Is Your Caching Resolver Polluting the Internet?

Duane Wessels
The Measurement Factory, and
CAIDA
wessels@measurement-factory.com

September 2004

A Disclaimer

- This data comes from monitoring two instances of the "F" DNS root server
  - Introduces some biases
  - We may be missing something interesting that occurs elsewhere
- It would be nice if we had additional data from other sources, like
  - Authoritative TLD and SLD servers
  - A variety of caching resolvers
- I'll try to not make this not all about the root servers.

What is DNS pollution?

- A-for-A queries
- A-for-. queries
- Queries and Updates for RFC 1918 Addresses
- Queries for Invalid TLDs
- Excessive Queries for [a–m].root-servers.net
- IPv6 Address Queries
- Repeated Queries
- Queries from Unroutable/Unreachable Sources

Why is this DNS pollution?

- Some queries are unanswerable because the server is not authoritative for the domain in question. e.g., lame delegation and "NXDOMAIN" replies.
- Some queries are unanswerable because the server cannot talk back to the client.
- Some represent local/private information that escapes onto the public Internet.
- Some queries are valid, but occur much more frequently than they would for properly configured systems.

A-for-A Queries

```
22:33:57.847573 228.57.66.241.53 > F.53:  52586 A? 93.122.94.102.
22:33:57.868436 11.176.132.84.31790 > F.53:  32062 A? 209.185.151.123.
22:33:57.879179 152.68.35.117.49283 > F.53:  6958 A? 4.43.140.160.
22:33:57.886175 78.150.111.9.42094 > F.53:  32304 A? 60.141.241.142.
22:33:57.888548 176.17.50.38.49902 > F.53:  17622 A? 203.66.149.153.
22:33:57.899417 19.191.37.135.53 > F.53:  55410 A? 151.208.189.26.
22:33:57.903560 176.17.50.38.49902 > F.53:  33116 A? 149.109.60.44.
22:33:57.916032 128.190.104.73.53 > F.53:  43559 A? 249.54.212.95.
22:33:57.921030 166.203.102.109.33638 > F.53:  57797 A? 88.116.197.24.
22:33:57.924153 144.137.97.110.32787 > F.53:  46316 A? 187.5.78.189.
22:33:57.924177 55.94.177.203.53 > F.53:  62802 A? 145.248.229.75.
```

- Caused by buggy Windows NT DNS server
- Some resolvers (i.e., djbdns) recognize and answer these queries.

A-for-. Queries

```
22:33:57.846826 233.214.38.235.1428 > F.53:  7360 A? .
22:33:57.851070 7.153.231.207.1117 > F.53:  12747 A? .
22:33:57.851696 14.102.158.207.33210 > F.53:  11210 A? .
22:33:57.851720 63.217.38.83.3924 > F.53:  7232 A? .
22:33:57.854827 14.102.158.207.33210 > F.53:  5078 A? .
22:33:57.859066 214.130.138.39.3004 > F.53:  14319 A? .
22:33:57.862064 233.214.38.235.1428 > F.53:  5334 A? .
22:33:57.867436 7.153.231.207.1117 > F.53:  12764 A? .
22:33:57.869584 63.217.38.83.3924 > F.53:  11348 A? .
22:33:57.872433 14.102.158.207.33210 > F.53:  3039 A? .
22:33:57.877180 63.217.38.83.3924 > F.53:  9308 A? .
22:33:57.877205 233.214.38.235.1428 > F.53:  1243 A? .
```

- Caused by buggy resolvers that accept null query names?
- Why not have the resolver recognize and stop these?

RFC 1918 Addresses

```
22:33:57.875681 102.31.88.27.53 > F.53:  12270 PTR? 185.25.73.198.in-addr.arpa.
22:33:57.927422 170.106.101.76.53 > F.53:  11308 PTR? 228.114.106.114.in-addr.arpa
22:33:57.983493 21.230.155.233.21301 > F.53:  10007 PTR? 122.101.201.23.in-addr.ar
22:33:58.029992 21.230.155.233.21301 > F.53:  10008 PTR? 122.101.201.23.in-addr.ar
22:33:58.040788 64.207.181.62.53 > F.53:  6518 PTR? 191.246.143.93.in-addr.arpa.
22:33:58.042961 64.207.181.62.53 > F.53:  9522 PTR? 236.192.208.156.in-addr.arpa.
22:33:58.049204 30.82.18.155.53 > F.53:  2636 PTR? 120.93.57.129.in-addr.arpa.
22:33:58.061992 21.230.155.233.21301 > F.53:  10009 PTR? 122.101.201.23.in-addr.ar
22:33:58.073315 17.39.143.35.1116 > F.53:  9518 SOA? 51.50.10.in-addr.arpa.
22:33:58.091679 21.230.155.233.21301 > F.53:  10010 PTR? 122.101.201.23.in-addr.ar
```

- Sites that use RFC 1918 addresses should configure their resolver to answer authoritatively for them.
- The AS112 project servers take the bulk of this abuse.
  - 20 anycasted servers authoritative for RFC 1918 space
  - Certain popular operating systems enable dynamic DNS update by default

Invalid TLDs

```
22:33:57.847825 57.95.26.22.32988 > F.53:  52024 SOA? _ldap._tcp.ForestDnsZones.Primefuels.local.
22:33:57.850071 229.97.210.1.2796 > F.53:  9490 A? 7741-S4.7741-SW.
22:33:57.853445 175.252.10.24.32829 > F.53:  4035 SOA? _kpasswd._udp.D-4240669.S3000.
22:33:57.856318 101.71.170.2.53 > F.53:  44256 MX? w.r[.
22:33:57.856692 101.71.170.2.53 > F.53:  55176 SOA? _ldap._tcp.Default-First-Site._sites.DomainDnsZones.chapplehome.l
22:33:57.867812 160.182.126.21.38242 > F.53:  10314 AAAA? rnde16.
22:33:57.867837 93.239.82.47.51595 > F.53:  11231 A? localhost.
22:33:57.872558 11.131.20.20.53 > F.53:  59300 SOA? _ldap._tcp.18a20066-37fb-420b-a406-2c2324dde8f4.domains._msdcs.ya
22:33:57.873182 5.34.171.157.49616 > F.53:  9324 A? src="http-//banners.aftrk.com/ab/lifetimeopportunity/top500/html4
22:33:57.875705 255.91.199.150.52295 > F.53:  38421 SOA? _ldap._tcp.Default-First-Site._sites.gc._msdcs.merlin.local.
22:33:57.882677 69.144.90.160.61075 > F.53:  45124 A? aloha15.domain.local.
22:33:57.883302 87.30.247.246.1029 > F.53:  9760 A? LIVLNX01.bpionet.local.
22:33:57.884926 219.110.202.94.53 > F.53:  29057 A? WEBDEV.beta.enterprise.sscims.cmo.
22:33:57.888424 75.229.97.50.45481 > F.53:  34440 SRV? _ldap._tcp.CAFolsom._sites.dc._msdcs.CARCRDCDB1Y925H.
22:33:57.888984 104.113.9.195.47688 > F.53:  53968 A? denso.
22:33:57.892196 233.168.229.9.26228 > F.53:  5529 A? SCL-TREE.
22:33:57.893173 87.30.247.246.1029 > F.53:  15918 A? LIVLNX01.commonwealthnet.local.
```

- Common invalid TLDs: *localhost*, *local*, *corp*, *workgroup*, *domain*, *htm*, *txt*, *c*
- Negative caching not good enough to stop these

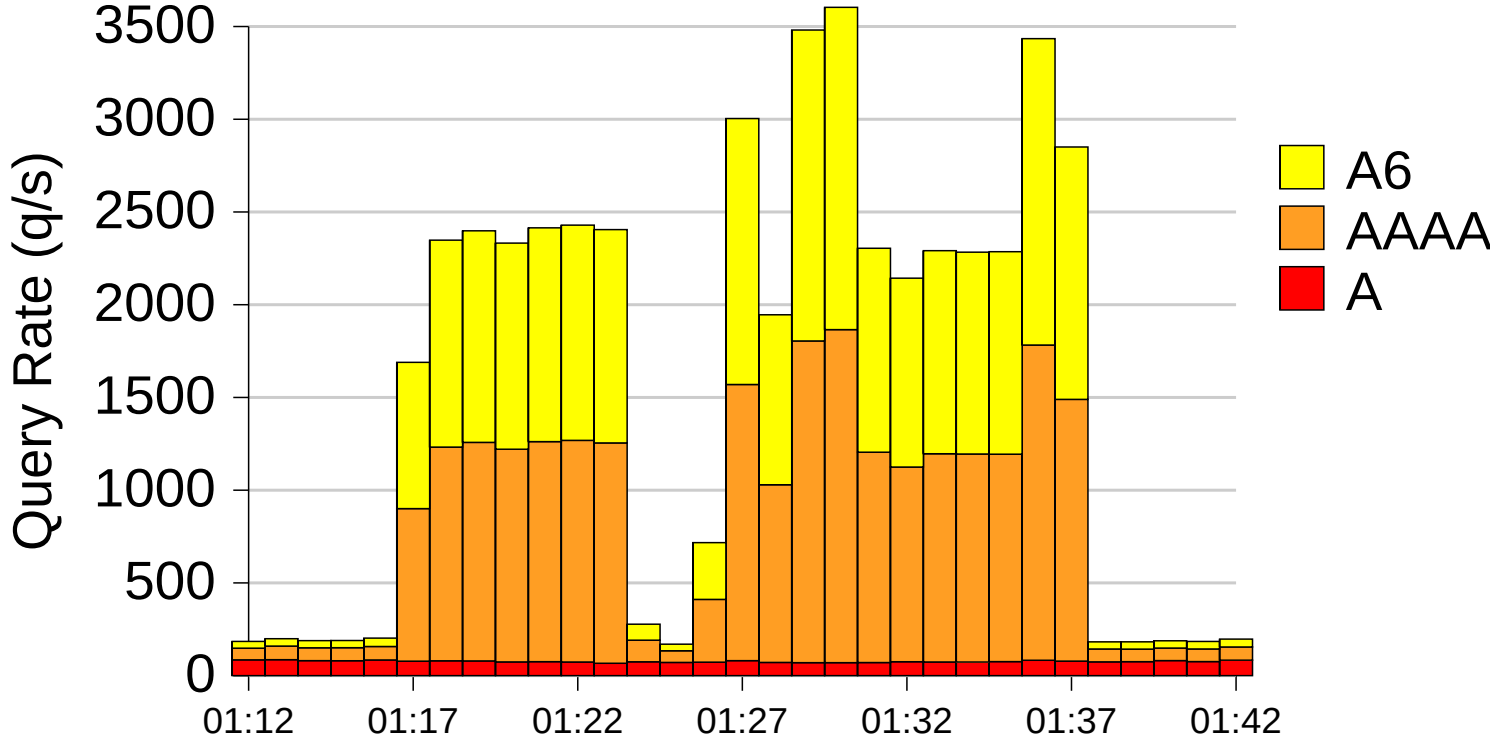
[a-m].root-servers.net

```
20:00:30.085662 80.41.136.212.33821 > F.53:  33822 A6? A.ROOT-SERVERS.NET.
20:00:30.085870 80.41.136.212.33821 > F.53:  31888 AAAA? A.ROOT-SERVERS.NET.
20:00:30.086014 80.41.136.212.33821 > F.53:  51435 A? A.ROOT-SERVERS.NET.
20:00:34.087164 80.41.136.212.33821 > F.53:  36477 A6? A.ROOT-SERVERS.NET.
20:00:34.087394 80.41.136.212.33821 > F.53:  45228 AAAA? A.ROOT-SERVERS.NET.
20:00:34.087663 80.41.136.212.33821 > F.53:  33202 A? A.ROOT-SERVERS.NET.
20:00:38.087294 80.41.136.212.33821 > F.53:  5231 A6? A.ROOT-SERVERS.NET.
20:00:38.087563 80.41.136.212.33821 > F.53:  54557 AAAA? A.ROOT-SERVERS.NET.
20:00:38.087669 80.41.136.212.33821 > F.53:  51685 A? A.ROOT-SERVERS.NET.
20:00:42.098064 80.41.136.212.33821 > F.53:  55265 A6? A.ROOT-SERVERS.NET.
20:00:42.098315 80.41.136.212.33821 > F.53:  112 AAAA? A.ROOT-SERVERS.NET.
20:00:42.098440 80.41.136.212.33821 > F.53:  57604 A? A.ROOT-SERVERS.NET.
20:00:46.091344 80.41.136.212.33821 > F.53:  47264 A6? A.ROOT-SERVERS.NET.
20:00:46.091467 80.41.136.212.33821 > F.53:  27313 AAAA? A.ROOT-SERVERS.NET.
20:00:46.091592 80.41.136.212.33821 > F.53:  25386 A? A.ROOT-SERVERS.NET.
```

[a-m].root-servers.net, cont

- Caching resolvers like to update/validate their "hints" when they startup.
- Some caches query for all 13 root servers, and for both IPv4 and IPv6 addresses.
- Excessive root-servers.net queries usually indicates a unidirectional communication channel.
- Certain versions of BIND sometimes pummel the roots with AAAA and A6 queries for *[a-m].root-servers.net*.

Query Spikes for root-server.net IPv6 addresses



- Sources are BIND 8.3.3 – 8.3.4

IPv6 Address Queries

- Not necessarily pollution, but...
- BIND optimistically issues AAAA and/or A6 queries for other nameservers.
- A random sampling of 3150 authoritative nameservers found 17 (0.5%) with AAAA records, and none with A6 records.

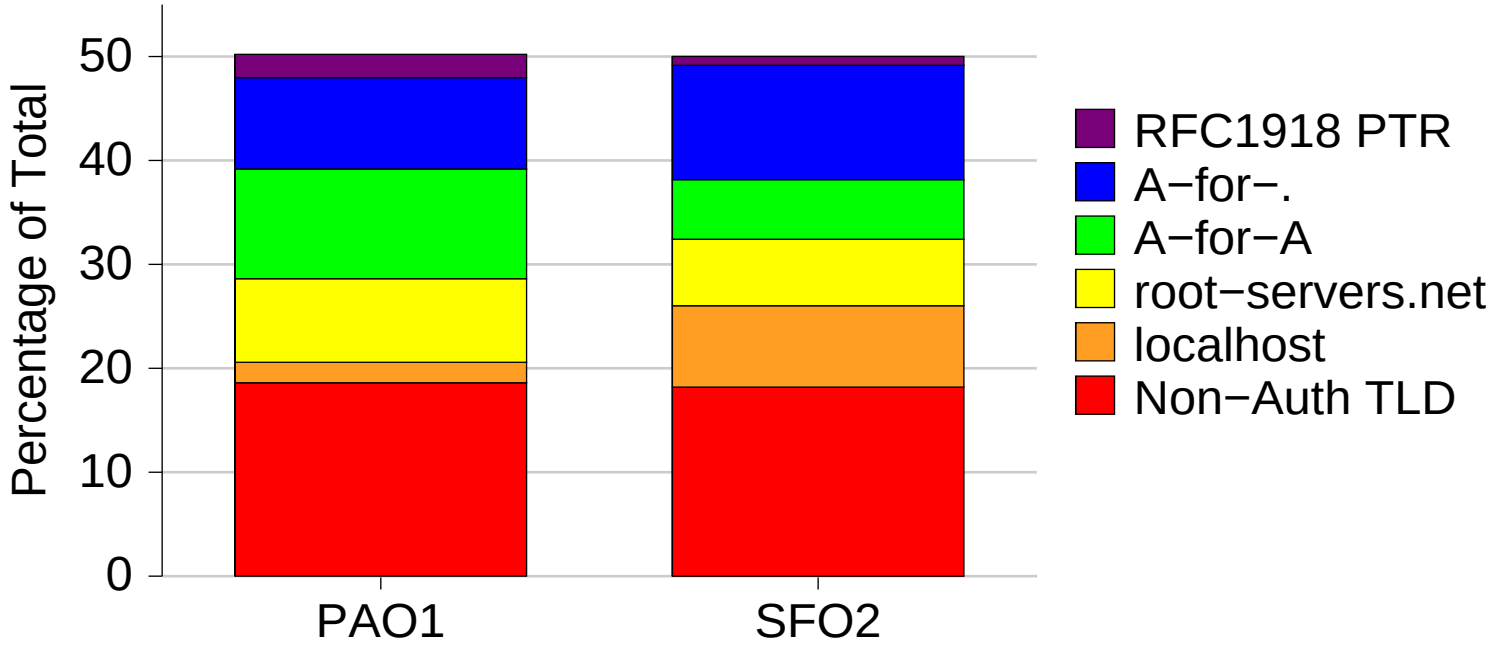
Repeated Queries

- Repeated queries are not included in the current analysis.
- Repeat analysis requires keeping history or state.
- Our real-time analysis tools don't (yet?) keep history.
- Repeated query analysis is complicated by cache poison-prevention techniques. That is, some resolvers start certain queries at the roots, rather than trust cached referrals.
- In an earlier study we found that up to 70% of F-root traffic is repeated queries.

Unroutable/Unreachable Sources

- Source address from RFC 1918 space
- No route back to source address
- DNS reply is blocked by misconfigured packet filter
- Source port is zero

DNS Pollution Seen at F-Root
Aug 20–27, 2004



So What, Who Cares?

- The root servers are generally overprovisioned and the amount of traffic we're talking about is not that significant.
  - okay, but it's not only about the roots
- Viruses, spam, and DDoS represent much, much more pollution than this.
- "The DNS works well enough for me anyway."
- "I run up-to-date code and have smart people working for me. I'm sure my resolvers are well-behaved."
- Your policy may be to not "spy" on your customers.

Why You Should Care

- The Internet is a public commons that we should all strive to keep clean.
- Less pollution makes it easier to differentiate good from bad traffic in the event of a real attack.
- Your DNS pollution may give away private or sensitive information.
- You may discover configuration errors that you didn't know you had.
- As the Balkanization of the Internet continues you'll find that others willingless to communicate with you depends on the amount of garbage leaving your network (DNSBLs, rfc-ignorant, Dshield).

Tools

dnstop

- *dnstop* is a curses-based Unix application that displays sorted tables of DNS queries
- Recent versions have filters to include only certain types of DNS pollution
  - A-for-A queries
  - RFC 1918 PTR queries
  - RFC 1918 UPDATEs
  - Unknown TLDs
- `http://dns.measurement-factory.com/tools/dnstop/`

Finding Invalid TLDs with dnstop

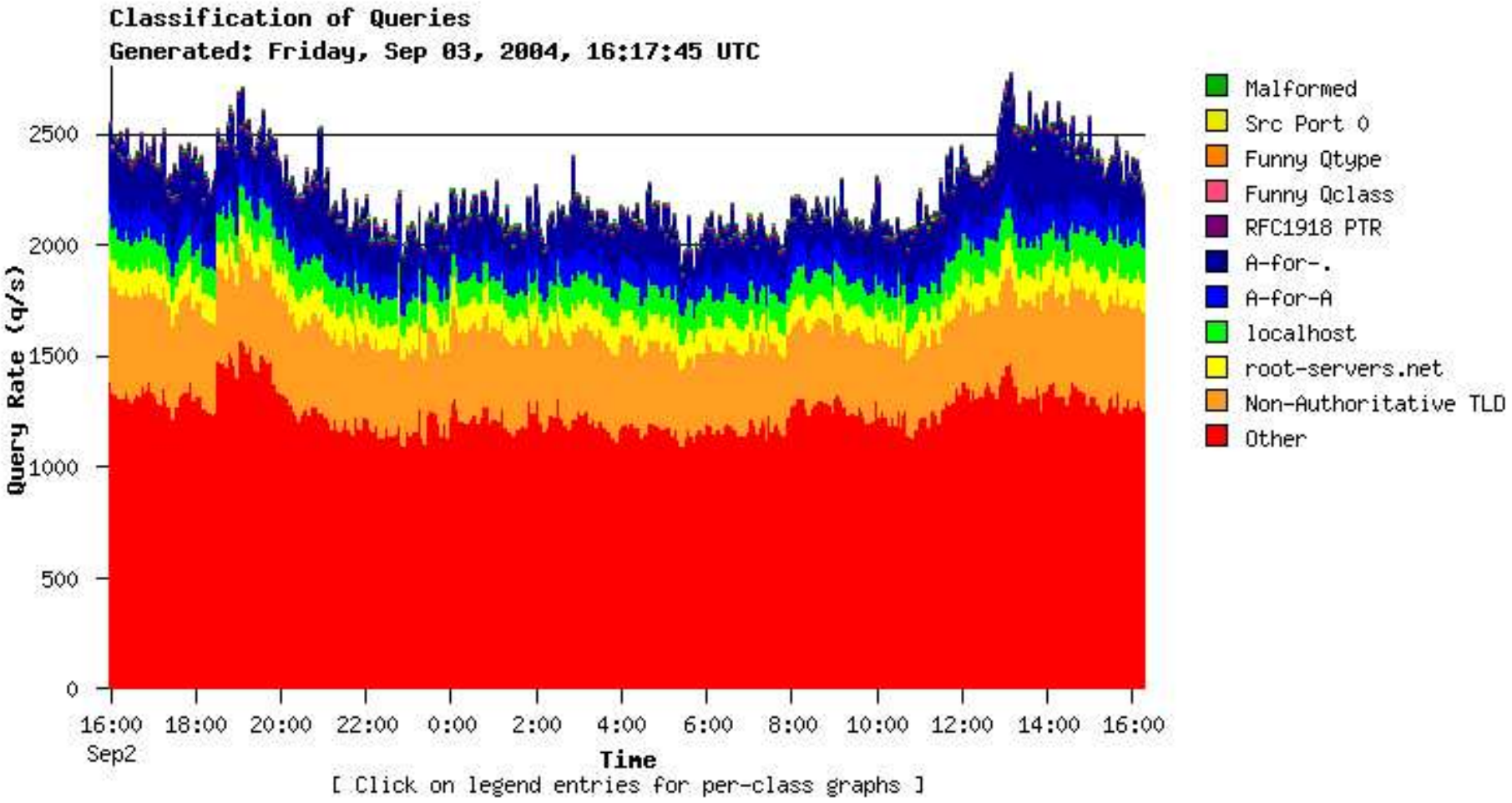
```
Wed Apr 14 19:14:08 2004
9 new queries, 3045 total queries

TLD                       count      %
------------------- --------- ------
local                       414   13.6
localhost                   251    8.2
txt                          85    2.8
147                          31    1.0
1                            23    0.8
invalid                      22    0.7
null                         22    0.7
belkin                       21    0.7
workgroup                    20    0.7
212                          19    0.6
50                           18    0.6
c                            17    0.6
105                          17    0.6
iec                          17    0.6
10                           17    0.6
emails                       17    0.6
2                            16    0.5
8                            15    0.5
56                           15    0.5
3                            14    0.5
lan                          14    0.5
```

DSC: DNS Statistics Collector

- Kind of an "MRTG" for DNS servers
- Colorful, interactive graphs
- Distributed architecture
- Long-term data archival
- Currently "alpha release" quality/status
- `http://dns.measurement-factory.com/tools/dsc/`

DSC Sample Graph



The End