DNS Resolver Recommendations in Practice

Shane Kerr | RIPE 89 | 2024-10-31 🎃

Why Are We Here?

- The RIPE community published the *RIPE DNS Resolver Recommendations* (RIPE-823) on 2024-05-01.

- Was a response to the increasing importance of DNS Public Resolvers.

- At RIPE 88 we had a short panel discussion in the RIPE DNS working group, covering a few topics.

- The BoF today adds more panelists, gives us more time to dig into topics, and acts as a sort of "sanity check" of the document.

What's Going On with DNS Resolution?

- Traffic going to public resolvers is going down!

- Traffic going to public resolvers is going up!

- Our goal is to improve DNS resolution by providing more high-quality DNS resolvers.

Our Panel of Experts

Andronikos Kyriakou	DNS4EU
Babak Farrokhi	Quad9
Dave Knight	UltraDNS
Farzaneh Badiei	Digital Medusa
Joeri de Ruiter	SURF

Topics Covered in Previous Session

- Multiple implementations

- Infrastructure: cloud vs. metal

- High availability

- ECS

- RPKI

- NTA

- DoT/DoH/DoQ

- NSID

- Cookies

Audience Input

- Questions & Comments are highly encouraged!

- Any initial discussion ideas before we start digging in?
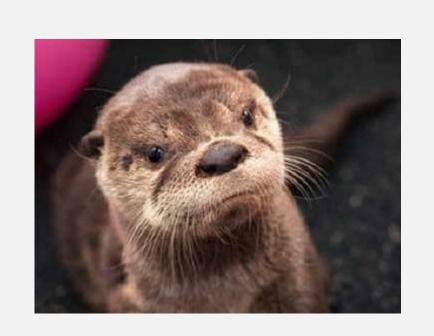
DNS Extended Errors

- Fun presentation at RIPE DNS Working Group about extended DNS errors.

- Do you provide them? Are they customized or enhanced?

- What about reporting blocking/filtering?
  - 4.16. Extended DNS Error Code 15 – Blocked
  - 4.17. Extended DNS Error Code 16 – Censored
  - 4.18. Extended DNS Error Code 17 – Filtered
  - 4.19. Extended DNS Error Code 18 – Prohibited

Block Lists, Filtering

- Brief mention of RPZ as a possible distribution mechanism

- Legal blocking

  – Recommend maximal transparency, but not always possible.

  – Provide Extended DNS Errors when blocking?

  – Community governance of blocking

DNS Error Reporting

- Sends resolution and other failures from resolver to authoritative.

- Was a draft when RIPE-823 published, now RFC 9567.

- Any plans to implement this? Rate limited? Other operational concerns?

Privacy & Anonymity

- Apply RFC 8932

  – Which means addressing RFC ~~7626~~ 9076, and of course RFC 6973...

  – Use DoT/DoH, QNAME minimization, non-ECS service, ...

  – Have a Recursive Operator Privacy Statement (RPS)

- Avoid giving out personal data

- Publish advertising policy (if any advertising exists)

Logging

- "Protect the Logs"

- Good presentation about pseudo-anonymizing logs at DNS OARC

- Should also be covered in the RPS

- RIPE-823 does *not* say "log minimally" (maybe it should have)

Alternate Provisioning (Opt-In/Opt-Out)

- Is there a way to get different service? How?
  - Different IP addresses?
  - Client authentication (source IP, certificates)?

- What types of service are available?
  - "raw"?
  - "family friendly"?
  - ?

Plans for the Future: Panelists

- Can you share any plans?

- Are there any "hot topics" you want to bring up?

Plans for the Future: RIPE

- What is next for RIPE regarding DNS Resolvers?

- More guidance?
  - RIPE-823 is not normative, no checklists, "think about" style text
  - Checklist or other compliance helpers?

- Update document periodically? When?

- More research?

- Nothing?

- Let Adam Smith's Invisible Hand care for the public interest?