DNS Resolver Information

draft-reddy-add-resolver-info-06

IETF#115, London

November 2022

T. Reddy (Nokia) & M. Boucadair (Orange)

Changes Since IETF#114

- Mainly to address the comments raised by the WG participants in IETF#114:
  - ***Abandon*** the JSON encoding
  - ***Use*** “key=value” syntax
  - ***Leverage*** DNS-SD (RFC6763) for encoding rules and verifications

What's Next?

- The draft provides a straightforward solution to address the following WG item:

> "The Adaptive DNS Discovery (ADD) working group will work on the following deliverables:
>
> …
>
> - Define a mechanism that allows communication of **DNS resolver information to clients for use in selection decisions.** This could be part of the mechanism used for discovery, above."

- All received comments are addressed
- Consider WG adoption

Appendix

ADD Discovery Mechanisms

- Stub resolvers can discover and authenticate encrypted DNS servers provided by a network using the techniques specified in
  - DNR
  - DDR

- However, ***these mechanism does not provide means to retrieve DNS resolver information***
  - A solution to address this functionality is still missing

Filling the Void

- Define a new RRtype: RESINFO
  - Clients use this new type to retrieve the resolver information with a QNAME set to:
    - ADN, when DNR
    - "resolver.arpa", when DDR
  - The server returns the resolver information that is structured as "key/value" pair
  - Retrieved information feeds the server selection procedure, typically
    - The exact details of the procedures are *implementation-specific and, thus, out of scope*

When to Retrieve the Information?

- The DNS resolver information can be retrieved
  - after the encrypted connection is established to the DNS server
  - before the encrypted connection is established to the DNS server by using local DNSSEC validation

Sample Discovered Information

- QNAME minimization support
- Support of extended DNS error (EDE) (RFC8914)
- ~~Client authentication is required or not~~
- An URL that points to the generic unstructured resolver information for troubleshooting only, e.g.,
  - DoH APIs supported, possible HTTP status codes returned by the DoH server, how to report a problem, etc.
- ~~An URL that points to a human-friendly description of the resolver identity~~