RFC8806 – is it enough?

Wes Hardaker

November 15, 2021

Background

RFC8806

- Creates a local copy of the root zone
- Protects against root outages
- Helps in low-latency situations
  - especially with negative answers
- Works because of DNSSEC data signing

LocalRoot

- Disclaimer: My pet project
- Caches more than just the root
    - including *.arpa*

- My questions today:
    - Is the root (RFC8806) enough?
    - What other zones are worth caching?

Testing root outages

Conducting an experiment: no root

Testing 8806

1. start a local resolver with RFC8806
2. remove access to the root
3. perform network tests

Testing LocalRoot

1. start a local resolver with LocalRoot
2. remove access to the root
3. perform network tests

First, we remove access to the roots

```
DROP       all  --  0.0.0.0/0              198.41.0.4
DROP       all  --  0.0.0.0/0              199.9.14.201
DROP       all  --  0.0.0.0/0              192.33.4.12
DROP       all  --  0.0.0.0/0              199.7.91.13
DROP       all  --  0.0.0.0/0              192.203.230.10
DROP       all  --  0.0.0.0/0              192.5.5.241
DROP       all  --  0.0.0.0/0              192.112.36.4
DROP       all  --  0.0.0.0/0              198.97.190.53
DROP       all  --  0.0.0.0/0              192.36.148.17
DROP       all  --  0.0.0.0/0              192.58.128.30
DROP       all  --  0.0.0.0/0              193.0.14.129
DROP       all  --  0.0.0.0/0              199.7.83.42
DROP       all  --  0.0.0.0/0              202.12.27.33
```

Testing traceroutes:

We perform a simple test with traceroute:

```
traceroute www.nlnetlabs.nl
```

Traceroute with RFC8806

```
traceroute to www.nlnetlabs.nl (185.49.140.10), 30 hops max, 60 byte packets
 1  router (10.0.0.1)  0.234 ms  0.137 ms  0.122 ms
 2  68.78.72.22 (68.78.72.22)  1.221 ms  1.622 ms  1.982 ms
 3  * * *
 4  71.147.199.98 (71.147.199.98)  24.887 ms  25.339 ms  25.970 ms
 5  12.122.160.166 (12.122.160.166)  29.491 ms  31.944 ms  37.875 ms
 6  12.122.2.78 (12.122.2.78)  32.974 ms  33.828 ms  34.275 ms
 7  12.122.114.29 (12.122.114.29)  37.531 ms  22.482 ms  24.600 ms
 8  192.205.32.98 (192.205.32.98)  25.185 ms  40.611 ms  41.062 ms
 9  89.149.141.206 (89.149.141.206)  170.043 ms  171.549 ms  171.975 ms
10  134.222.152.117 (134.222.152.117)  174.312 ms  174.725 ms  176.587 ms
11  94.247.72.20 (94.247.72.20)  177.019 ms  177.449 ms  177.914 ms
12  94.247.72.38 (94.247.72.38)  178.330 ms  183.420 ms  184.446 ms
13  185.49.141.2 (185.49.141.2)  183.931 ms  183.343 ms  170.473 ms
```

Traceroute with LocalRoot

```
traceroute to www.nlnetlabs.nl (185.49.140.10), 30 hops max, 60 byte packets
 1  router (10.0.0.1)  0.231 ms  0.149 ms  0.204 ms
 2  68.78.72.22 (68.78.72.22)  0.939 ms  1.410 ms  2.003 ms
 3  * * *
 4  71.147.199.98 (71.147.199.98)  25.840 ms  26.260 ms  27.169 ms
 5  12.122.160.166 (12.122.160.166)  49.940 ms  52.329 ms  50.310 ms
 6  12.122.2.78 (12.122.2.78)  52.605 ms  55.830 ms  55.256 ms
 7  sffca402igs.ip.att.net (12.122.114.29)  57.976 ms  29.267 ms  26.576 ms
 8  192.205.32.98 (192.205.32.98)  28.053 ms  28.856 ms  28.348 ms
 9  ae3.cr2-ams3.ip4.gtt.net (89.149.141.206)  163.865 ms  163.170 ms  164.986 ms
10  134.222.152.117 (134.222.152.117)  165.646 ms  166.887 ms  168.106 ms
11  94.247.72.20 (94.247.72.20)  169.277 ms  170.614 ms  172.276 ms
12  cs01.vlan202.mx3.infracom.nl (94.247.72.38)  174.968 ms  177.042 ms  175.867 
13  usg.nlnetlabs.nl (185.49.141.2)  176.210 ms  159.966 ms  184.618 ms
```

Questions

Conclusions lead to Questions

- When network troubles arise:
  - What services do we need?
  - e.g. debugging network issues without reverse DNS may be trickier
- What other services may get impacted?
  - Anti-spam techniques do reverse lookups
  - When names don't match, your SPAM score goes up
  - Are you more likely to have E-Mail regarded as spam?

Question: What else can go wrong?

- Are there other globally critical zones?
    - EG: *.com*
        - (unlikely to ever be cachable)
        - using NSEC aggressive is the best we can do
    - Any SLD or other "critical" domains?
- Are there regional concerns?
    - CCTLDs are the obvious one