DNS over QUIC

draft-huiitema-dprime-dnsoquic-00
Christian Huitema, Allison Mankin, Sara Dickinson
IETF-DPRIVE Virtual Meeting, 8 April 2020
What?

<table>
<thead>
<tr>
<th>DNS over QUIC (DoQ)</th>
<th>QUIC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>IP</td>
</tr>
</tbody>
</table>

- Simple mapping of DNS over dedicated QUIC connections
  - One QUIC Stream per DNS Query/Response
  - Query and Response size up to 64K (65536)
  - Parallel processing, no head of queue blocking
  - QUIC handles timers, retransmissions, connection management

- Draft-00 targets the stub-recursive scenario
  - Recursive-authoritative requires discovery

- Operates on dedicated port (TBD-IANA)
Example flow, First connection, 1-RTT

- QUIC handshake embeds TLS handshake
  - Size of server responses depends on size of server certificate, signature
- DNS Query can be sent as soon as server first flight is received
- Response arrives after 2-RTT plus service time.

Initial packet (Client Hello)

Initial (Server Hello) +
Handshake (extensions, certificate, server finished)

Handshake (ACK, Client finished)
+ 1-RTT (Stream 0: DNS query)

1-RTT (Handshake Done, Session Ticket, ACK, Stream 0: DNS Response)

1-RTT (ACK)
Example flow, Second connection, 0-RTT

- Session Ticket obtained during previous connection
- DNS Query sent immediately as 0-RTT data
- DNS Response sent with first server flight
- Response arrives after 1-RTT plus service time.

Initial packet (Client Hello + Ticket) + 0-RTT (Stream 0: DNS query)

Initial (Server Hello) + Handshake (extensions, server finished) + 1 RTT (ACK, Stream 0: DNS Response)

Handshake (ACK, Client finished)

1-RTT (Handshake Done, Session Ticket)

1-RTT (ACK)
Example flow, Additional Queries

- Each Query uses a new QUIC stream (Query-ID is always 0)
- Responses can arrive in any order
Why?

- Differences with DoT
  - QUIC instead of TLS + TCP
- Difference with DoH3
  - DoH3 has integration with the Web
  - DoQ does not need to use the HTTP-3 layer
  - DoQ has no dependency on HTTP platforms
- With ESNI/ECHO, all 3 solutions can cross firewalls
Why Now?

• QUIC Transport is (almost) ready
  • Spec is largely frozen, very high bar for changes
  • More than 16 interoperating implementations

• DNS over QUIC does not require changes in QUIC
  • DNS over QUIC use case taken into account during development

• Work to do in DPRIVE
  • Connection Management
  • Details of DNS mapping
  • Policy for using 0-RTT
ADOPT?