DDR status

IETF 110

Tommy Pauly, Tommy Jensen

IP Address Hints

- Issue #2
  - What happens when neither ipv4hint nor ipv6hint are present?

- Issue #5
  - Compliant SVCB clients only use IP address hints until A/AAAA queries are completed (draft-ietf-dnsop-svcb-httpssvc-03 Section 6.4)

Revise

DDR resolvers should include the hints. DDR clients should use the IP hints until there are A/AAAA values for the DoH server template name (no need to wait or artificially reconnect). Connections using hints or A/AAAA must meet the same cert requirements (claiming referring IP address, etc.)

Security Considerations

- Issue #3
  - How are private IP addresses used as a security property?

- Issue #4
  - Can you clarify why we need both target name and referring IP address?

Clarify:

Private IP addresses are identified to enforce same-address use / no cert check

Target name for HTTPS, referring IP address for validating insecure bootstrap

SUDN and Forwarders

- Issue #6
  - We should not address forwarders caching records for SUDN
- Issue #7
  - SUDN queries should never be sent upstream
  - Should directly address .arpa's special nature

Revise:

Resolvers should not forward

Resolvers should always return NXDOMAIN for dns://resolver.arpa queries unless they are specifically configured with one or more SVCB records to designate resolvers

*verbiage for case of 100% blind forwarding, nuance around clients validating

Document Scope

- Issue #8
  - Should specify behavior when local forwarders represent upstream resolvers

- Issue #9
  - Why is dns://resolver.arpa necessary for opportunistic scenarios?

Clarify:

Local forwarders designating upstream resolvers is out of scope
Need for resolver metadata in opportunistic case (name for TLS confirmation to avoid encouraging client to ignore self-signed certs, port numbers, etc.)