Who's Asking?

Geoff Huston, Joao Damas

APNIC

Roy Arends

ICANN

Background

Experiments that are intended to expose the way in which recursive resolvers interact with the DNS root and its authoritative servers share a common weakness:

It isn't possible to trigger a particular response from root servers by varying the contents of the root zone, or by deliberating altering the behaviour of root servers in non-standard ways

Background

What we **can** do is create a comparable condition in a delegated zone at a lower point in the DNS name hierarchy to reproduce questions we'd like to ask of the root

Background

What we **can** do is create a comparable condition in a delegated zone at a lower point in the DNS name hierarchy to reproduce questions we'd like to ask of the root

- *What proportion of resolvers perform DNSSEC validation?*
- *How many resolvers are capable of asking a query over TCP?*
- *What proportion of resolvers are capable of querying using IPv6?*
- *How do resolvers handle large DNS responses?*

Background

But are these two environments the same?

Does the profile of query traffic seen an an authoritative name server match that seen at an authoritative name server?

Root Query Profiles

Let's look at the profile of query traffic sent to a number root servers in the period January – March 2017

Root Query Profile

Queries of the Root Zone itself:	3.4%
Queries about delegated Zones:	30.3%
Queries about non-existent Zones:	66.3%

Most of the queries directed to root servers appear to relate to non-existant names (NXDOMAIN)

This does not include consideration of the validity of the 2ld (or deeper) in queries to delegated zones, so the "junk" ratio of queries seen at root servers is likely to be well in excess of 66÷

Root Query Profile

TCP vs UDP:

UDP Queries:	98.3%
TCP Queries:	1.7%

Root Query Profile

TCP vs UDP:

UDP Queries:	98.3%
TCP Queries:	1.7%

There is an open question here whether this TCP query rate is a result of a prior query using no or a small EDNS(0) UDP Buffer size and receiving a truncated UDP response, or whether the resolver has chosen to use TCP without a prior UDP query and truncated response

Root Query Profile

DNS over IPv4 vs DNS over IPv6:

Queries over IPv4:	84.3%
Queries over IPv6:	15.7%

Root Query Profile

Query Types seen **at** a root server:

A	63.6%
AAAA	21.5%
NS	4.3%
PTR	3.4%
DS	2.7%
SRV	1.5%
SOA	1.1%
TXT	0.7%
MX	0.3%
CNAME	0.3%
DNSKEY	0.2%
ANY	0.1%

Root Query Profile

Query Types seen **at** a root server vs queries seen directed **to** a root server relating to the root zone itself:

Qtype	AT Root	TO Root
A	63.6%	2.6%
AAAA	21.5%	0.3%
NS	4.3%	93.7%
PTR	3.4%	0.0%
DS	2.7%	0.0%
SRV	1.5%	0.0%
SOA	1.1%	1.1%
TXT	0.7%	0.0%
MX	0.3%	0.0%
CNAME	0.3%	0.0%
DNSKEY	0.2%	2.1%
ANY	0.1%	0.1%

Resolvers querying the Root

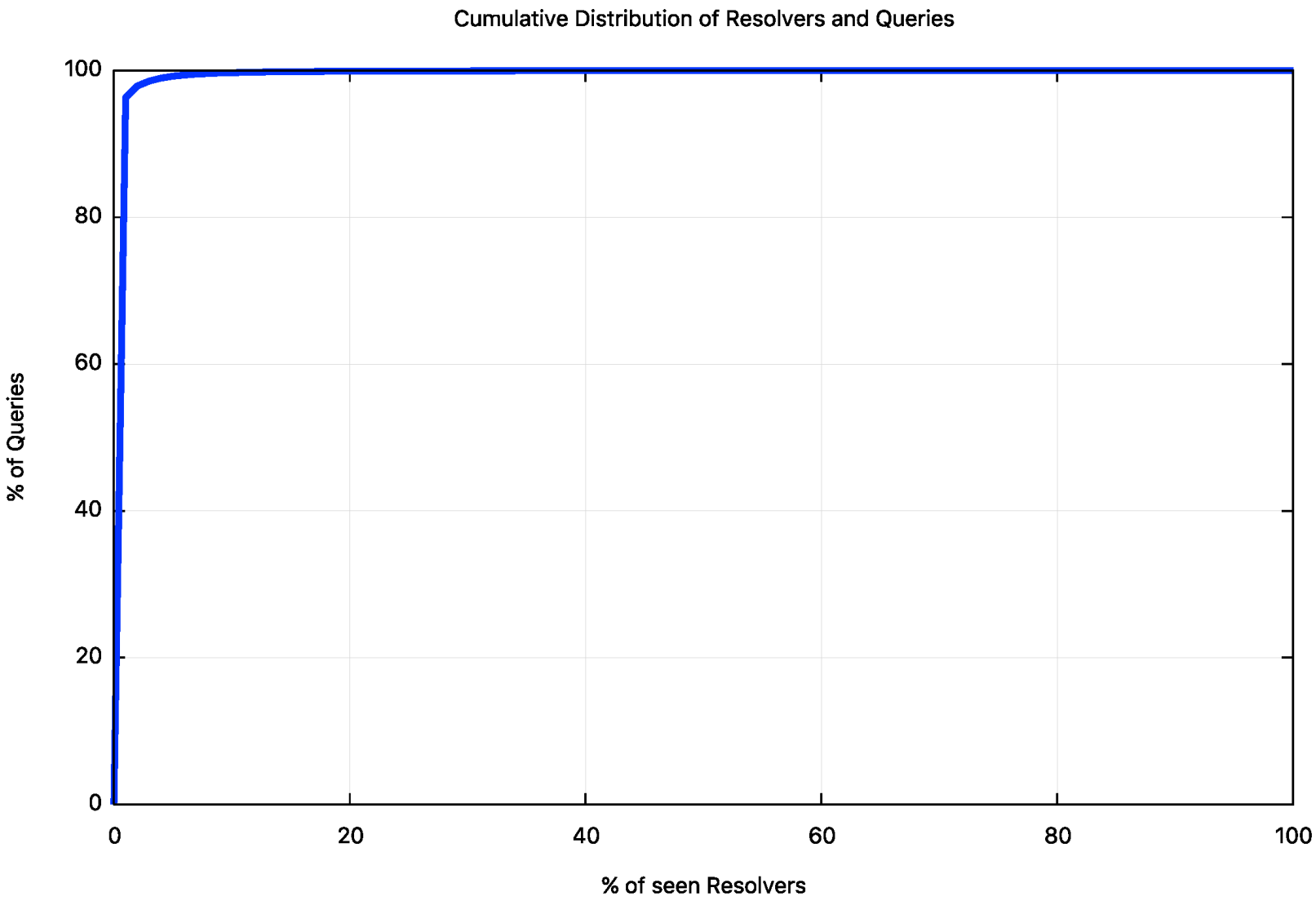
20M unique resolver IP addresses were seen in the analyzed data set

Top 20 Queriers

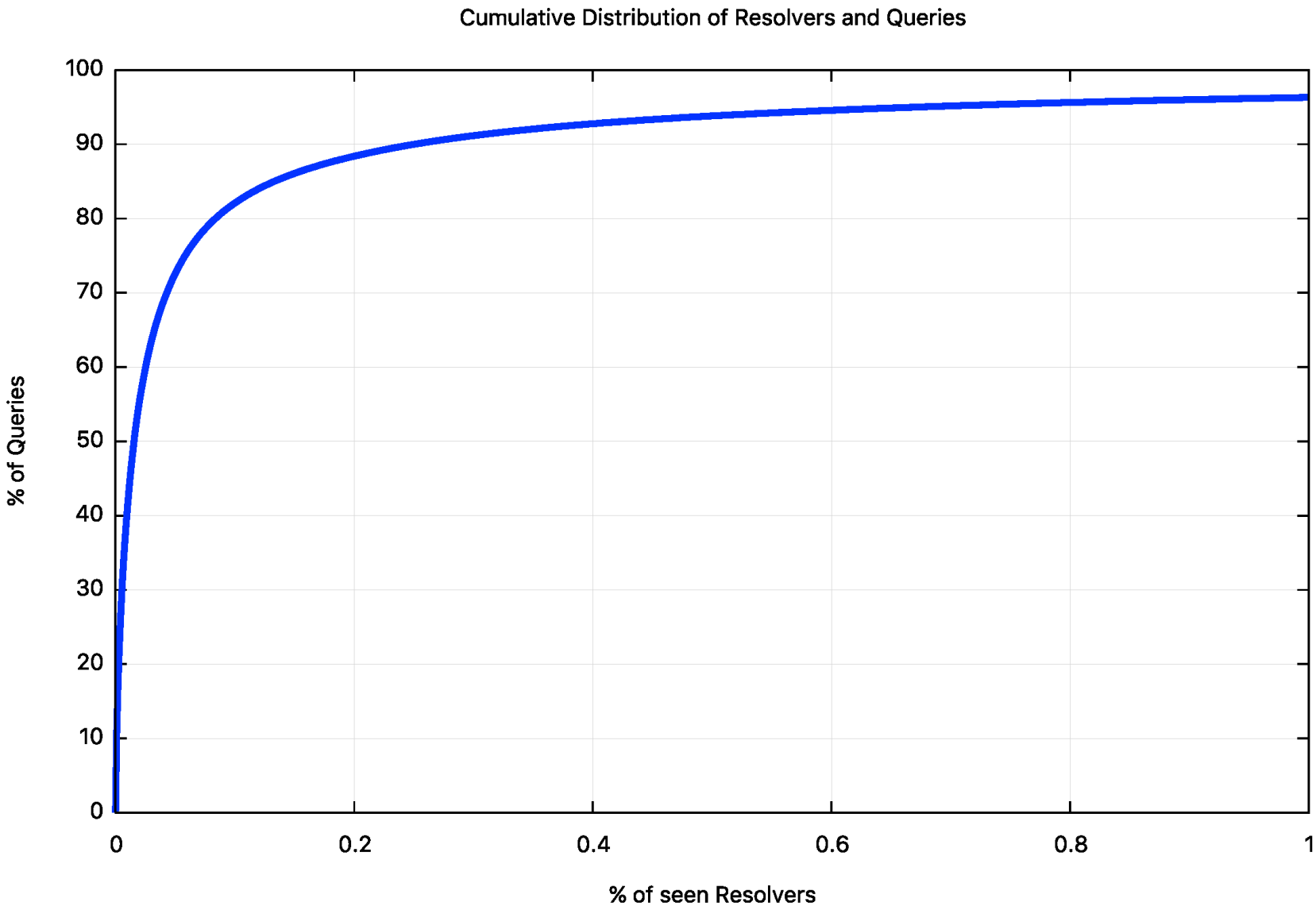
Resolver	Total Share of Queries	NXDOMAIN resp. rate	AS Name
199.16.156	0.22%	6.9%	AS13414 - TWITTER - Twitter Inc., US, United States of America
212.19.128	0.21%	0.5%	AS50482 - KAZAKHTELECOM-AS , KZ Kazakhstan
129.56.0	0.17%	1.4%	AS327952 - AS-NATCOM, NG Nigeria
213.5.255	0.16%	99.8%	AS50188 - KOLNET, PL Poland
213.5.255	0.16%	99.9%	AS50188 - KOLNET, PL Poland
116.9.94	0.15%	67.9%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN China
62.201.215	0.14%	99.3%	AS44217 IQNETWORKS, IQ Iraq
129.56.0	0.11%	1.7%	AS327952 - AS-NATCOM, NG Nigeria
104.156.86	0.11%	0.0%	AS54113 - FASTLY, US United States of America
2a02:cb80:2110::	0.11%	94.5%	AS43766 - MTC-KSA-AS , SA Saudi Arabia
85.62.233	0.11%	100.0%	AS12479 - UNI2-AS , ES Spain
177.74.154	0.10%	100.0%	AS263650 - Clicfacil Computadores, Servisos e Telecomunicate, BR Brazil
85.62.229	0.10%	100.0%	AS12479 - UNI2-AS , ES Spain
199.59.148	0.09%	6.6%	AS13414 - TWITTER - Twitter Inc., US, United States of America
61.164.15	0.09%	0.0%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN China
204.194.239	0.09%	94.2%	AS30607 302-DIRECT-MEDIA-ASN, US United States
2620:119:13::	0.09%	94.3%	AS36692 - OPENDNS - OpenDNS, US United States of America
2620:119:13::	0.09%	94.1%	AS36692 - OPENDNS - OpenDNS, US United States of America
2620:119:13::	0.09%	94.0%	AS36692 - OPENDNS - OpenDNS, US United States of America
2620:119:13::	0.09%	94.1%	AS36692 - OPENDNS - OpenDNS, US United States of America

As seen by one root server system over Feb 2017

Query Intensity



Query Intensity



Lets filter out NXDOMAIN queries…

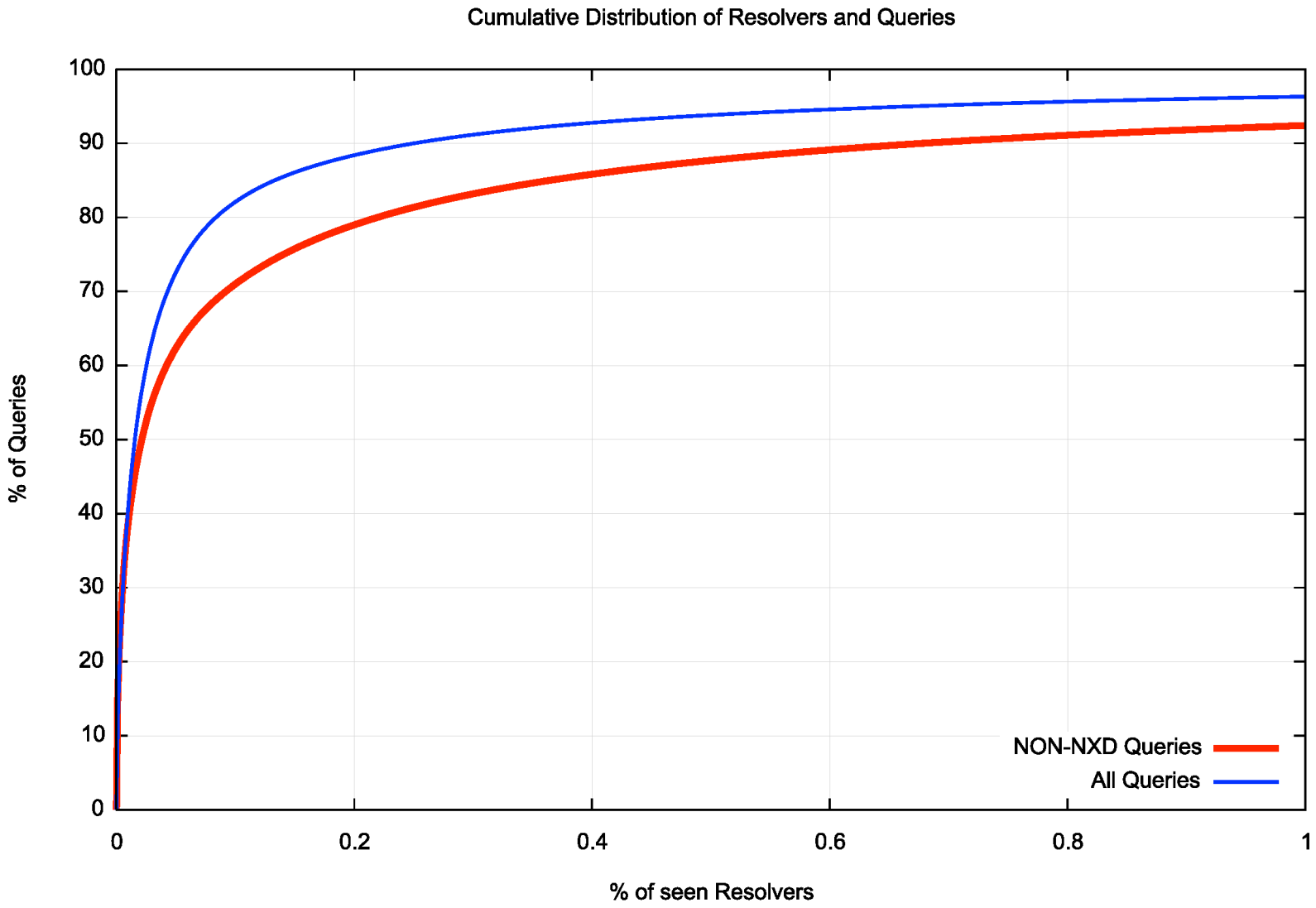
- Some 18M resolvers asked a query that related to either the root zone or a tld that is defined in the root zone (90% of the original resolver set)

Top 20 Queriers

Resolver	Total Share of Queries	Root vs TLD Query	AS Name
199.16.156	0.62%	3.8%	AS13414 - TWITTER - Twitter Inc., US
212.19.128	0.61%	0.1%	AS50482 - KAZAKHTELECOM-AS , KZ
129.56.0	0.51%	0.3%	AS327952 - AS-NATCOM, NG
104.156.86	0.33%	0.0%	AS54113 - FASTLY - Fastly, US
129.56.0	0.33%	0.4%	AS327952 - AS-NATCOM, NG
61.164.15	0.26%	0.0%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN
199.59.148	0.24%	3.8%	AS13414 - TWITTER - Twitter Inc., US
207.179.70	0.22%	0.4%	AS14103 - ACDNET-ASN1 - ACD.net, US
108.171.129	0.21%	1.3%	AS25605 - SCANSAFE - SCANSAFE SERVICES LLC, US
209.143.22	0.19%	1.0%	AS7106 - OHIOBRIGHTNET - Com Net, Inc., US
220.188.114	0.18%	0.0%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN
180.137.252	0.16%	0.0%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN
64.237.48	0.16%	0.1%	AS20473 - AS-CHOOPA - Choopa, LLC, US
213.111.4	0.16%	1.7%	AS39886 - NOMOTECH 53 avenue de la pierre vallee, FR
179.190.28	0.15%	0.0%	AS52925 - ASCENTY DATA CENTERS LOCATIO E SERVICOS SA, BR
61.164.15	0.15%	0.0%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN
116.9.94	0.15%	7.7%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN
216.117.191	0.14%	0.7%	AS10843 - AITNET - Advanced Internet Technologies, US
61.164.15	0.14%	0.0%	AS4134 - CHINANET-BACKBONE No.31,Jin-rong Street, CN
85.93.93	0.14%	1.9%	AS8972 - PLUSSERVER-AS , DE

As seen by one root server system over Feb 2017

Query Intensity



Measuring the DNS

At APNIC the approach we've used for some years has been to use an online Ad campaign to test a particular DNS behavior across a large volume of end user browsers

The tests have included:

- DNSSEC validation
- large DNS responses
- TCP fall back
- Use of IPv6
- Mapping users to the resolvers that they use

Similarity

The question is how similar are the sets of resolvers that we see in queries generated by the Ads against what is seen by Root Servers?

Top 20 Queriers

As seen by APNIC DNS servers

Resolver	Share of Queries	AS Name
74.125.47.6	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.13	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.1	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.7	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.9	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.3	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.12	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.2	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.11	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.8	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.10	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.5	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.14	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.4	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.47.15	0.23%	AS15169 - GOOGLE - Google Inc.
74.125.181.6	0.22%	AS15169 - GOOGLE - Google Inc.
74.125.181.12	0.22%	AS15169 - GOOGLE - Google Inc.
74.125.181.8	0.22%	AS15169 - GOOGLE - Google Inc.
74.125.181.4	0.22%	AS15169 - GOOGLE - Google Inc.
74.125.181.7	0.22%	AS15169 - GOOGLE - Google Inc.

Similarity

The two data sets are obviously very different!

The APNIC data set is generated by presenting end users with unique domain names that are intended to negate any form of DNS caching

The root data set is (in theory) a set of cache miss queries

So its no surprise that these data sets are quite different

Similarity

So how can we compare the resolvers seen on these data collections?

One approach is to use the experiment's script to direct the end user's resolvers to query the root AND to query our experiment's servers

Query Set

w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-apnic-test
c.14u-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net.
c.14s-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net.
c.1du-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net.

Experiment Query Set

w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-apnic-test

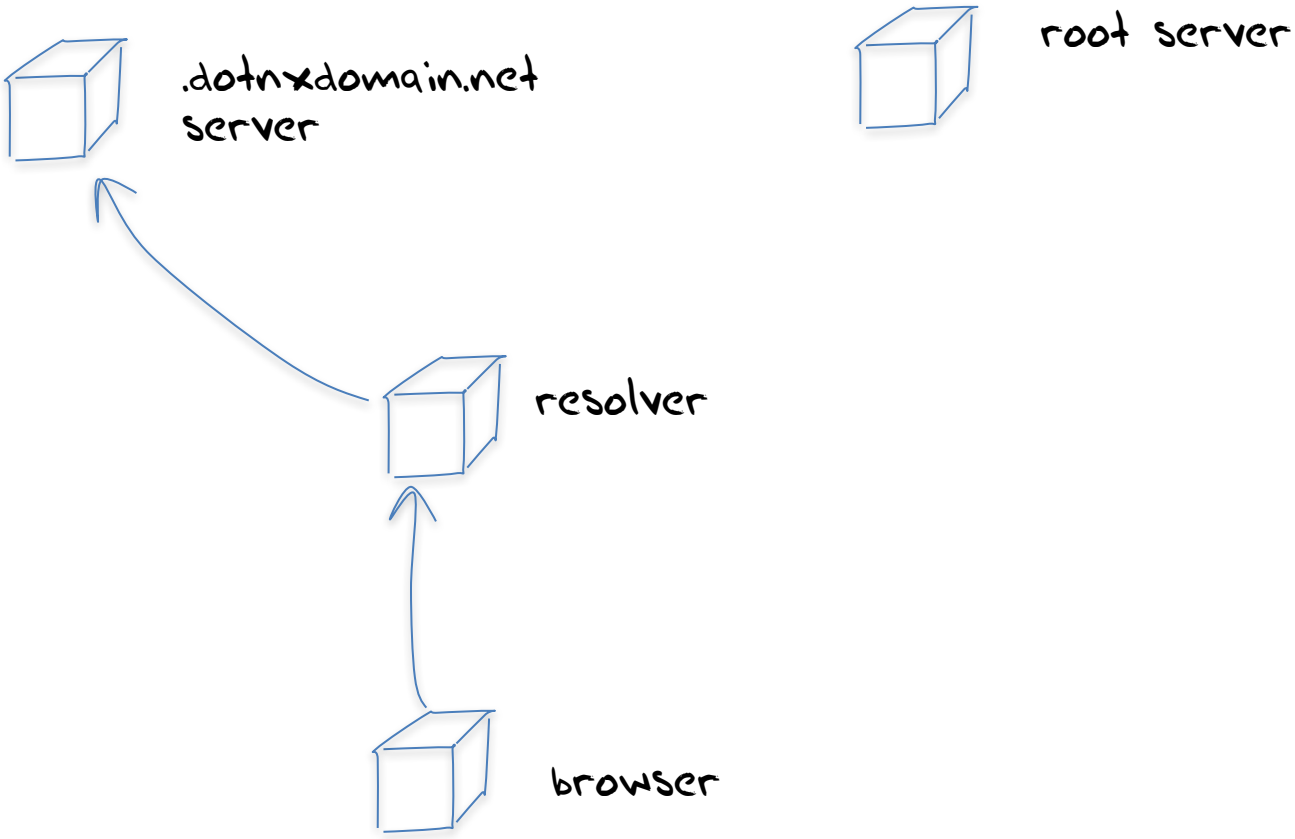
Query directed to the root

c.14u-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net.
c.14s-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net.
c.1du-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net.

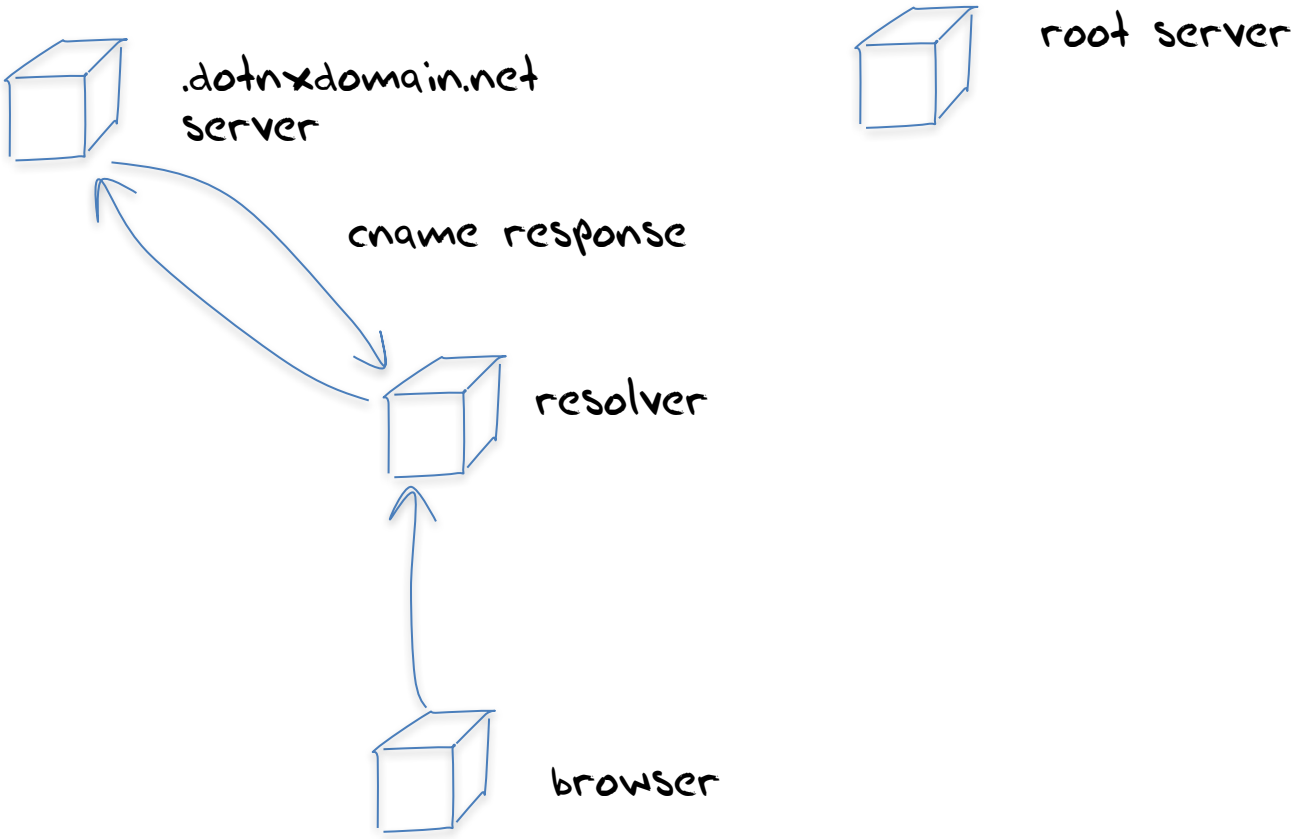
Queries directed to the experiment's server

These will resolve to a CNAME that redirects the resolver towards a non-existant domain name (that will be seen at a root server)

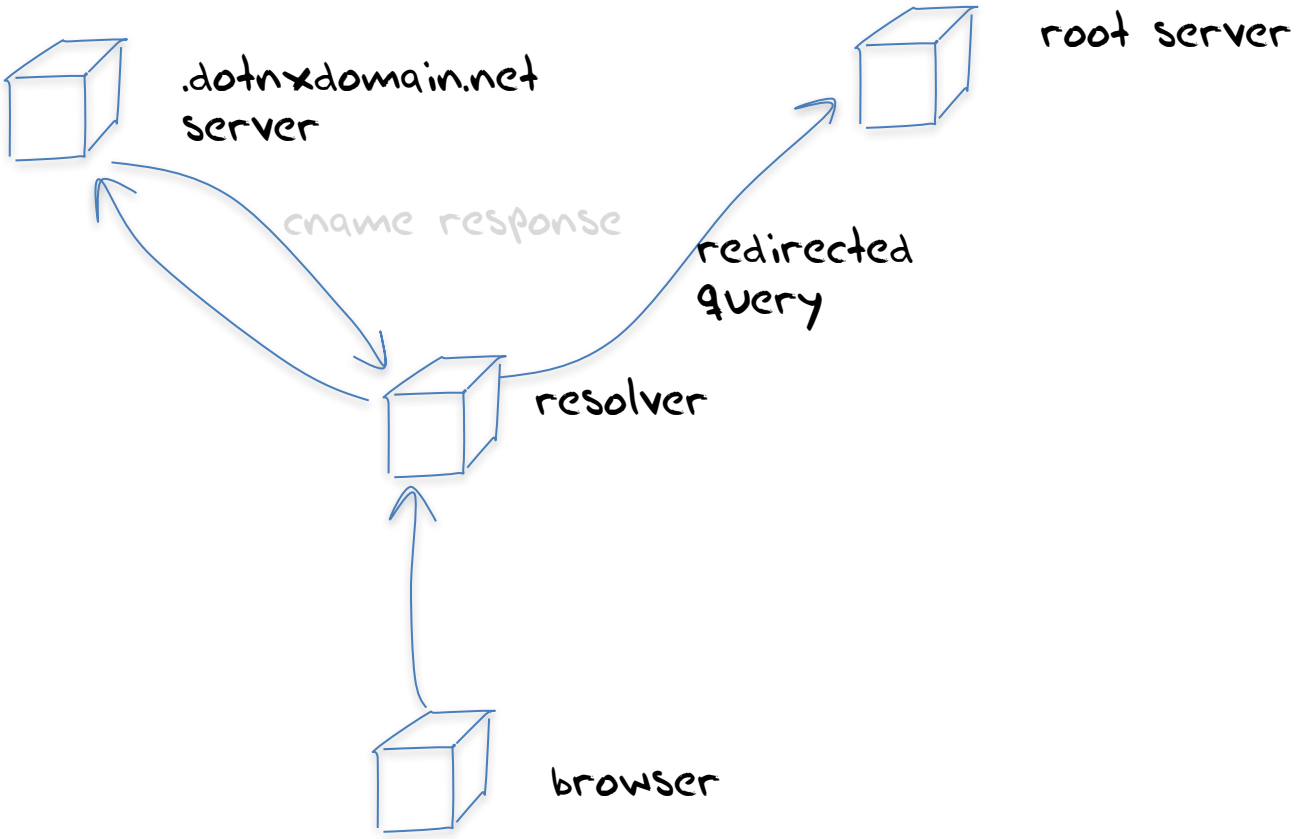
Query Behaviour



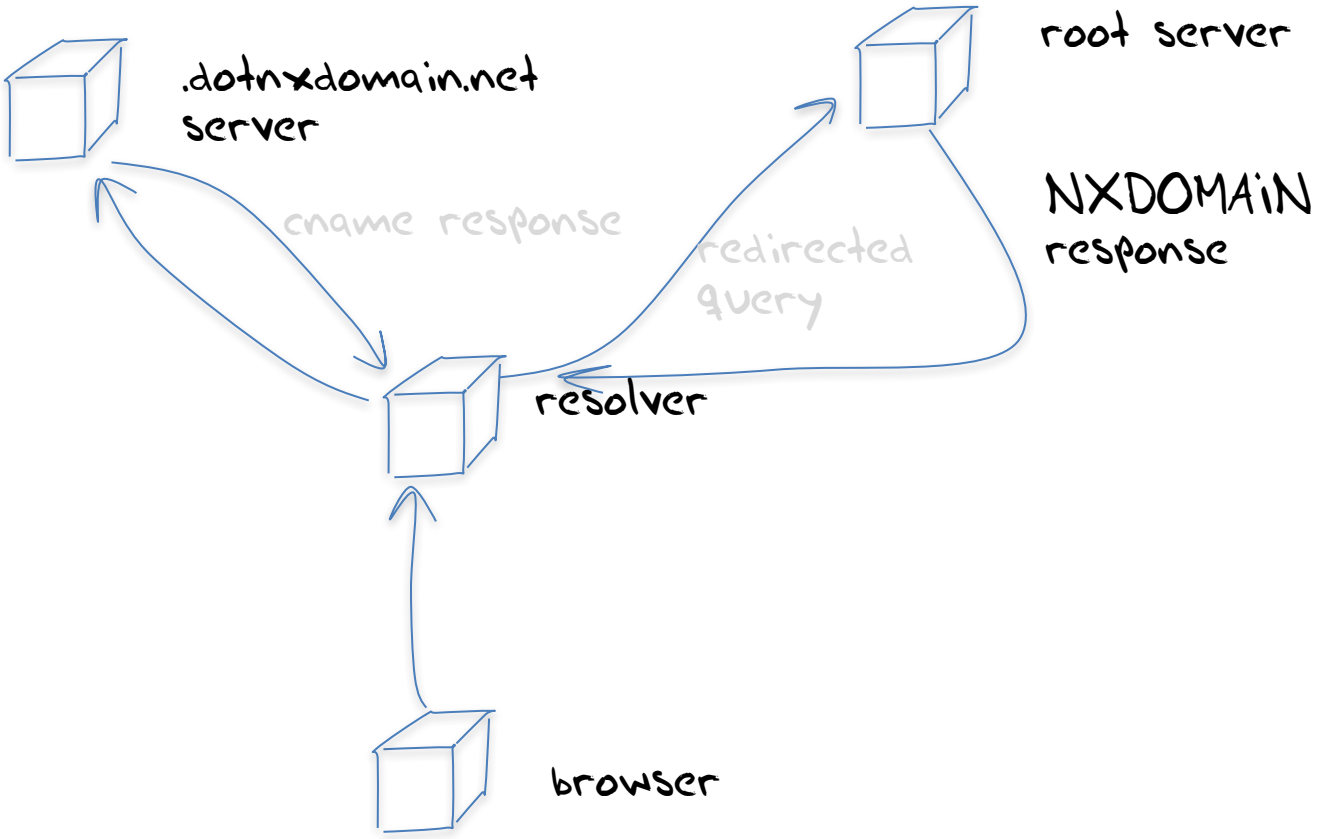
Query Behaviour



Query Behaviour



Query Behaviour



Seen at the APNIC Server

04:40:28.029000 client 153.128.52.x#20314: q: c.14u-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net. IN AAAA
04:40:28.028924 client 153.128.52.x#20822: q: c.14u-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net. IN A
04:40:28.025044 client 153.128.52.x#20448: q: c.14s-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net. IN A
04:40:28.045443 client 153.128.52.x#20069: q: c.1du-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net. IN A
04:40:28.046542 client 153.128.52.x#20876: q: c.14s-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net. IN AAAA
04:40:28.057989 client 153.128.52.x#21203: q: c.1du-u2f235731-c113-s1488343227-ib4040201.ape.dotnxdomain.net. IN AAAA

The end user appears to be a dual stack-connected device and these queries all generate CNAME responses that redirect the resolver to an undelegated name

Seen at a Root Server

04:40:27.980944 IP 153.128.52.x#20983: q: w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-apnic-test. IN AAAA
04:40:27.983060 IP 153.128.52.x#20339: q: w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-apnic-test. IN A
04:40:28.121397 IP 153.128.52.x#20104: q: w.w.w.14u-u2f235731-c113-s1488343227-ib4040201-cname-apnic-test. IN AAAA
04:40:28.146902 IP 153.128.52.x#20336: q: w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-cname-apnic-test. IN A
04:40:28.440938 IP 153.128.52.x#20460: q: w.w.w.14s-u2f235731-c113-s1488343227-ib4040201-cname-apnic-test. IN A

Seen at a Root Server

04:40:27.980944 IP 153.128.52.x#20983: q: w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-apnic-test. IN AAAA
04:40:27.983060 IP 153.128.52.x#20339: q: w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-apnic-test. IN A

These queries were originally directed to a root

04:40:28.121397 IP 153.128.52.x#20104: q: w.w.w.14u-u2f235731-c113-s1488343227-ib4040201-cname-apnic-test. IN AAAA
04:40:28.146902 IP 153.128.52.x#20336: q: w.w.w.1du-u2f235731-c113-s1488343227-ib4040201-cname-apnic-test. IN A
04:40:28.440938 IP 153.128.52.x#20460: q: w.w.w.14s-u2f235731-c113-s1488343227-ib4040201-cname-apnic-test. IN A

CNAME-generated responses that direct the resolver to a root. *

* Why are the cname generated queries only for A OR AAAA and not both?

Query Ratio

- Each experiment generates approximately the same number of queries towards a root server as to the experiment's server (5:6)
- But we are using the logs from a single root server here
- If resolvers evenly distribute queries across all root server letters over time then we could expect to see a query ratio of 0.08 in the data

Query Ratio

Average query ratio: 0.06

This slightly less than the anticipated number

A possible reason is that the larger resolvers are performing some form of local root zone caching

Query Ratio

If

- the resolver is performing NSEC caching, or
- the resolver is working with a local copy of the root zone (RFC7706), or
- The resolver has latched onto a different root server letter,

Then we should see a far lower query ratio for that resolver

Google PDNS Query Ratio

Google DNS query ratio: 0.0008

- This is around 1/100 of the calculated ratio
- It is a likely side effect of some form of NSEC caching being performed by Google's resolvers

Comcast Resolver Query Rate

Comcast DNS query ratio: 0.004

- This is 1/20 of the expected query rate – either Comcast's resolvers are performing some form of local root zone caching or their resolvers have latched onto a different Root Zone server letter

Correlation

- In a one month period (Feb 17) 10,000 resolvers made 90% of the queries to the experiment servers (out of a total of 375,206 resolver IP addresses)
- Of these 10,000 resolvers:
  - 8,600 were seen by this root server letter cluster
  - 1,400 were not seen at all by this root server letter (of these 1,116 were IPv6 addresses, indicating a possible IPv6 reachability issue with this root server)

Correlation

These 8,600 resolvers:

- Made 75% of the queries seen at the experiment servers
- Made 87% of the experiment-related queries seen at this root
- Appear to carry the bulk of the browser level DNS resolution traffic for the Internet

Preliminary Findings

- Most of the resolvers seen at the root appear to make a very small number of queries
  - 99% of the seen resolvers asking queries of the root are responsible for less than 4% of the total query count
  - 10% of the seen resolvers ask only for non-existent domain names
  - This is a very long tail distribution set

Preliminary Findings

- Resolvers who are seen to query at lower levels of the DNS are also likely to be seen by the root servers
  - Although the intensity of queries may differ due to various forms of local root zone content caching

- The opposite is not necessarily the case, in that resolvers seen to ask queries of the root may not necessarily be observed asking queries of servers at lower levels of the DNS (10% of the seen resolvers were not observed to ask a query about a delegated name)

Preliminary Findings

- Resolvers appear to be less likely to exclusively latch onto a single root letter, and appear to distribute their queries to all root server letters over time

Preliminary Findings

- Some resolvers (and some large scale resolvers) are using either NSEC caching or some form of RFC7706-style of local root zone caching
- This has dramatically reduced their query rate to root servers for non-existent domain names

Preliminary Findings

- IPv6 still presents some reachability issues for some roots and some resolvers

This is work in progress

Further questions in this study:

- Can we map users to the resolvers to root server letter preference (if any)?
- Can we cast any light on resolver “latching” to a root service letter?
- How widespread are the IPv6 connectivity issues?
- Can we track the uptake of aggressive NSEC caching of the root zone in resolvers?

Questions?