AS112 Operations Update and Survey Analysis

The Name Servers at the End of the Universe

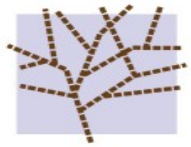
William Sotomayor

UKNOF31

Manchester

20th April 2015

www.dns-oarc.net



DNS-OARC

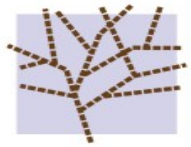
Domain Name System Operations Analysis and Research Center

OARC's Mission Statement

The Domain Name System Operations Analysis and Research Center (DNS-OARC) is a non-profit, membership organization that seeks to improve the security, stability, and understanding of the Internet's DNS infrastructure.

DNS-OARC's mission is:

- *to build relationships among its community of members and facilitate an environment where information can be shared confidentially*
- *to enable knowledge transfer by organizing workshops*
- *to promote research with operational relevance through data collection and analysis*
- *to increase awareness of the DNS's significance*
- *to offer useful, publicly available tools and services*

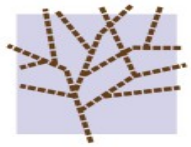


DNS-OARC

Domain Name System Operations Analysis and Research Center

OARC's Functions

- Facilitate co-ordination of DNS operations community
- Ongoing data gathering
- Operate community info-sharing resources
- Maintain/host DNS software tools
- Outreach via external and shared meetings
  - **https://indico.dns-oarc.net/event/21/**
  - Amsterdam, 9-10th May 2015



DNS-OARC
Domain Name System Operations Analysis and Research Center

What is…

- A global, loosely organised, volunteer-driven effort to divert ‘junk’ DNS reverse lookups from the root servers to decrease their workload
- Junk being the in-addr.arpa queries of RFC1918 network addresses coming from many resolvers
- Also absorbs dynamic DNS update attempts from certain mis-configured operating systems
- The name AS112 is taken from the autonomous system number used for the project, using a well-known set of network prefixes, that attracts this type of DNS traffic
  - The service is also anycasted for better performance.

It’s in Your Patch

- Perhaps
- According to the AS112 operators list there are 12 AS112 nodes in the UK
  - Well, in England
  - One in Manchester, by Exa Networks
- Are they really all there or is that list creaky now? You can help!
- https://www.as112.net/ops-listing.html


Aberdeen
SCOTLAND
Dundee
Glasgow
Edinburgh
Londonderry / Derry
NORTHERN IRELAND
United Kingdom
Middlesbrough
Darlington
Isle of Man
Blackpool
Leeds
Hull
Liverpool
Sheffield
Dublin
Galway
Ireland
Stoke-on-Trent
Nottingham
Derby
Limerick
Norwich
ENGLAND
Ipswich
Cork
Waterford
WALES
Swansea
Cardiff
Swindon
Bristol
Reading
Taunton
Southampton
Portsmouth
Exeter
Bournemouth
Plymouth
English Channel
Amiens

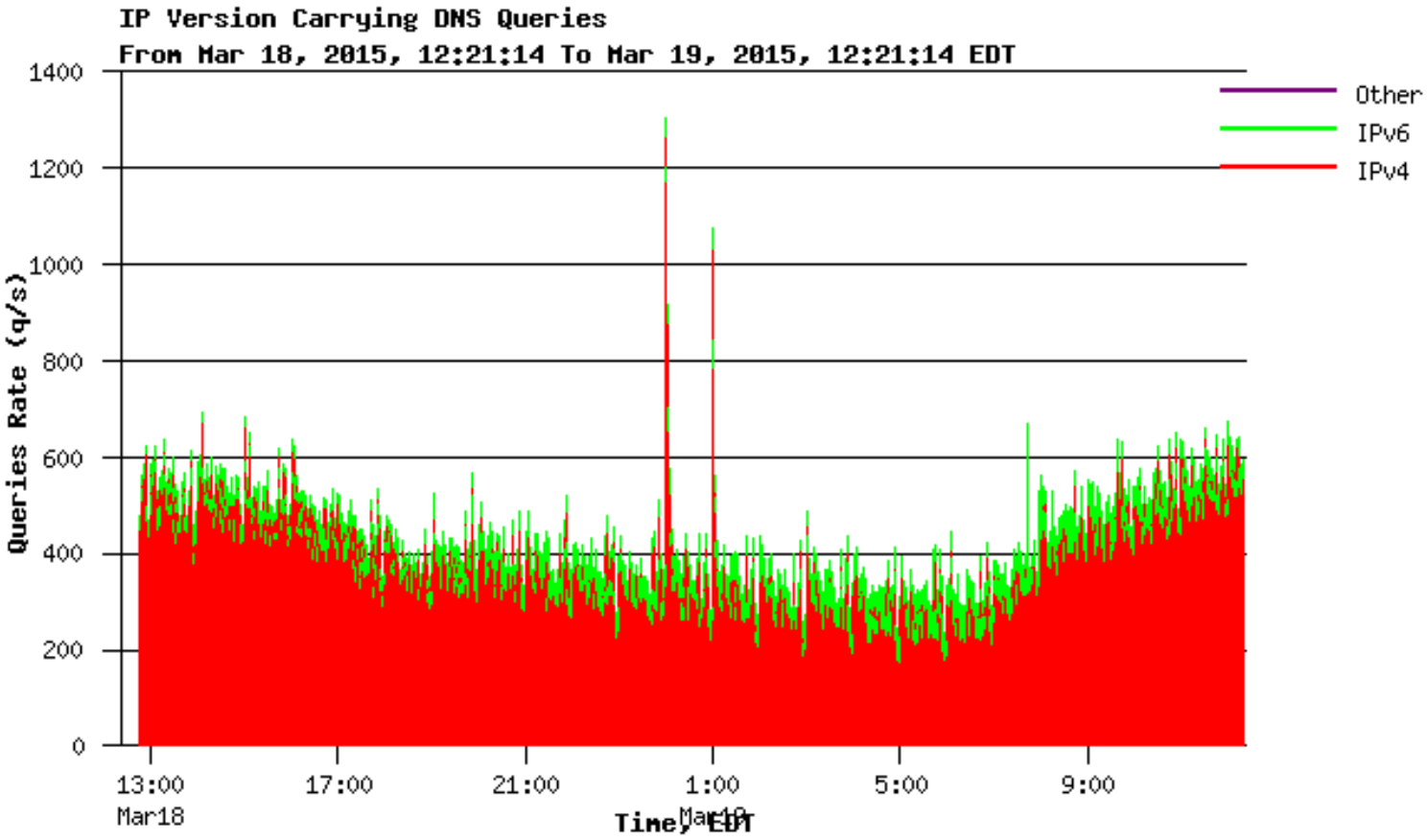
AS112 Update

- Progress made on AS112 on two fronts:
  - *draft-ietf-dnsop-rfc6304bis* updates include IPv6 transport and some new advice for reserving the AS112 project ASN and prefixes in the IANA special use registry, advice on logging and potentially leak information on internal infrastructure behind a NAT, plus other fixes. Informational RFC
  - *draft-ietf-dnsop-as112-dname* addresses the problem of delegating new zones to AS112 operations without relying on AS112 operators making required changes to their nodes for every change. Informational RFC
- Both have passed IETF WGLC and are in RFC-Editor review
- But we know who the authors are, and if there's anything we've missed do let us know
- https://www.as112.net/

AS112 Operations

- As a result of being in RFC Editor's hands, on March 17, 2015, certain IANA actions were (suddenly) triggered:
  - AS112 nodes must now expect queries on IPv6 sockets and AS112 operators should follow new directions in RFC6304bis
  - There are new IPv4 and IPv6 prefixes for use as described in the AS112 'DNAME' draft to attach and listen for delegated traffic
- Yes, there are IPv4 NATs using IPv6 DNS to ask about IPv4 reverse junk...note the irony

AS112 Dual-stack



AS112 Surveys, 2015

- For the past 4 years, AS112 surveys have been conducted by my self
  - The official as112.net operators list is never 100% accurate.
- Based on the following question: How does one find an unpublished public or ‘private’ AS112 server?
  - The same way as detecting a blackhole – by inference.
- Open DNS resolvers are so very, very useful
  - Ask the open resolver if it can identify which AS112 node is responding to it and maybe get some extra info too
- Route Views is good for this too
  - Automated login to various route views servers and query for the AS112 IPv4 route to derive first upstream ASN
  - But not as useful as open resolvers to find localised AS112 nodes.
- Results have been posted to the AS112 website for everyone’s enjoyment
- Trivia: There is an AS112 server in New Caledonia! Yes, really!

Survey Methodology

- Automation is pretty much key, as well as trying to get the results quickly
  - Fetch the open resolvers file
  - Find number of lines, calculate the number of factors, then use those to split the file up into 100 or more pieces of even size by number of lines
  - Initiate parallel ‘dig’ queries and save results in unique files
  - Resulting output combined
  - Import results into database or spreadsheet and start count analysis
  - Remove duplicates
- Then publish the final result

AS112 Survey Results

- Of 7,601,333 allegedly open resolvers tested, 926,555 responded to any of 2 questions (January 2015)
- A number of observations stated on the website, but in summary:
  - AS112 nodes need to better identify themselves, as per the RFC
    - Eg, “Osaka, JAPAN” or “Widgets, Anytown, AnyCountry”, are not useful to operators, etc.
  - The mechanism of the test is infrequent (once a year)
  - Many AS112 nodes were geographically close to AS112 clients, but because of poor local peering (deliberate or otherwise), many clients cross half the world to reach their ‘nearest’ AS112 server
  - There seems to be a small churn of AS112 nodes, some drop off, some new ones come online but the number remains within a range of 71-73 nodes.
- Number 1 AS112 node appears to be Hivane’s
- ‘Nodes’ is a term used very loosely as there could be more than one instance of a poorly described AS112 server duplicated in these counts.

Open Resolver's Choice

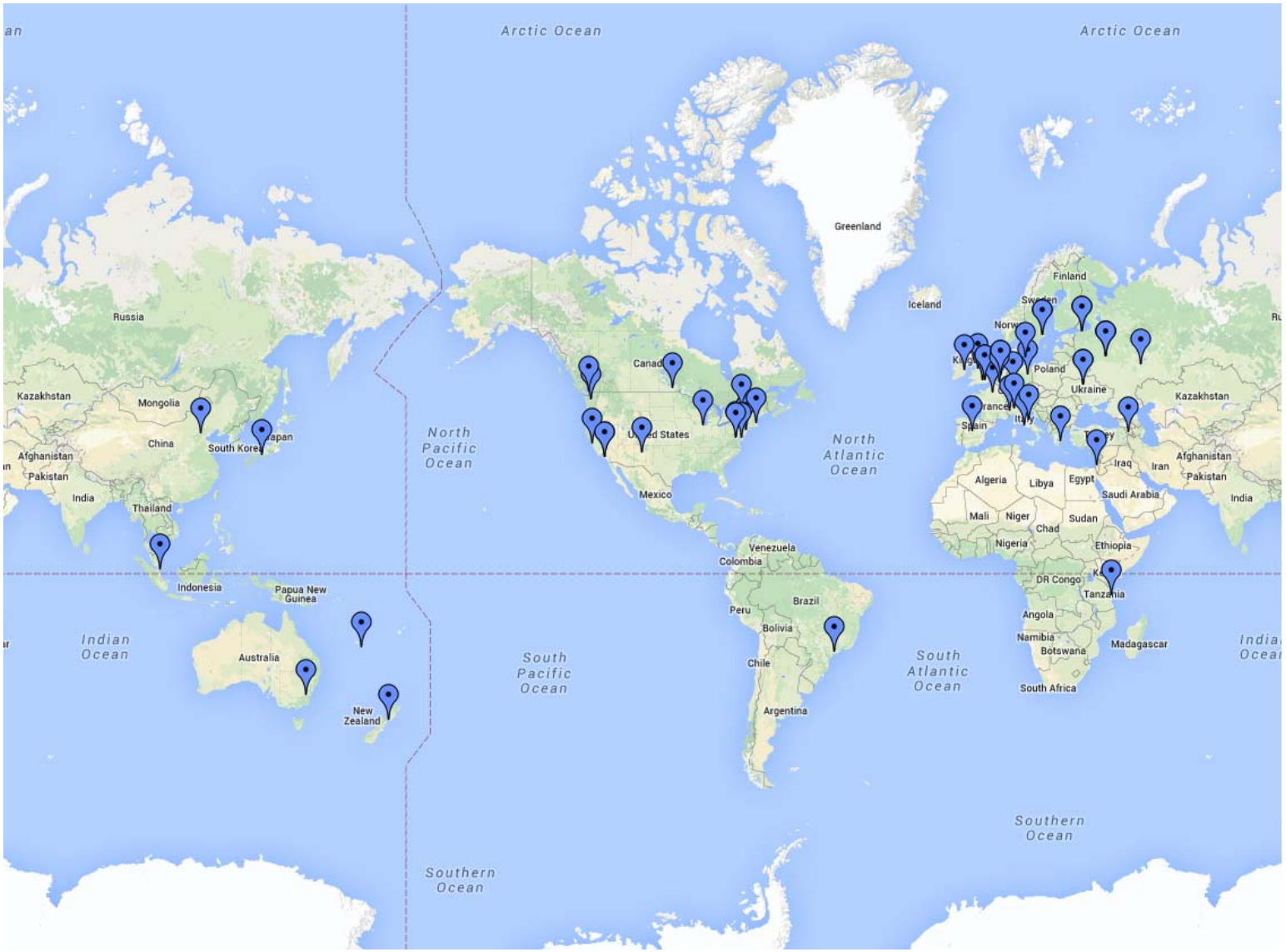
- Truly not indicative of all resolvers by far, but we do have suspicions
- Most 'popular' nodes accessible by open resolvers
  - Hivane
  - WIDE
  - ICANN
  - NIC.br
  - Qwest
  - Afilias
  - RIPE
  - AS3277
  - OttIX
  - Individual Network Berlin

AS112 Ops list vs Survey

- What about the operator's listing?
- Using Google Maps, Red markers for ops listing, blue markers for survey listing just to compare
- Note that despite the AS112 server density in Europe, not all European clients use them.
- Also note there of course more nodes per organisation, for example Verisign has several.

2014 AS112 Ops Listing

2014 AS112 Survey Results

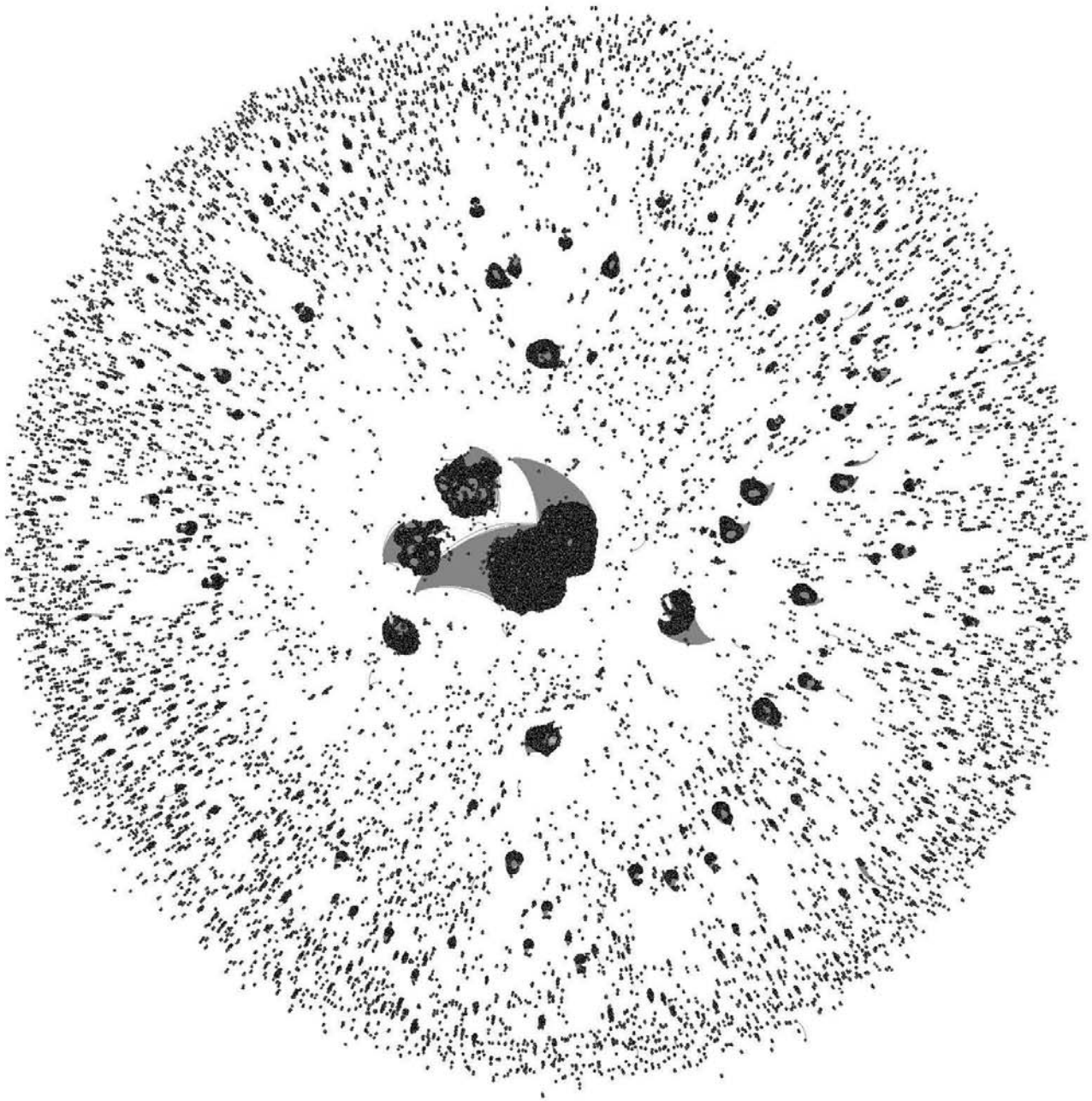


AS112 Maps

- They don’t look all that different, but the devil is of course in the details, as there are fewer
  - In fact for 2015 they’re the same, respectively
- Despite this, it is useful to visualise not just the proximity of these AS112 nodes but also how these nodes are reached
- However this would require a greater degree of co-operation between AS112 operators to contribute data to pinpoint proximities between clients and nodes to optimise network placement
- An example follows

How to explain AS112 to an Enterprise IT Mindset

- All this techno-babble is interesting, but not very useful if not explained in a business language
- How does one express the state of an improperly configured DNS or Windows clients behind a NAT?
- What is the incentive to the CIO to either fix the problem or deploy AS112 inside?
- Well, why bother with language at all?



AS112 Traffic on One Node

- In all seriousness, the foregoing is a visualisation of one AS112 node's traffic (it happens to be the one on a NREN, the subject of this presentation)
- Each galactic 'bloom' in this universe represents one server making in.addr-arpa queries
- The bigger the bloom, the greater the number of queries from a single source to that AS112 node's universe in a given time period
- Do the larger ones represent an overly aggressive set of resolvers, or infer the *size* of a particular NATed network??
- 'Sir, the second blob to the left is us leaking internal data'