Structured Data for Filtered DNS

draft-ietf-dnsop-structured-dns-error

IETF123, July 2025

D. Wing (Citrix)

T. Reddy (Nokia)

N. Cook (Open-Xchange)

M. Boucadair (Orange)

Last Call Feedback

- Background of RFC8914's EXTRA-TEXT
- Signalling Intent with EDE
- ENUM all of the categories for filtering
- Discovered and Trusted Resolvers
- DNS Filtering Details for Applications (draft-nottingham-public-resolver-errors)

Background of EXTRA-TEXT

- Free-form text, introduced in RFC8914
- RFC8914 allows server to send Extra-Text
  - Without client requesting Extra-Text in DNS query
- RFC8914 does not attempt to localize response
  - Which is fine: intended as troubleshooting tool

Signalling Intent with EDE

- Client requests structured-dns-error in query by sending EDE
  - allows server to send RFC8914 or structured-dns-error's JSON, based on client support

Signalling Intent with EDE

Last Call Feedback:

- using the well-known EDE option in a way that is **not defined** by RFC8914 (i.e., in a query instead of a response).
  - Introduce new OPTION-CODE specifically for use in DNS queries.
  - RFC 6891 Section 6.1.2 ensures that unknown OPTION-CODE values are safely ignored by responders

Authors Proposal

- Option A> Signal client support in query: Introduce new OPTION-CODE specifically for use in DNS queries.
- Option B> Do not signal client support in query: client cannot influence EXTRA-TEXT to be JSON or plaintext

ENUM or text

- Suggestion to enumerate all possible sub-errors
  - Solves free-form text and localization
- **Impossible** to reach consensus on enumeration
  - E.g., one service has *NNN* categories, another has *N* categories, and they overlap

- How does the WG want to proceed ?

Trusted and Discovered resolvers

Contact

Justification

Language

Sub-error code

```
{ "c": [
        "tel:+358-555-1234567",
"sips:bob@bobphone.example.com"
        ],
  "j": "malware present for 23 days",
  "l": "en",
  "s": 1   }
```

displayed only when received from trusted resolvers

draft-nottingham-public-resolver-errors (1/2)

- draft-nottingham: compiled list of trusted public resolvers (§ 5)
- ietf-dnsop: configured list of trusted resolvers and discovered resolvers (§ 10.2)

draft-nottingham-public-resolver-errors (2/2)

- Adds Resolver Operator Identity, Filtering Incident Identifier, and URL Template
- ietf-dnsop avoided URL (already discussed and rejected)
  - Display advertising, domain spoofing, and other abuse (web fingerprinting, reveals client IP address)
- Unique response value
  - Tracking raises privacy concerns

Discussion on next steps

- ietf-dnsop allows extensibility.
- Can we progress ieft-dnsop draft after addressing these issues ?