DNS Resolver Information

draft-reddy-add-resolver-info-04
IETF#113
March 2022

T. Reddy (Akamai) & M. Boucadair (Orange)
ADD Charter (Excerpt)

“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.”
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 JSON
  ▪ 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, e.g.,
  - DoH APIs supported, possible HTTP status codes returned by the DoH server, how to report a problem, etc. for troubleshooting purposes
- An URL that points to a human-friendly description of the resolver identity

- More information can be added, if required
Next Steps

• The draft addresses a specific issue in the WG charter

• Consider adopting this document