Linear DNS-Over-QUIC Servers

(as a project for *Course of Topics in Internet Security, SNU, 2023*)

Jihong Min & Jungyoon Kwon

Computer Systems and Platforms Lab

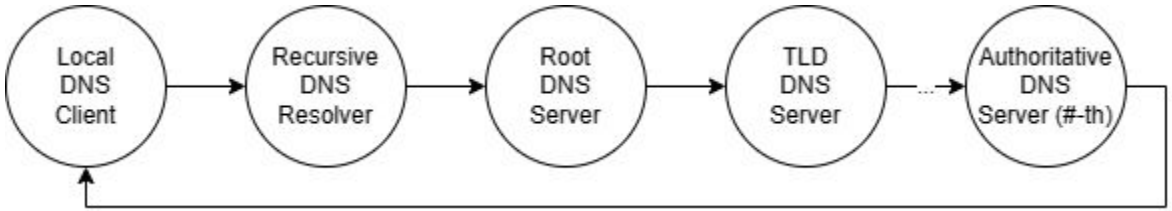
Department of Computer Science and Engineering

Seoul National University

Goal

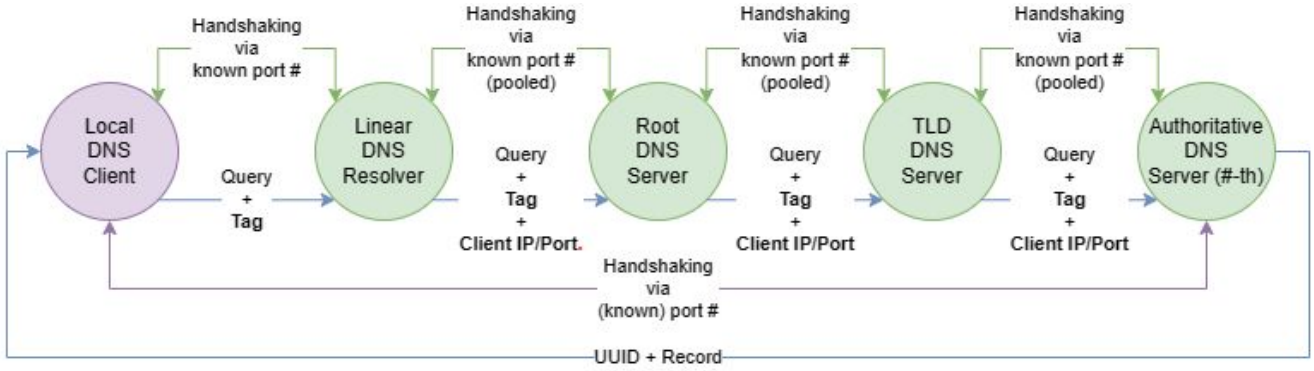
- **Reduce RTT** by linearizing the network route
  - + **Reduce total load in network**
  - + **Maintain security** (aspect of DNS encryption, not authentication)
    - The original DNSSEC will cover authentication part.

- The last DNS server resolving DNS query must know the followings (but not limited to):
  1) **The client's IP address** (+ QUIC (UDP) port # (optional))
  2) (optional) **Tag of DNS query**
  - **The above information must be encrypted (otherwise MITM attack is possible).**
    - QUIC is suitable for faster encryption establishment on each stage.
      - Reduced # of round trips for handshaking (with larger messages), connection resumption, etc.



Architecture

- Assumption: **All DNS servers are trusted and support our method**.
  - Also, they are presumably communicating with each other frequently so **pooling connections** are desirable.
- QUIC server-client model (***picoquic*/*picotls*** + ***quicdoq***)

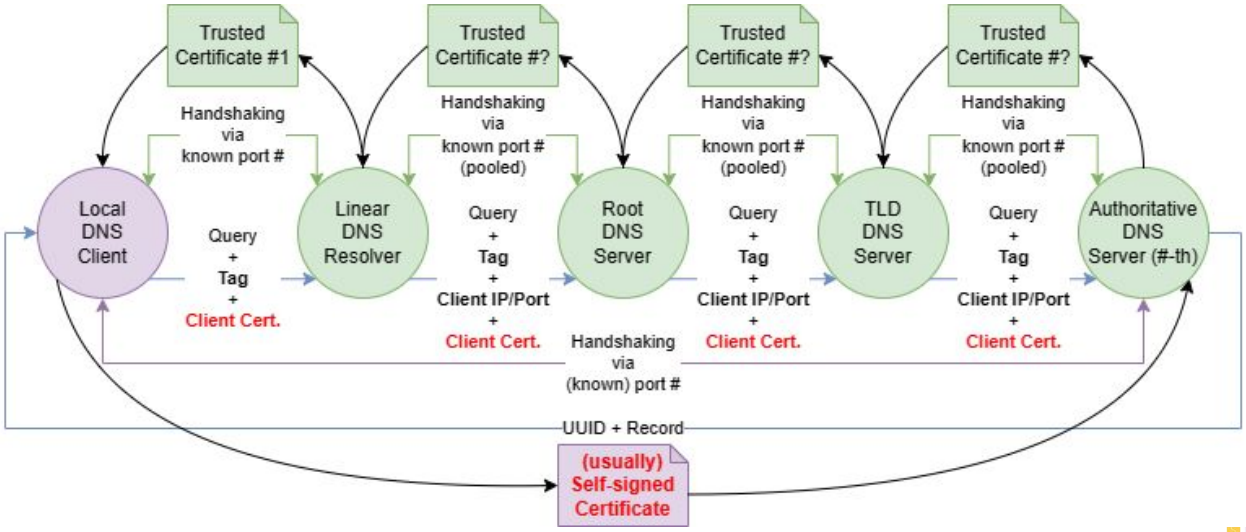


- ~~QUIC P2P~~ (TBD) (*qp2p* + (*picoquic*/*picotls* + *quicdoq*))
  - No server (+ no fixed port #) after the resolver
    - Data plane carries client port # as well.
  - Handshaking is still required for each stage (if not pooled).

Client Certificate (or symmetric key)

- While QUIC is implemented on UDP, it needs its handshaking process.
  - Setting up encryption, etc.

- **Thus, the client's 'server' port also requires certificate for establishing QUIC connection with the last server.**
  - The server's needs to **carry the client's (usually) 'untrusted' certificate** to validate at the last stage.
    - **Or, use raw UDP/TCP on the last step and carried symmetric key** instead of certificate.



Evaluation

(please refer the separate slide(s))

Future Improvement

- **Falling back** when the next endpoint does not support linear DOQ resolving
- **Caching** DNS entries in the linear resolver
  - Carry “request cache” bit or the linear resolver’s address to selectively cache.
- Supporting QUIC session ticket for **maintaining connection even when the client address shifts**