

How Ready is the global DNS for IPv6?

Ralf Weber

16.2.2023



Introduction and methodology

- Inspired by Momoka Yamamotos OARC39 talk
- Gather large FQDN data sets
 - From our anonymized customer logs
 - From domain categorisation
- Run resolution to find zone cuts
 - Gets a smaller number of delegated domains
 - The reachability of the name server is the same for all its FQDNs
- Check if delegated domains are reachable
 - Over dual stack
 - Over v4 only
 - Over v6 only

Global Query Data

Worldwide
service
providers



Real-time
anonymized
query streams
200-300B/day

Akamai
infrastructure



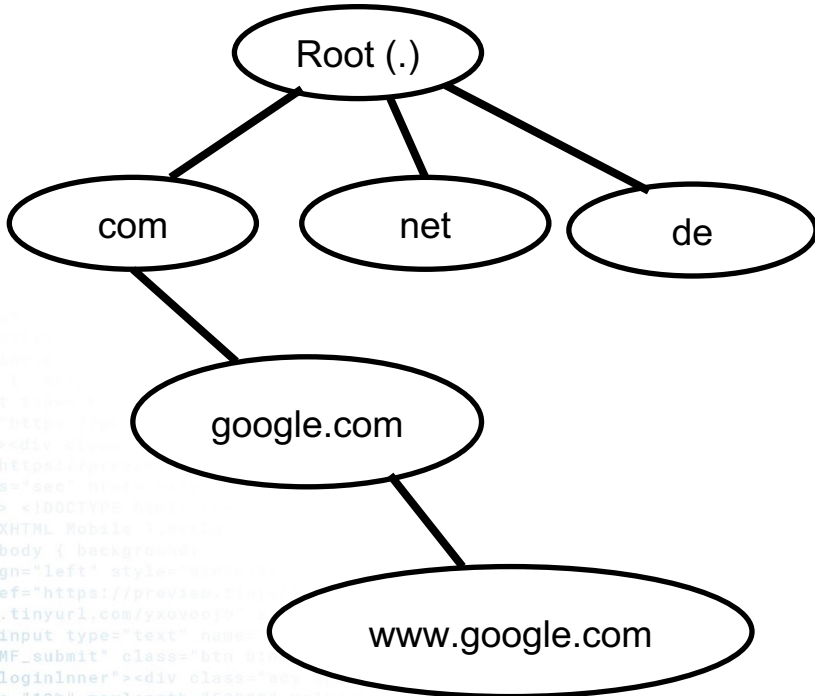
Data science
Security research



Data analysed

- From customer query logs
 - 300 billion queries (302,956,617,039)
 - 1 week of data
 - ~500kqps average
 - 2 billion unique FQDNs (2,241,672,371)
- From domain categorisation
 - 100 million categorised domains (106,401,193)

DNS delegation



```
; <<>> DiG 9.16.1-Ubuntu <<>> +trace +nodnssec www.google.com
;; global options: +cmd
.      452735 IN NS  a.root-servers.net.
.      452735 IN NS  b.root-servers.net.
.      452735 IN NS  c.root-servers.net.
.      452735 IN NS  d.root-servers.net.
.      452735 IN NS  e.root-servers.net.
.      452735 IN NS  f.root-servers.net.
.      452735 IN NS  g.root-servers.net.
.      452735 IN NS  h.root-servers.net.
.      452735 IN NS  i.root-servers.net.
.      452735 IN NS  j.root-servers.net.
.      452735 IN NS  k.root-servers.net.
.      452735 IN NS  l.root-servers.net.
.      452735 IN NS  m.root-servers.net.
;; Received 239 bytes from 127.0.0.53#53(127.0.0.53) in 4 ms
```

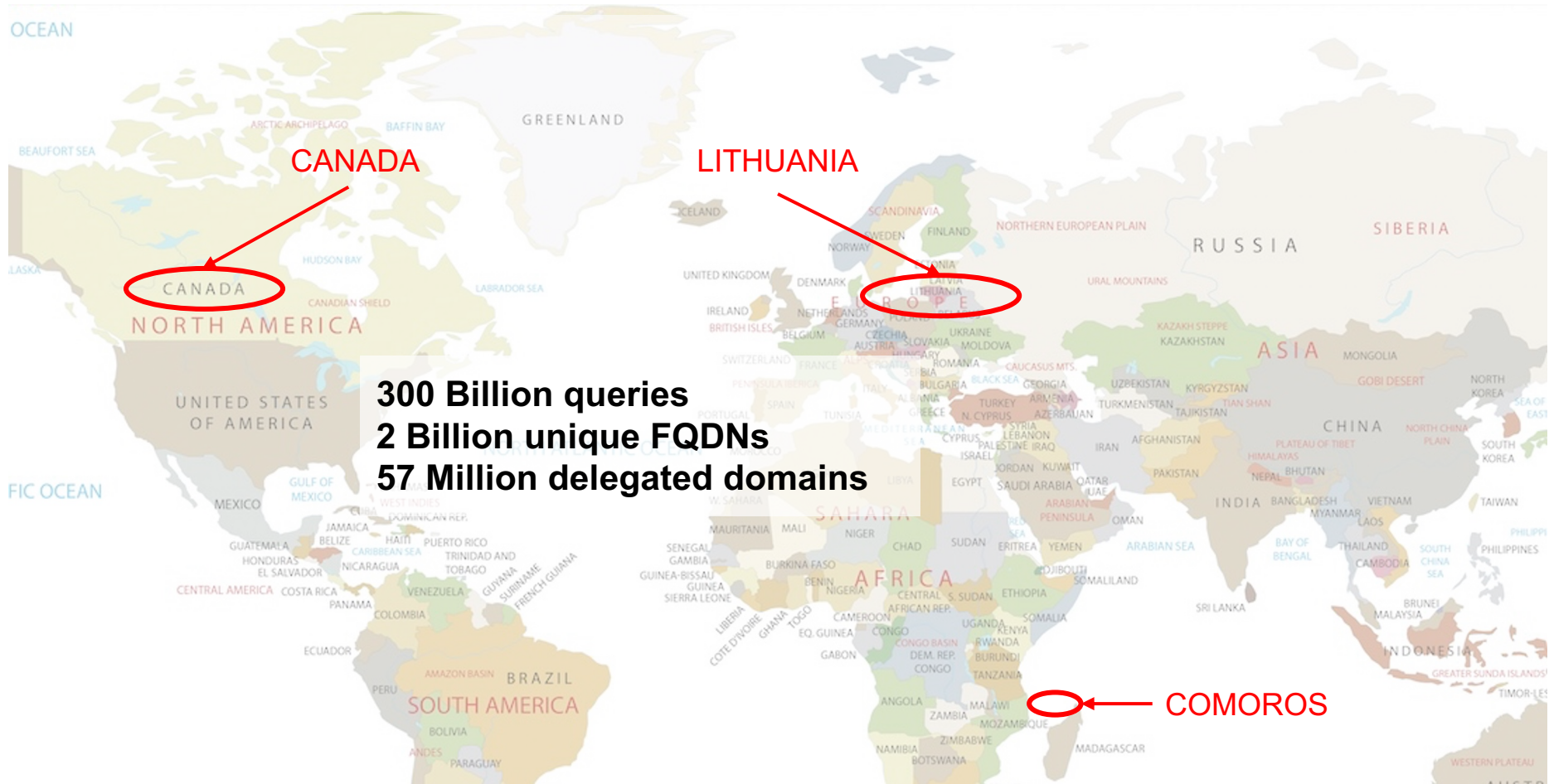
```
com.    172800 IN NS  a.gtld-servers.net.
com.    172800 IN NS  b.gtld-servers.net.
com.    172800 IN NS  c.gtld-servers.net.
com.    172800 IN NS  d.gtld-servers.net.
com.    172800 IN NS  e.gtld-servers.net.
com.    172800 IN NS  f.gtld-servers.net.
com.    172800 IN NS  g.gtld-servers.net.
com.    172800 IN NS  h.gtld-servers.net.
com.    172800 IN NS  i.gtld-servers.net.
com.    172800 IN NS  j.gtld-servers.net.
com.    172800 IN NS  k.gtld-servers.net.
com.    172800 IN NS  l.gtld-servers.net.
com.    172800 IN NS  m.gtld-servers.net.
;; Received 839 bytes from 199.7.83.42#53(1.root-servers.net) in 8 ms
```

```
google.com. 172800 IN NS  ns2.google.com.
google.com. 172800 IN NS  ns1.google.com.
google.com. 172800 IN NS  ns3.google.com.
google.com. 172800 IN NS  ns4.google.com.
;; Received 291 bytes from 2001:503:d2d::30#53(k.gtld-servers.net) in 148 ms
```

```
www.google.com. 300 IN A 142.250.184.228
;; Received 59 bytes from 216.239.38.10#53(ns4.google.com) in 8 ms
```

Delegated domains

- From customer query logs
 - 57 million (57,371,853)
 - 45 million caused by singular hits (44,933,295)
 - 2 billion out of 300 billion requests (1,916,121,064)
- From domain categorisation
 - 49 million (48,949,650)
- Overall
 - 86 million (85,989,871)



A word on one hit wonders

- googlesyndication.com.
 - by far the most “popular” one FQDN hit machine (1% of single hit traffic)
 - gstatic.com, google.com are also towards the top of the list
- s3.amazonaws.com.
 - Sort of expected as some S3 buckets are not popular
- guizhou.gov.cn.
 - The Chines province of Guizho (no idea why)
- Lots of CDNs and “Measurement”
 - Amazon, Netflix, Dailymotion, Microsoft, Nielsen, Cedexis

One hit wonder patterns

- "Random" prefixes or encodings?
 - ybar-bojdu3dss2report.wc.yahoodns.net
 - aa4e403b69cfce762947190e3a48cf0e.safeframe.google syndication.com
 - ad24a7b45dc44618a3cf2982c783da65.fp.measure.office.com
 - avian-jaguar-wo5crsw3ll45xhg6q393txol.www.oiegmycentre.com.herokudns.com
 - aifbva6ppo33cirsbhgyb2od7jbhq1670081759.nuid.imrworldwide.com
 - i2-aveyyuahbfwvmnlyobpcpuuzhcbeki.init.cedexis-radar.net
- Word riddles?
 - w1boardsdev2b0bciphoneapi5-gallery-content-2018.peck.gat.guizhou.gov.cn
 - mta-sts.audibene-info.mail.eo.cadburygifting.in
 - gluta-panacea-online.ipaidthat.io

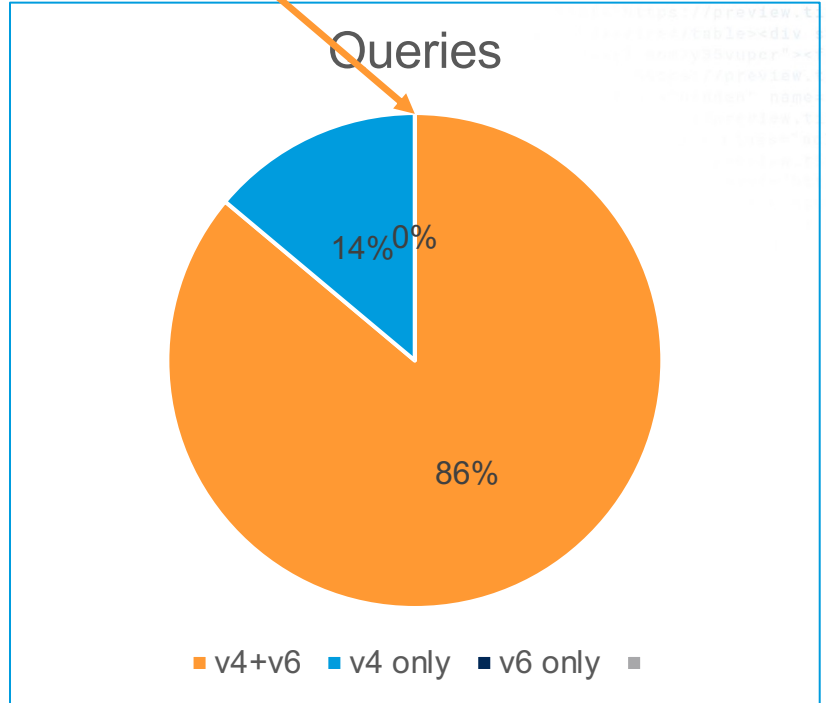
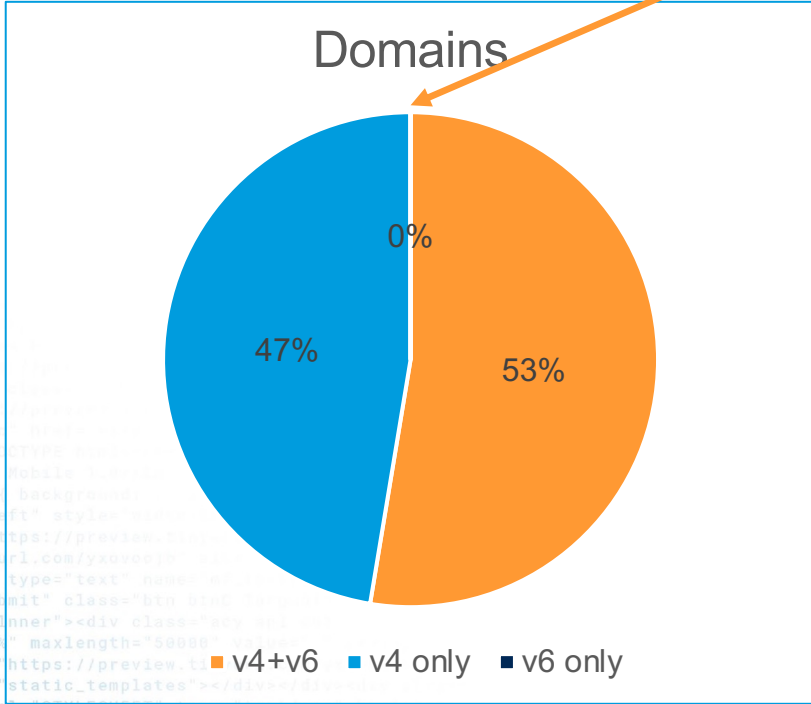
Looking through the data

- Using 100 instances to crawl through data
- Discovering zone cuts from 2 billion FQDNs took two weeks
 - No DNSSEC, 0x20 or qname minisation
- Discovering resolution results for 86 million domains took 11 days
 - Three resolution attempts (dual stack, v4, v6)
 - Failed queries take much longer than successful
- DNS is dynamic
 - 4.7 million delegated domains SERVFAIL (4,781,809)
 - 2 million no longer exist – NXDomain (1,942,818)
 - 80 millions to consider (79,265,244)

The results are in

337 domains

413654 queries



Looking at TLDs

- Most TLDs support IPv6
 - 1477 observed
 - 23 are IPv4 only
- Common TLDs are most popular
 - Most common
 - Com
 - Net
 - Org
 - lo
 - Hk
- Failed TLDs ->

to.
sl.
mp.
cd.
uz.
dj.
ck.
et.
mm.
kp.
hm.
sr.
gf.
pf.
fk.
mq.
mh.
xn--ygbi2ammx.
xn--wgbh1c.
xn--mgba3a4f16a.
xn--mgbai9azgqp6j.
xn--l1acc.
xn--lgbbat1ad8j.

What causes IPv6 only failures

- Name Servers need to be reachable over IPv6
- So this should be ok ?

```
;; <<>> DiG 9.16.1-Ubuntu <<>> hwcdn.net. NS @2001:4de0:ac11::1:0:1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32694
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;hwcdn.net.          IN  NS

;; ANSWER SECTION:
hwcdn.net.          86400  IN  NS  ns1.hwcdn.net.
hwcdn.net.          86400  IN  NS  ns2.hwcdn.net.

;; ADDITIONAL SECTION:
ns1.hwcdn.net.     86400  IN  A    69.16.174.10
ns1.hwcdn.net.     3600   IN  AAAA 2001:4de0:ac11::1:0:1
ns2.hwcdn.net.     86400  IN  A    209.197.2.10
ns2.hwcdn.net.     3600   IN  AAAA 2001:4de0:ac12::1:0:2

;; Query time: 0 msec
;; SERVER: 2001:4de0:ac11::1:0:1#53(2001:4de0:ac11::1:0:1)
;; WHEN: Mon Feb 13 03:46:58 UTC 2023
;; MSG SIZE rcvd: 151
```

What causes IPv6 only failures

- Name Servers need to be reachable over IPv6
- So this should be ok ?
- No because delegation happens at the parent
- **You need to add your IPv6 name server to the parent through your registrar**

```
;<<>> DiG 9.16.1-Ubuntu <<>> hwcdn.net. NS @c.gtld-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16289
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
hwcdn.net.                IN      NS

;; AUTHORITY SECTION:
hwcdn.net.                172800 IN      NS    ns2.hwcdn.net.
hwcdn.net.                172800 IN      NS    ns1.hwcdn.net.

;; ADDITIONAL SECTION:
ns2.hwcdn.net.           172800 IN      A      209.197.2.10
ns1.hwcdn.net.           172800 IN      A      69.16.174.10

;; Query time: 0 msec
;; SERVER: 2001:503:83eb::30#53(2001:503:83eb::30)
;; WHEN: Mon Feb 13 03:50:51 UTC 2023
;; MSG SIZE rcvd: 106
```

Top 10 IPv4 only domains

akadns.net. ← Ooops

trafficmanager.net.

g.aaplimg.com.

fastly.net.

bytefcdn-oversea.com.

ovscdns.net.

wsdvs.com.

v.aaplimg.com.

ms-acdc.office.com.

ha.office365.com.

Top 10 IPv4 only domains

akadns.net.



Ooops (it
can happen)

trafficmanager.net.

g.aaplimg.com.

fastly.net.

bytefcdn-oversea.com.

ovscdns.net.

wsdvs.com.

v.aaplimg.com.

ms-acdc.office.com.

ha.office365.com.

```
;<<<> DiG 9.16.1-Ubuntu <<<> akadns.net @d.gtld-servers.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 4033
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;akadns.net.          IN      A

;; AUTHORITY SECTION:
akadns.net.          172800 IN      NS      a3-129.akadns.net.
akadns.net.          172800 IN      NS      a7-131.akadns.net.
akadns.net.          172800 IN      NS      a11-129.akadns.net.
akadns.net.          172800 IN      NS      a1-128.akadns.net.
akadns.net.          172800 IN      NS      a9-128.akadns.net.
akadns.net.          172800 IN      NS      a5-130.akagtm.org.
akadns.net.          172800 IN      NS      a28-129.akagtm.org.
akadns.net.          172800 IN      NS      a13-130.akagtm.org.
akadns.net.          172800 IN      NS      a18-128.akagtm.org.
akadns.net.          172800 IN      NS      a12-131.akagtm.org.

;; ADDITIONAL SECTION:
a3-129.akadns.net.  172800 IN      A       96.7.49.129
a7-131.akadns.net.  172800 IN      A       23.61.199.131
a11-129.akadns.net. 172800 IN      A       84.53.139.129
a1-128.akadns.net.  172800 IN      A       193.108.88.128
a9-128.akadns.net.  172800 IN      A       184.85.248.128

;; Query time: 0 msec
;; SERVER: 2001:500:856e::30#53 (2001:500:856e::30)
;; WHEN: Mon Feb 13 04:11:51 UTC 2023
;; MSG SIZE rcvd: 344
```


Top 10 IPv6 only domains

jiangxi.gov.cn

hitlist.sdstrowes.co.uk.

cns.mtnet.gov.tw.

dnsbl.beetjevremd.nl.

cablevideodigital.com.

rpkitest6.nlnetlabs.nl.

bionik.tv.

costumemaker.com.

v6-any1.67ysto.c.100e6.net.

v6-any2.67ysto.c.100e6.net.

What ?



Top 10 IPv6 only domains

jiangxi.gov.cn

hitlist.sdstrowes.co.uk.

cns.mtnet.gov.tw.

dnsbl.beetjevremd.nl.

cablevideodigital.com.

rpkitest6.nl.netlabs.nl.

bionik.tv.

costumemaker.com.

v6-any1.67ysto.c.100e6.net.

v6-any2.67ysto.c.100e6.net.

What ?

```
;; AUTHORITY SECTION:
cablevideodigital.com. 172800 IN NS ns1.cablevideodigital.com.
cablevideodigital.com. 172800 IN NS ns2.cablevideodigital.com.

;; ADDITIONAL SECTION:
ns1.cablevideodigital.com. 172800 IN A 131.255.63.232
ns1.cablevideodigital.com. 172800 IN AAAA 2803:5b80::232
ns2.cablevideodigital.com. 172800 IN A 131.255.63.232
ns2.cablevideodigital.com. 172800 IN AAAA 2803:5b80::232
```

- Domains have IPv4 addresses
- But don't respond if IP is not a known nameserver
- These "protections" are not active on IPv6



Takeaways

- DNS is not IPv6 ready
 - Especially the long tails and CDNs need work
 - Popular stuff looks better
- Actions needed
 - Add IPv6 addresses to your name servers
 - **Register them in the parent**

Questions



