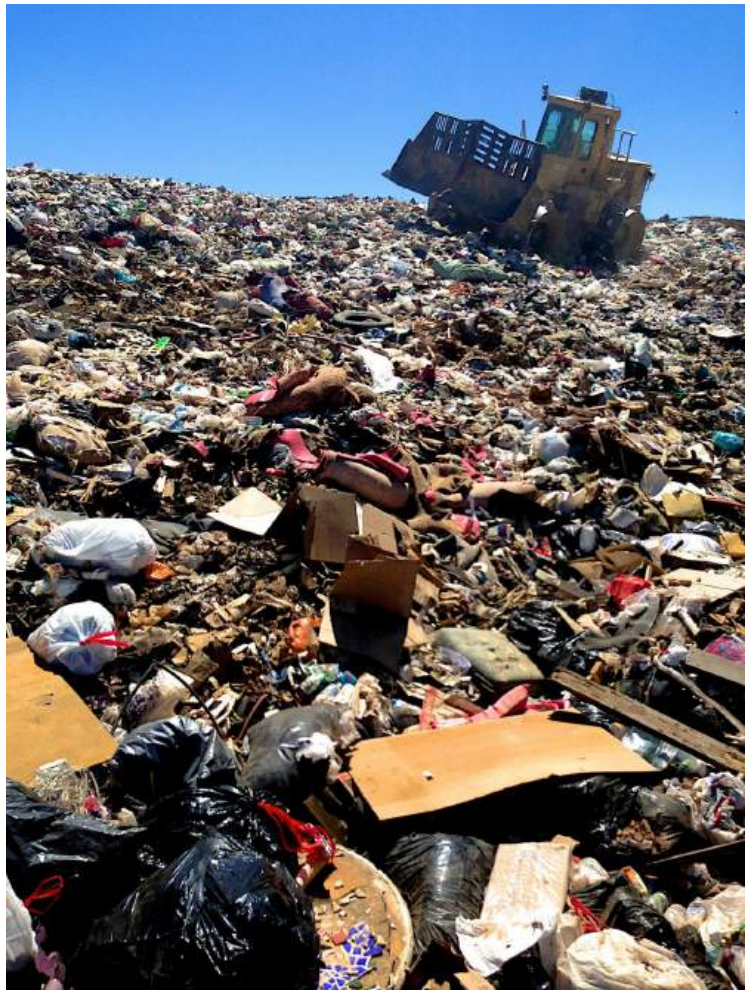
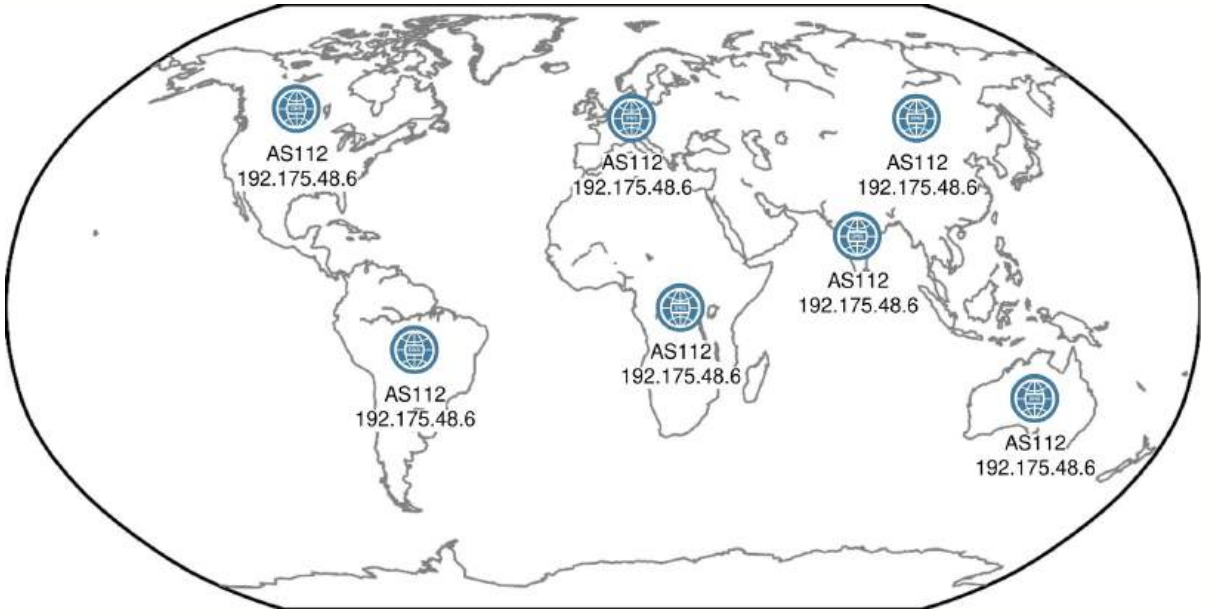


Image by Alan Levine, https://pxhere.com/en/photo/213020

What is AS112?

- Anycast DNS deployment that captures **junk queries**
  - Diverts them from root/.arpa servers
  - Reverse DNS queries for private/link-local IPv4 addresses, queries for **`home.arpa`** and **`service.arpa`**
- Volunteer-run network
  - **Anyone** can add a site!
  - “loosely coordinated”, with self-reported information (as112.net)



University of Glasgow

What we don’t know...

- We don’t know:
  - **How many** AS112 sites are there? **Who** runs them?
  - **Where** are they **located**? From where are they **accessed**?
  - How does it **compare** to other anycast networks?
- Why is this important?
  - Queries sent to AS112 can contain **sensitive information**, e.g. hostnames, which could be **received by anyone**
  - **Protects** important parts of the DNS, needs to be resilient
  - Uniquely uncoordinated DNS deployment

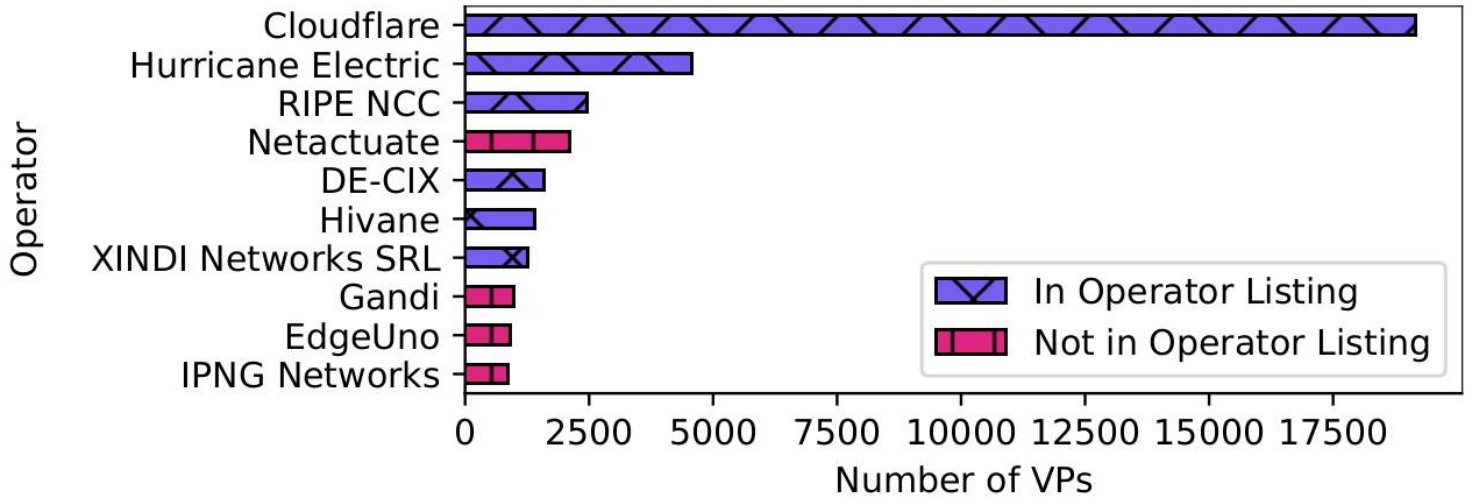
University of Glasgow

Our measurements

- AS112 sites respond to TXT queries for **`hostname.as112.arpa`** or **`hostname.as112.net`** with information about their **location and operator**
  - `el@camorta:~$` **`dig +short TXT hostname.as112.arpa`**
  - **`"RIPE NCC, Amsterdam, The Netherlands"`**
  - **`"See http://www.as112.net/ for more information."`**
- By sending such queries from a large number of vantage points, we can find a large number of sites
  - Sent **`hostname`** queries from 11,833 **RIPE Atlas probes** and 35,312 **open recursive resolvers**

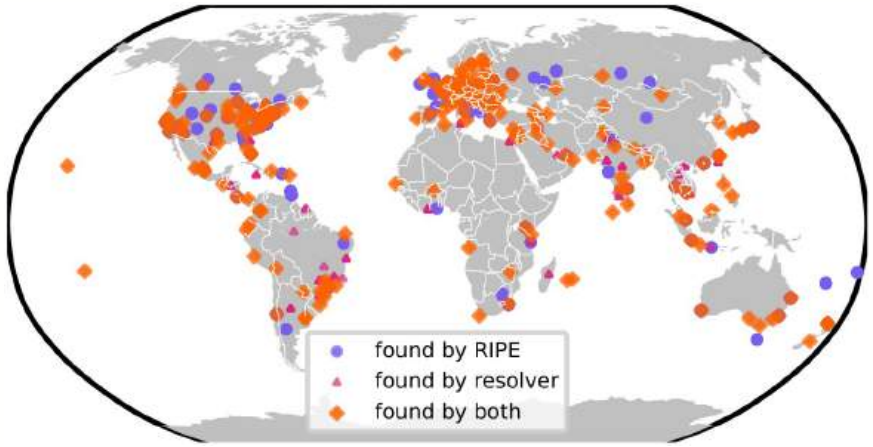
Who runs AS112?

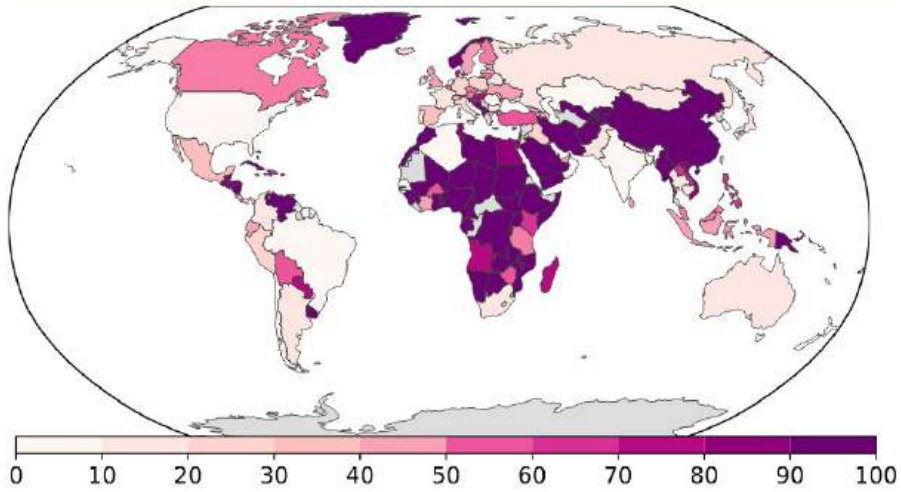
- Found **456 AS112 sites**, run by **94 operators**
  - 38 operators are not on the self-reported “official” list
  - **Cloudflare**: 217 sites, queried by 45.04% of probes/resolvers
    - Resilience issue?



Where is AS112?

- Good coverage in **Europe, North America, Oceania**
- Some sites have very **large geographical reach**
- 28% of probes/resolvers sent queries across borders

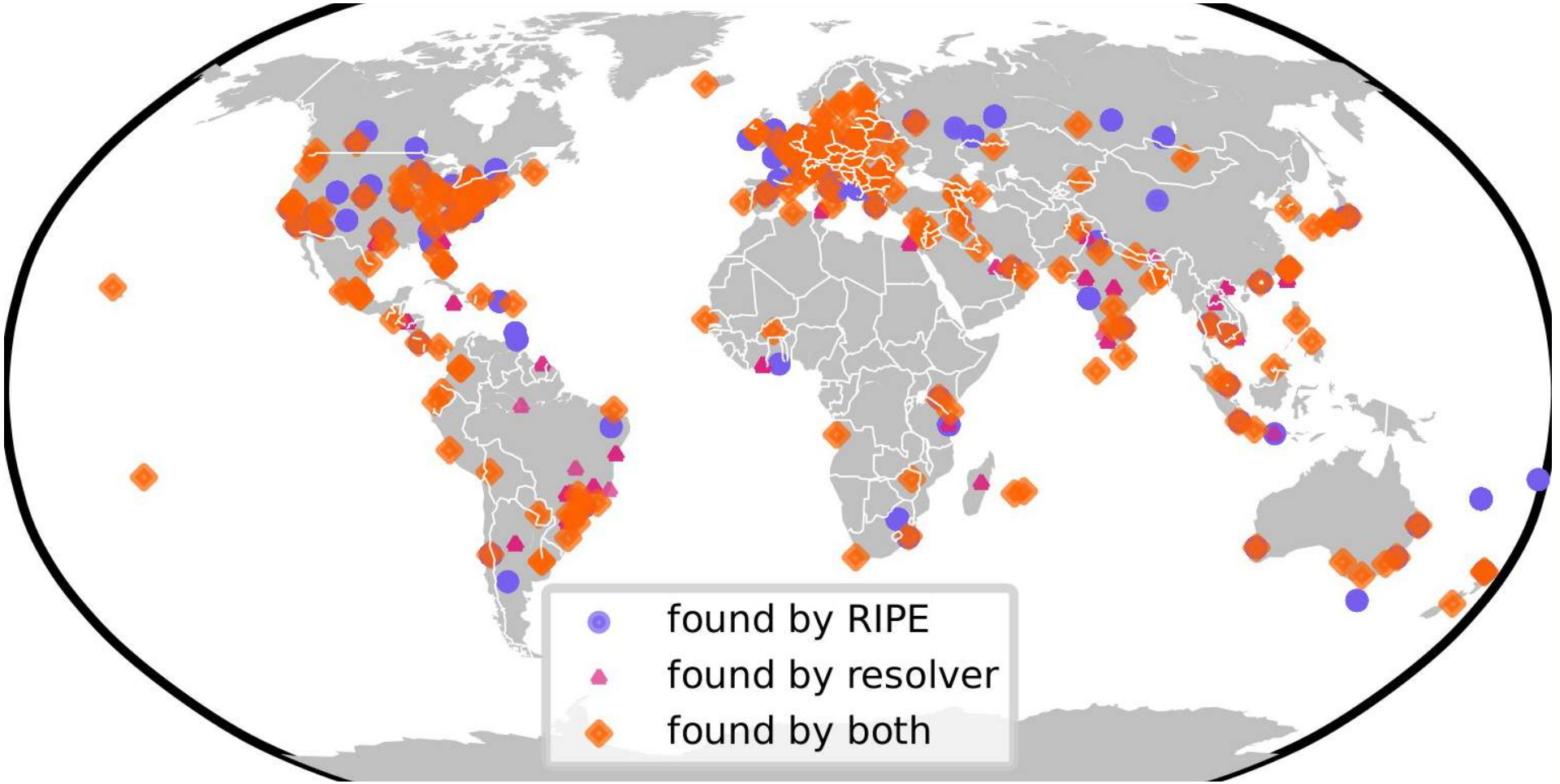




% queries sent to other countries

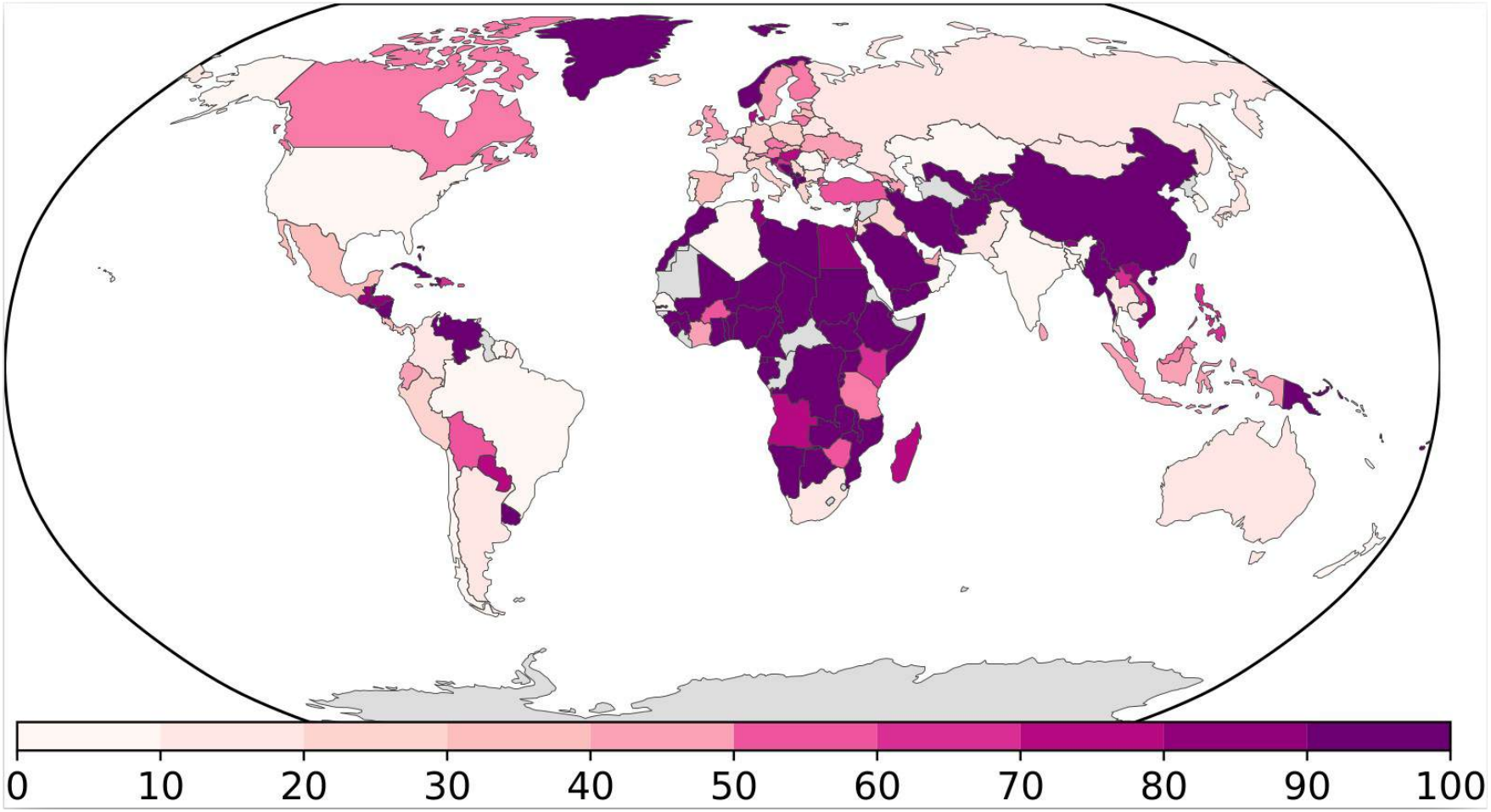
University of Glasgow

Where is AS112? (2)



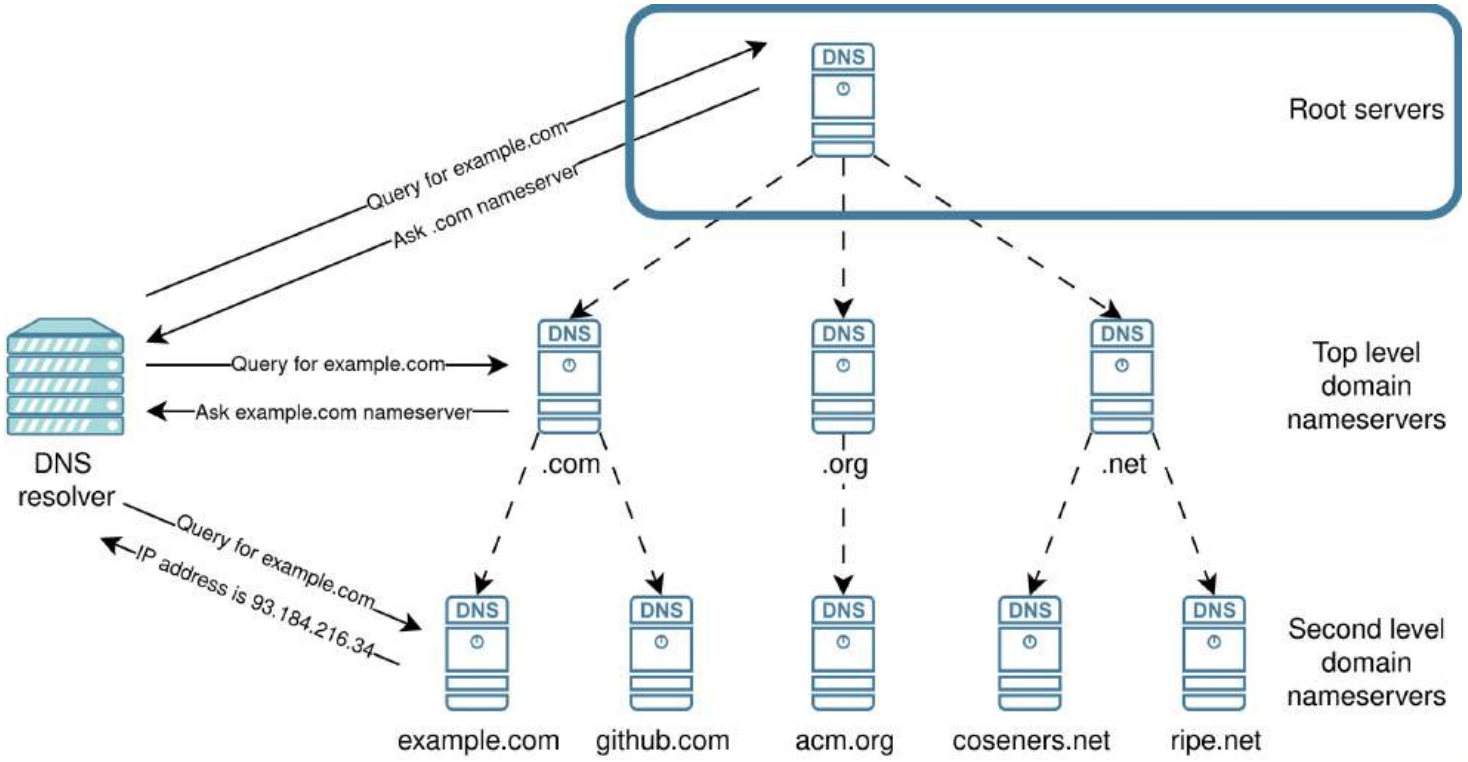
University of Glasgow

Where is AS112? (3)



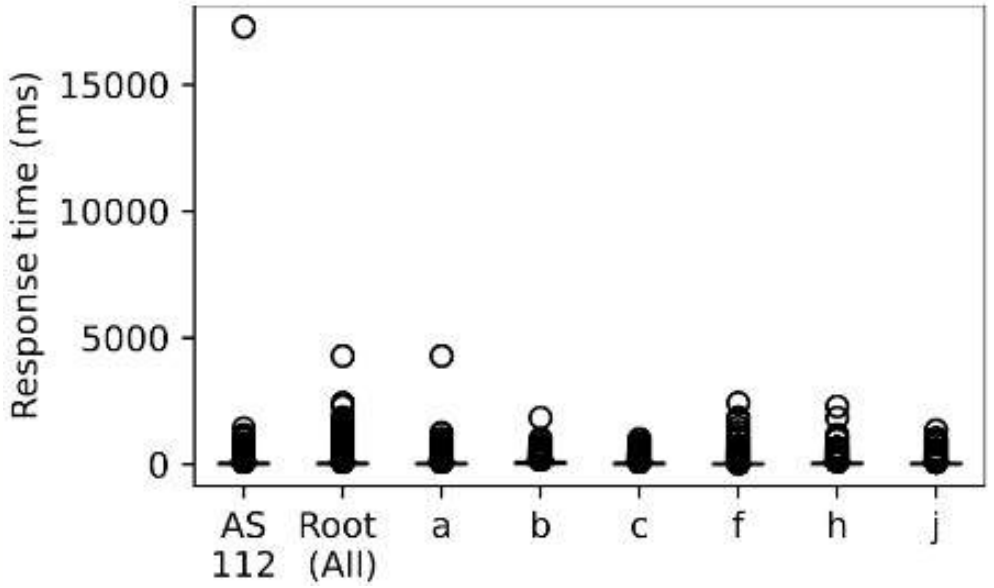
DNS root servers

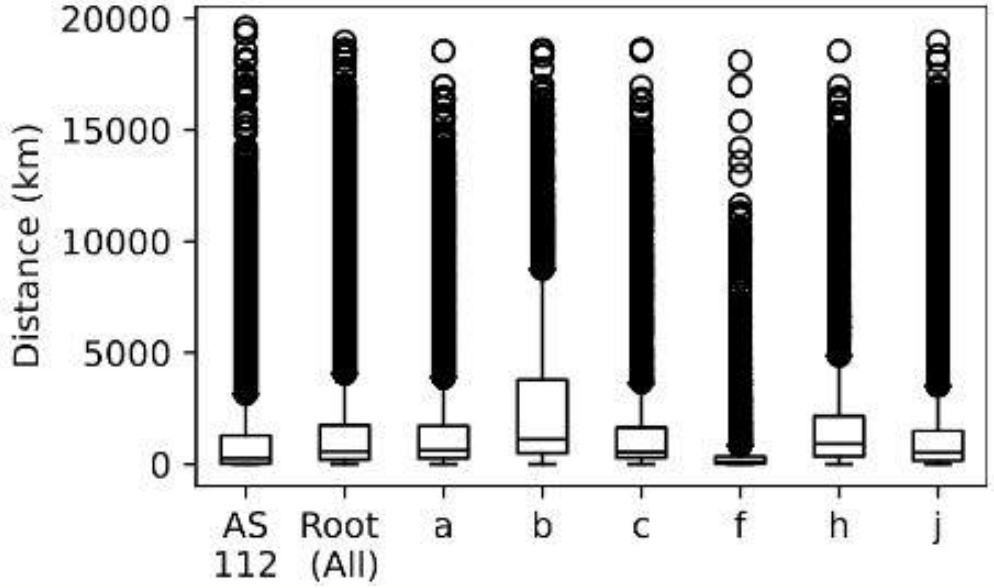
- Top of the DNS hierarchy, serve the root zone and .arpa
- 13 anycast networks (A-M root), run by 12 operators



AS112 vs DNS root

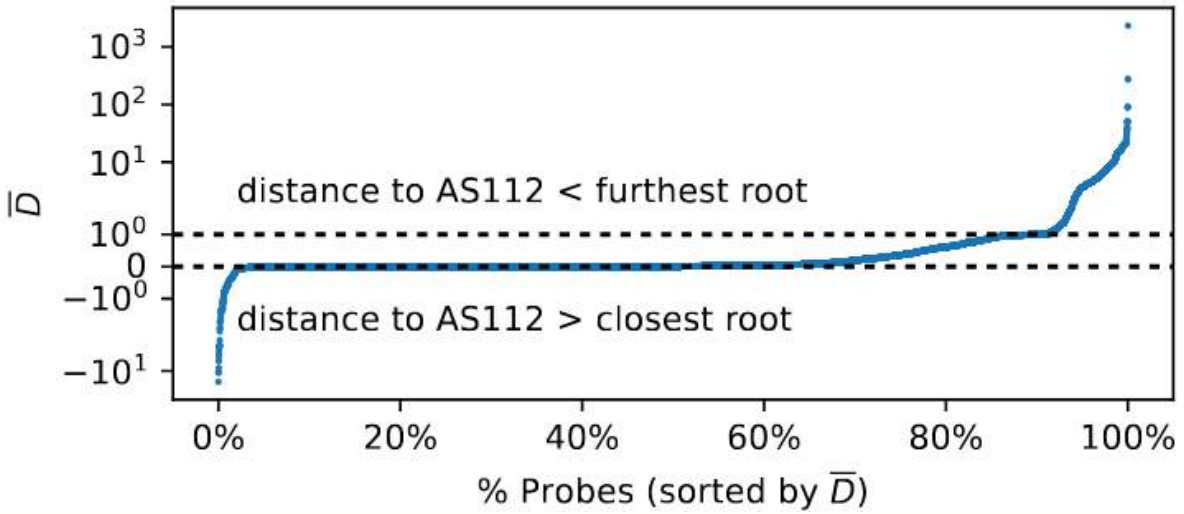
- Compared AS112 to 6/13 DNS root servers (A, B, C, F, J, H-root)
  - Can determine their location with **`CHAOS TXT hostname.bind`** queries
- AS112 has 52.86% lower average distance, 22.91% lower average response time





AS112 vs DNS root (2)

- For 43.8% of RIPE Atlas probes, distance to AS112 ≤ distance to the *closest* queried root site
- Distance to AS112 could be lower:
  - ~24% of probes/resolvers query the closest AS112 site (J-root: ~33%, B-root: ~85%)
  - Routing issues, local sites



Conclusions

- AS112 is a volunteer-run anycast DNS deployment that responds to junk queries
- Widely deployed, similar/better than some root deployments
  - 456 sites, 94 operators
  - But coverage varies, resilience might be limited

Elizabeth Boswell

University of Glasgow

e.boswell.2@research.gla.ac.uk

https://www.gla.ac.uk/pgrs/elizabethboswell/