VERISIGN

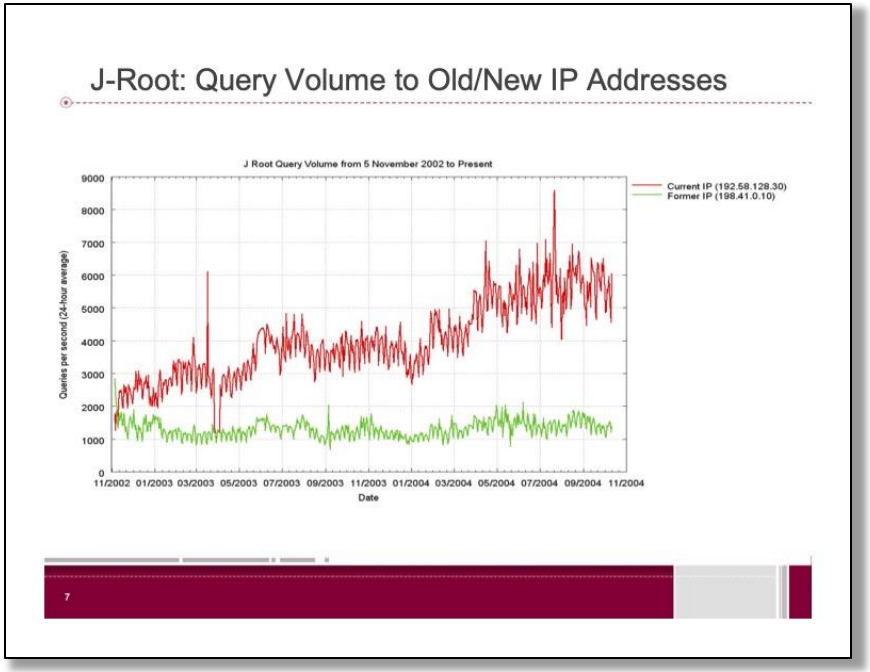
A Break in the Case of Old J-Root Query Traffic

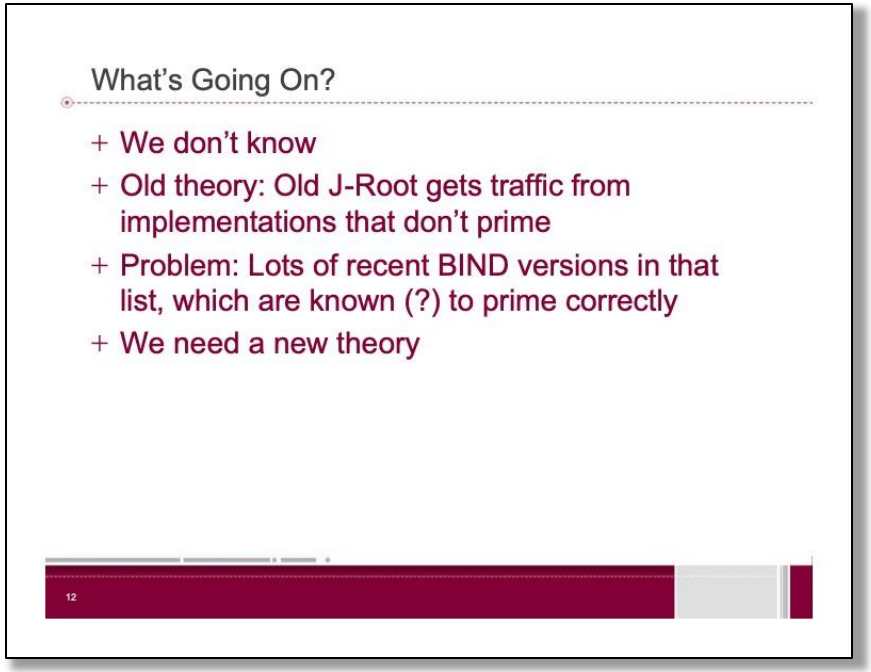
Duane Wessels

DNS-OARC 45

October 5, 2025

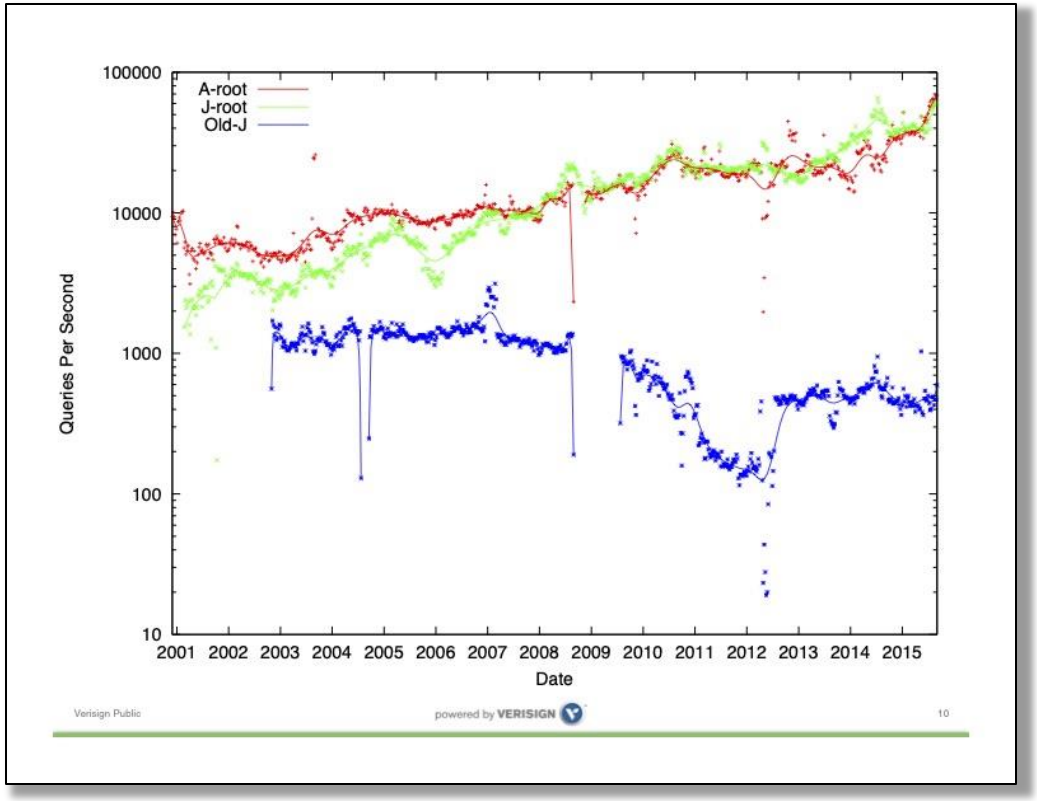
“Life and Times of Old J Root” (NANOG, Oct 2004)





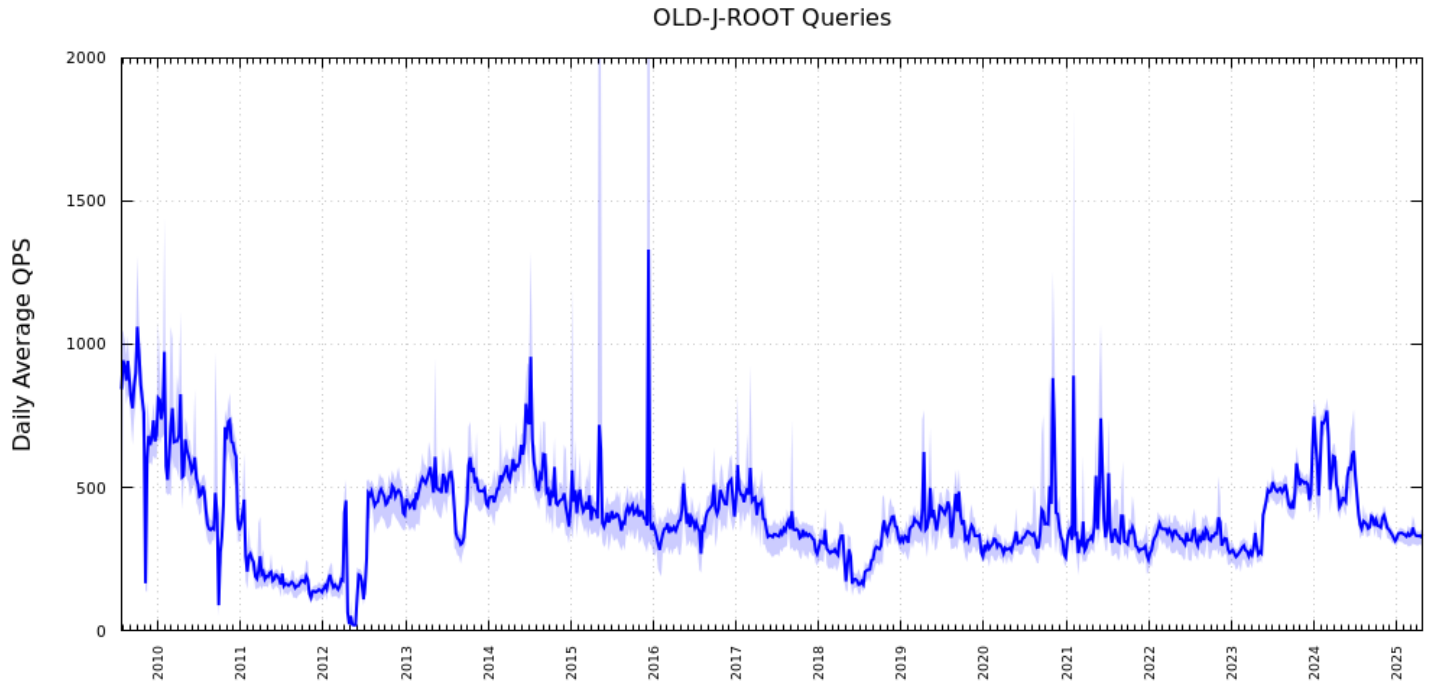
- In 2002, the IP address for J-Root was changed in preparation for anycast.
- Two years after the change, the old address continues to receive 1500 queries/second.

“Thirteen Years of Old J-Root” (OARC, Oct 2015)



- By late 2015 there were about 500 queries per second on old J-Root IP address.

Even More Years of Old-J-Root



- As of April 2025, seeing 350 queries per second on old J-Root IP.

Verisign data source: dag_hydra_listener_one_min_table

Sidebar: What Is Priming?

- DNS resolvers need to know the IP addresses of root name servers.
- When a resolver starts up, it might have stale root server data.
- The resolver sends a “priming” query to a root server.
- The priming response contains the list of current root name servers and their addresses.
- Further described in RFC 9609 “Initializing a DNS Resolver with Priming Queries.”

RSSAC028

- The Root Server System Advisory Committee (RSSAC) wrote about alternative root server naming schemes and called for additional study.
- The RSSAC028 Implementation study report (p. 49) contains this nugget:

  “BIND 9.9.1 and PowerDNS Recursor version 4.1.15 and 4.2.1 fail to learn new (alternative) IP addresses for root servers in the additional section of priming responses, when the root NS RRset matches that of the built-in or loaded hints file (see Failed priming).”

Could this be a long-term issue?

- For which versions of BIND was this the case?
- It could certainly explain what we see for old J root.

Testing BIND

Testing BIND Resolver Priming Behavior

- Configure named with “wrong” root.hints.
- Start background packet capture.
- Query for domain names ending with edu, com, net, nl, org, uk.
- Count queries sent to old vs current root IPs.
- Repeat for all versions of BIND that can be compiled.

- Note: DNSSEC disabled to simplify comparison with pre-DNSSEC BIND versions.

```
a.root-servers.net.   IN   A   198.41.0.10
b.root-servers.net.   IN   A   198.41.0.10
c.root-servers.net.   IN   A   198.41.0.10
d.root-servers.net.   IN   A   198.41.0.10
e.root-servers.net.   IN   A   198.41.0.10
f.root-servers.net.   IN   A   198.41.0.10
g.root-servers.net.   IN   A   198.41.0.10
h.root-servers.net.   IN   A   198.41.0.10
i.root-servers.net.   IN   A   198.41.0.10
j.root-servers.net.   IN   A   198.41.0.10
k.root-servers.net.   IN   A   198.41.0.10
l.root-servers.net.   IN   A   198.41.0.10
m.root-servers.net.   IN   A   198.41.0.10
```

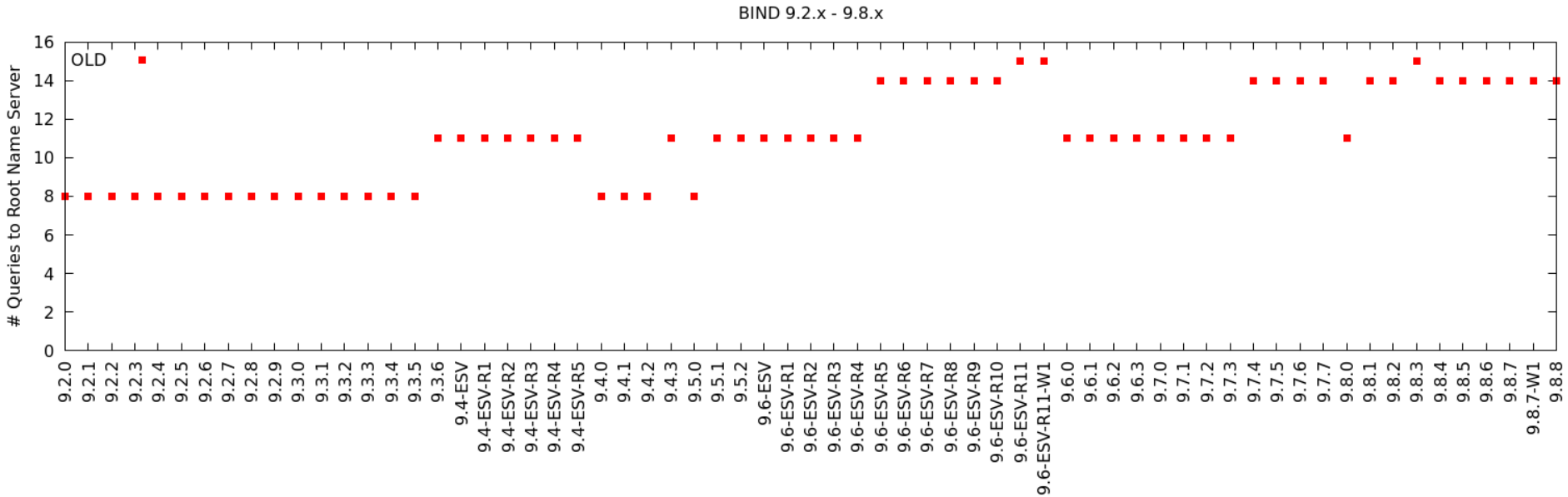
Sample Packet Capture (BIND 9.2.0)

```
$ tshark -r ...
    1   0.000000 209.131.180.145 → 198.41.0.10   DNS 82 Standard query 0xd99f A example.com OPT
    2   0.000043 209.131.180.145 → 198.41.0.10   DNS 70 Standard query 0x8ee7 NS <Root> OPT
    3   0.002053  198.41.0.10 → 209.131.180.145 DNS 1213 Standard query response 0xd99f A example.com NS l.gtld-servers.
    4   0.002098  198.41.0.10 → 209.131.180.145 DNS 1139 Standard query response 0x8ee7 NS <Root> NS l.root-servers.net
    5   0.019749 209.131.180.145 → 198.41.0.10   DNS 89 Standard query 0xc7e1 A a.iana-servers.net OPT
    6   0.019770 209.131.180.145 → 198.41.0.10   DNS 89 Standard query 0xb60e A b.iana-servers.net OPT
    7   0.021115  198.41.0.10 → 209.131.180.145 DNS 1217 Standard query response 0xc7e1 A a.iana-servers.net NS m.gtld-s
    8   0.021137  198.41.0.10 → 209.131.180.145 DNS 1217 Standard query response 0xb60e A b.iana-servers.net NS m.gtld-s
    9   0.046547 209.131.180.145 → 198.41.0.10   DNS 83 Standard query 0x26a5 A ns.icann.org OPT
   10   0.047847  198.41.0.10 → 209.131.180.145 DNS 820 Standard query response 0x26a5 A ns.icann.org NS a2.org.afilias-
   11   3.199985 209.131.180.145 → 198.41.0.10   DNS 83 Standard query 0x54bd A google.co.uk OPT
   12   3.201371  198.41.0.10 → 209.131.180.145 DNS 922 Standard query response 0x54bd A google.co.uk NS dns1.nic.uk NS
   13   4.382683 209.131.180.145 → 198.41.0.10   DNS 78 Standard query 0x44c1 A sidn.nl OPT
   14   4.383978  198.41.0.10 → 209.131.180.145 DNS 603 Standard query response 0x44c1 A sidn.nl NS ns3.dns.nl NS ns1.dn
   15   5.478356 209.131.180.145 → 198.41.0.10   DNS 78 Standard query 0x48a3 A wsu.edu OPT
   16   5.479761  198.41.0.10 → 209.131.180.145 DNS 1208 Standard query response 0x48a3 A wsu.edu NS d.edu-servers.net N
```

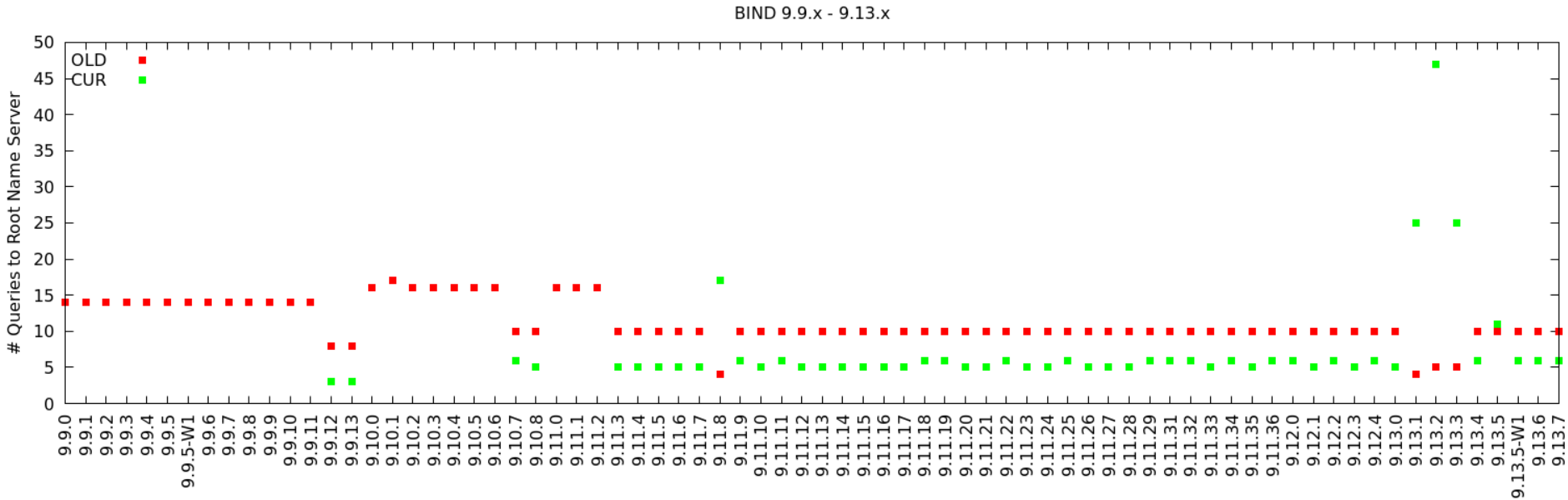
Sample Packet Capture (BIND 9.14.0)

```
 1   0.000000 209.131.180.145 → 198.41.0.10   DNS 86 Standard query 0x0078 NS com OPT
 2   0.000122 209.131.180.145 → 198.41.0.10   DNS 82 Standard query 0x2dde NS <Root> OPT
 3   0.001273  198.41.0.10 → 209.131.180.145 DNS 362 Standard query response 0x0078 NS com NS l.gtld-servers.net NS j
 5   0.001489  198.41.0.10 → 209.131.180.145 DNS 545 Standard query response 0x2dde NS <Root> NS l.root-servers.net N
 9   0.026216 209.131.180.145 → 198.41.0.10   DNS 108 Standard query 0xacb9 NS <Root> OPT
12   0.026397 209.131.180.145 → 198.41.0.10   DNS 112 Standard query 0x333e NS com OPT
13   0.050774  198.41.0.10 → 209.131.180.145 DNS 1165 Standard query response 0xacb9 NS <Root> NS l.root-servers.net
15   0.051316  198.41.0.10 → 209.131.180.145 DNS 1231 Standard query response 0x333e NS com NS l.gtld-servers.net NS
19   0.062832 209.131.180.145 → 198.41.0.10   DNS 101 Standard query 0x2822 A a.iana-servers.net OPT
20   0.062901 209.131.180.145 → 198.41.0.10   DNS 101 Standard query 0x7c2e AAAA a.iana-servers.net OPT
21   0.062976 209.131.180.145 → 198.41.0.10   DNS 101 Standard query 0x088b A b.iana-servers.net OPT
22   0.063053 209.131.180.145 → 198.41.0.10   DNS 101 Standard query 0xd989 AAAA b.iana-servers.net OPT
23   0.063860  198.41.0.10 → 209.131.180.145 DNS 1217 Standard query response 0x2822 A a.iana-servers.net NS m.gtld-s
24   0.063873  198.41.0.10 → 209.131.180.145 DNS 1217 Standard query response 0x7c2e AAAA a.iana-servers.net NS m.gtl
25   0.064184  198.41.0.10 → 209.131.180.145 DNS 1217 Standard query response 0x088b A b.iana-servers.net NS m.gtld-s
26   0.064319  198.41.0.10 → 209.131.180.145 DNS 1217 Standard query response 0xd989 AAAA b.iana-servers.net NS m.gtl
27   0.065468 209.131.180.145 → 198.41.0.10   DNS 95 Standard query 0xf842 A ns.icann.org OPT
28   0.065556 209.131.180.145 → 198.41.0.10   DNS 95 Standard query 0xeb34 AAAA ns.icann.org OPT
29   0.066212  198.41.0.10 → 209.131.180.145 DNS 820 Standard query response 0xeb34 AAAA ns.icann.org NS a2.org.afili
30   0.067435  198.41.0.10 → 209.131.180.145 DNS 820 Standard query response 0xf842 A ns.icann.org NS a2.org.afilias-
37   3.238777 209.131.180.145 → 199.7.91.13   DNS 85 Standard query 0x5034 NS uk OPT
38   3.239388  199.7.91.13 → 209.131.180.145 DNS 225 Standard query response 0x5034 NS uk NS nsa.nic.uk NS nsb.nic.uk
42   3.240065 209.131.180.145 → 199.7.91.13   DNS 111 Standard query 0xdb13 NS uk OPT
44   3.240656  199.7.91.13 → 209.131.180.145 DNS 938 Standard query response 0xdb13 NS uk NS nsa.nic.uk NS nsb.nic.uk
49   4.583877 209.131.180.145 → 192.112.36.4 DNS 85 Standard query 0x72cb NS nl OPT
50   4.620877 192.112.36.4 → 209.131.180.145 DNS 544 Standard query response 0x72cb NS nl NS ns1.dns.nl NS ns4.dns.nl
51   4.622302 209.131.180.145 → 198.97.190.53 DNS 93 Standard query 0xac15 AAAA ns3.dns.nl OPT
52   4.622440 209.131.180.145 → 198.97.190.53 DNS 93 Standard query 0x8f69 AAAA ns1.dns.nl OPT
53   4.622563 209.131.180.145 → 198.97.190.53 DNS 93 Standard query 0x7a0e AAAA ns4.dns.nl OPT
```

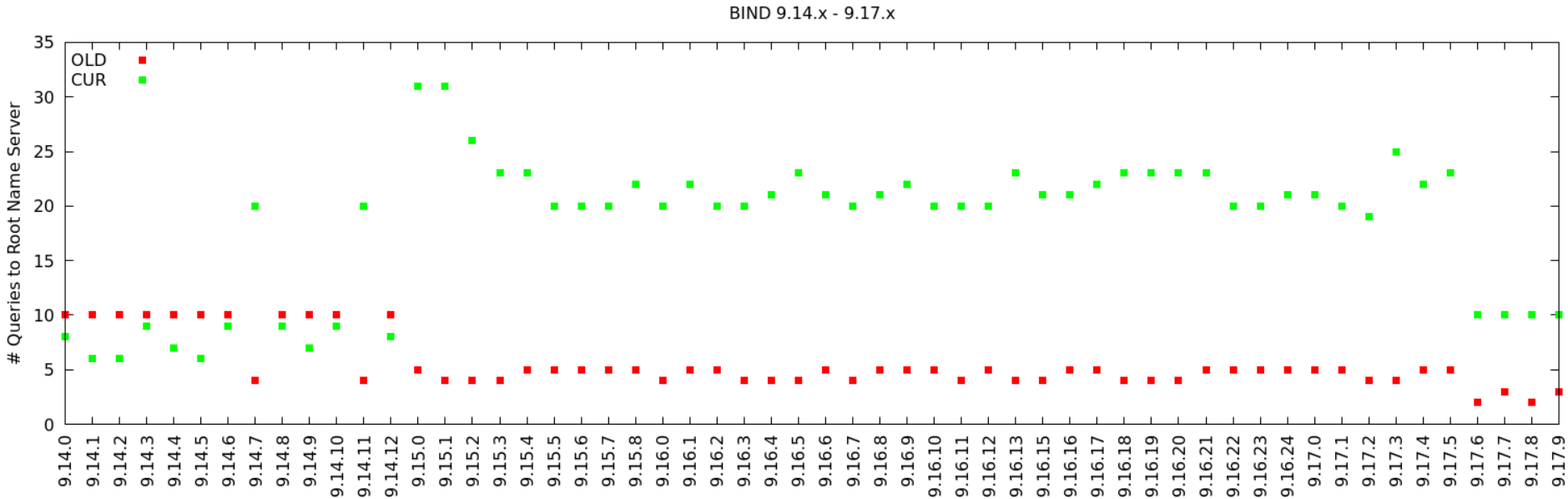
BIND 9.2.x – 9.8.x


BIND 9.2.x - 9.8.x
OLD
Queries to Root Name Server
0
2
4
6
8
10
12
14
16
9.2.0
9.2.1
9.2.2
9.2.3
9.2.4
9.2.5
9.2.6
9.2.7
9.2.8
9.2.9
9.3.0
9.3.1
9.3.2
9.3.3
9.3.4
9.3.5
9.3.6
9.4-ESV
9.4-ESV-R1
9.4-ESV-R2
9.4-ESV-R3
9.4-ESV-R4
9.4-ESV-R5
9.4.0
9.4.1
9.4.2
9.4.3
9.5.0
9.5.1
9.5.2
9.6-ESV
9.6-ESV-R1
9.6-ESV-R2
9.6-ESV-R3
9.6-ESV-R4
9.6-ESV-R5
9.6-ESV-R6
9.6-ESV-R7
9.6-ESV-R8
9.6-ESV-R9
9.6-ESV-R10
9.6-ESV-R11
9.6-ESV-R11-W1
9.6.0
9.6.1
9.6.2
9.6.3
9.7.0
9.7.1
9.7.2
9.7.3
9.7.4
9.7.5
9.7.6
9.7.7
9.8.0
9.8.1
9.8.2
9.8.3
9.8.4
9.8.5
9.8.6
9.8.7
9.8.7-W1
9.8.8

BIND 9.9.x – 9.13.x

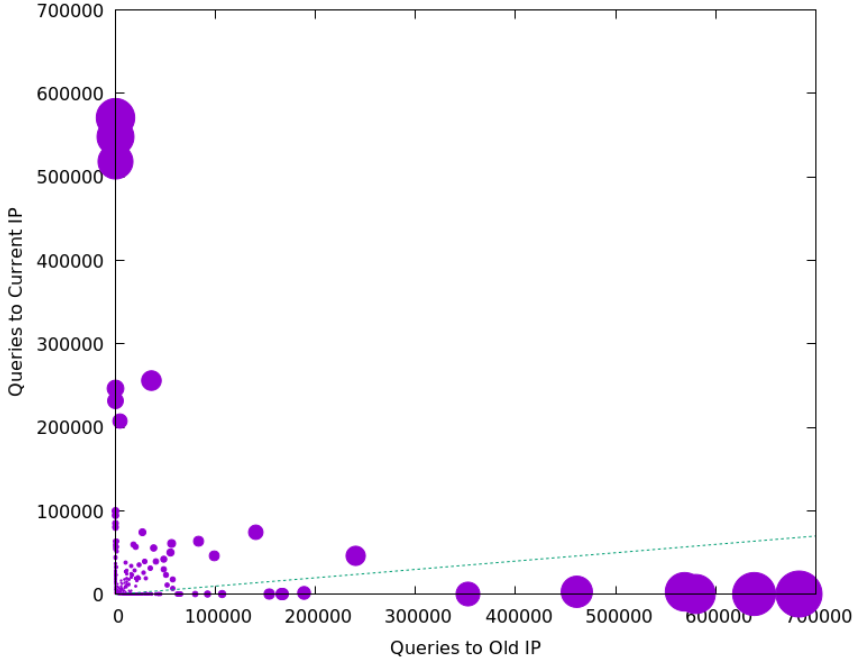


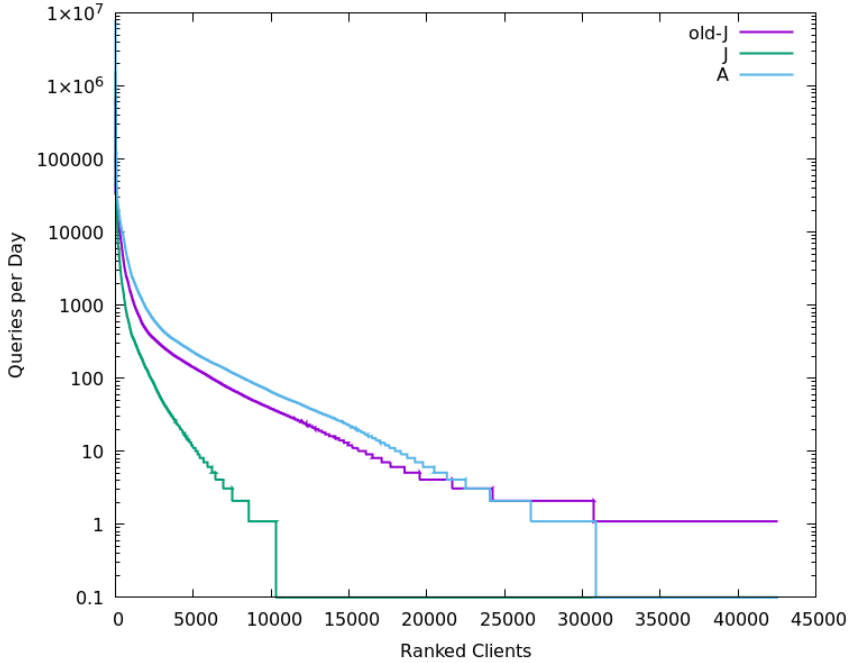
BIND 9.14.x – 9.17.x



Analysis of Current Old-J-Root Clients

Old-J-Root Client Addresses





- On April 28, 2025 there were 42,560 client IP addresses that sent queries to old-J-Root.
- 75% of these sent ZERO queries to current-J-Root, and are responsible for 62% of query traffic to old-J-Root.
- 79% of these clients sent 10x more to old-J than current-J and are responsible for 80% of old-J traffic.

Verisign data source: ea_orc_dns_responses_hourly April 28, 2025

version.bind analysis

- Sent version.bind/CH/TXT queries to Old-J-Root client IP addresses sending more than 10 queries per day.

Category	Count	%
Clients sending >10 queries to Old J-Root	14,051	100
Timeout	11,554	82.2
FORMERR, REFUSED, NOTIMP, SERVFAIL, NXDOMAIN	269	1.9
Obfuscated version	1,991	14.2
Unobfuscated version	237	1.7

Subcategory	Count	%
BIND 9 unpatched	193	81.4
BIND 9 patched	27	11.4
nsd, powerdns, dnsmasq, Microsoft	17	7.2

fpdns analysis

- Fingerprinted Old-J-Root client IP addresses sending more than 10 queries per day.
- fpdns is an old, unmaintained tool and you should probably never use it.

Fingerprint	Count	%
Clients sending >10 queries to Old J-Root	14,051	
Timeout	11,438	
Non-Timeout	2,613	100
ISC BIND 9.1.x - 9.7.x	1,847	70.1
Meilof Veeningen Posadis[1]	461	17.6
DJ Bernstein TinyDNS 1.05	111	4.3
Microsoft Windows DNS 2000 / 2003	50	1.9
Others	144	5.5

[1] https://github.com/kirei/fpdns/issues/13: fpdns mis-identifies newish BIND as "Mailof Veenignen Posadis"

Summary of Findings

- All versions of BIND released from 2001-2017 appear to “fail” priming as described in RSSAC028 implementation study report.
- Starting with BIND 9.9.12 (released March 2018) we start seeing queries to root IP addresses returned in the priming response.
- Verisign’s query data supports the theory that sources querying old-J “fail” at priming.
- Any 2001-2017 era BIND installation will keep querying old J-Root and probably never query the new IP address.

```
commit 5de02a075b19f6781a168da7b81fc78313546c90
Date:   Wed Oct 11 09:10:13 2017 +0200

[master] reduce unnecessary priming queries

4770. [bug] Cache additional data from priming queries
as glue.
Previously they were ignored as unsigned
non-answer data from a secure zone, and never
actually got added to the cache, causing hints
to be used frequently for root-server
addresses, which triggered re-priming. [RT #45241]
```

References

[1] “Life and Times of J-Root”, NANOG 32, Oct 2004; P. Barber, M. Larson, M. Kosters, P. Toscano; https://archive.nanog.org/meetings/nanog32/presentations/kosters.pdf

[2] “Thirteen Years of Old J-Root”, DNS-OARC 23, Oct 2015; D. Wessels, J. Casonguay, P. Barber; https://indico.dns-oarc.net/event/24/contributions/378/attachments/353/613/2015-old-j-root.pdf

[3] “RSSAC028 Implementation study report”, Sep 2023; W. Toorop, Y. Thessalonikefs, B. Overeinder, M. Müller, M. Davids; https://www.icann.org/en/system/files/files/rssac028-implementation-study-report-27sep23-en.pdf

[4] BIND Software; ftp://ftp.isc.org/bind9/

[5] “reduce unnecessary priming queries”, Oct 2017; https://gitlab.isc.org/isc-projects/bind9/-/commit/5de02a075b19f6781a168da7b81fc78313546c90

[6] fpdns (DNS server fiingerprinter); https://github.com/kirei/fpdns

Questions?

VERISIGN®

© 2025 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.