PROBE.RESOLVER.ARPA.

Standardized Query Name for DNS Resolver Reachability Probes

Ben Schwartz (Meta), Puneet Sood (Google), John Todd (Quad9)

DNSOP @ IETF 123

Questions

Debugging

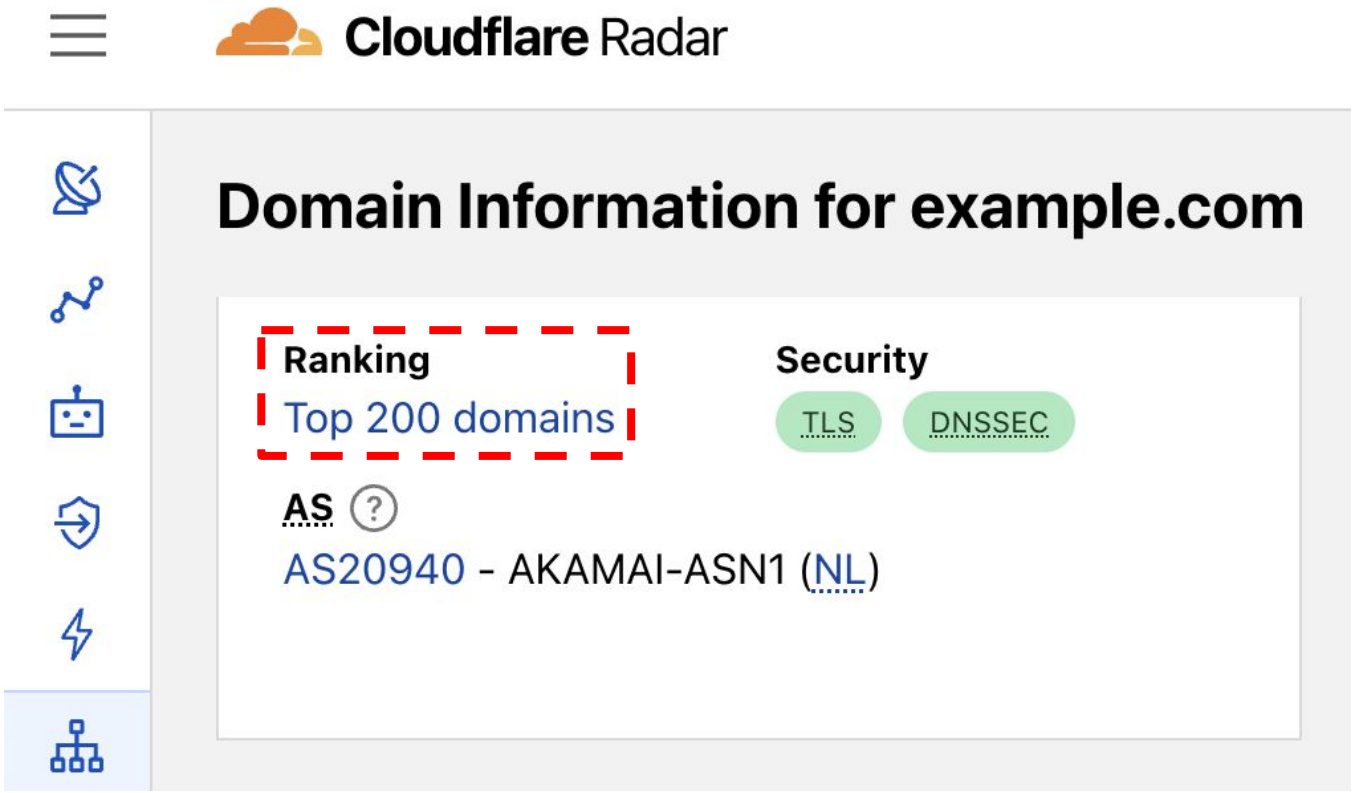
- Is the network working at all?
- I’m not getting ping replies — is ICMP blackholed?
- Is my DNS server broken?
- Is my IPv6 routing broken?
- Does this DNS resolver have basic TCP support?

Profiling

- Does this DNS resolver do DoT?
- Which of these resolver IPs is closest to me?
- What’s the availability of resolver fleet X from vantage point Y?

Raise your hand if

```
$ ping 8.8.8.8

$ dig example.com

$ dig @2620:fe::9 example.com

$ dig +tcp example.com

$ dig @resolver.example +tls example.com

$ curl https://example.com/
```



HTTPS://RADAR.CLOUDFLARE.COM/DOMAINS/DOMAIN/EXAMPLE.COM

Goal: Do better than "example.com"

- Make it clear what is going on.
  - Server logs clearly indicate "someone is doing a reachability probe"
- Skip iterative resolution.
  - Doesn't help
  - Wastes resources
  - Makes response latency inconsistent
- Don't waste bytes on RRSETs.
- Avoid reliability issues due to any upstream outage.
- Avoid fingerprinting the client with a distinctive QNAME.

Proposal: probe.resolver.arpa

- resolver.arpa is a Locally Served Zone
  - Defined: RFC 6303
  - Assigned: RFC 9462, Section 6.4
- “probe.resolver.arpa” is NXDOMAIN
  - NXDOMAIN is fine for our purposes.
- Naive resolvers will forward to the .arpa nameservers
  - Still NXDOMAIN either way.
  - Should be very reliable.
  - Minimizes leakage to external/commercial infrastructure.

Does it work?

- Tested by querying 8.8.8.8 for “www.google.com” and “probe.resolver.arpa”
  - From several thousand nodes in racks around the world.
  - Using UDP, TCP, and TLS
- Results:
  - Error distributions are a perfect match
  - Latencies are closely correlated but responses for “probe.resolver.arpa” are 5-8 ms faster on average.
    - 8.8.8.8 implements the Locally Served Zone!

The Details

NXDOMAIN = **It's working.** Anything else = **Broken.**

QTYPE doesn't matter -> **Use A or AAAA.**

getaddrinfo is bad but you **MAY.** DNSSEC-OK is **SHOULD NOT.**

Questions: **Is this a SUDN?**

What about authoritative servers?

Seeking adoption