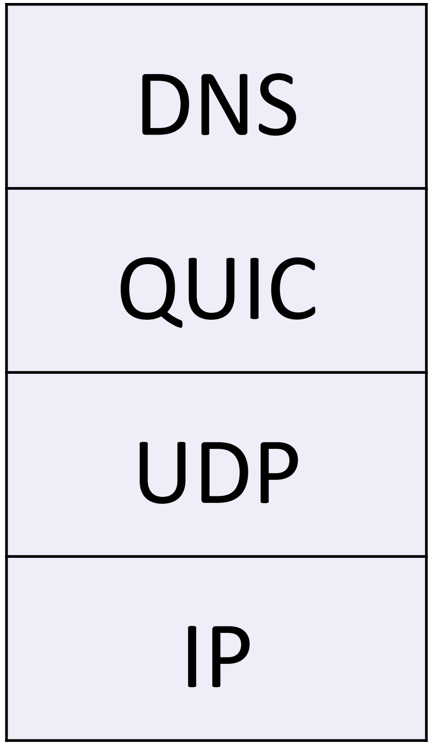
DNS over QUIC

Christian Huitema, Sara Dickinson

IETF 99, Prague, July 2017

draft-huitema-quic-dnsoquic-02

What is DNS over QUIC


DNS
QUIC
UDP
IP

- QUIC
  - Transport over UDP
  - Typically implemented in Application Process, not kernel
  - Functionally equivalent to TCP + TLS + streams
  - Incorporates TLS 1.3
  - Enables 0-RTT
- DNS over QUIC
  - High performance transport
  - Inform QUIC development, in parallel with HTTP/QUIC

DNS over QUIC: Features

	QUIC
Transport efficiency	
Connection set up time	0-RTT on Resumption
Head of queue blocking	Separate stream for each query
Retransmission efficiency	Similar to modern TCP (SACK, RACK)
Long messages (DNSSEC)	Arbitrary length (up to 2^64 bytes)
Security	
Three ways handshake	1-RTT for initial connection
Encryption & Authentication	TLS 1.3, AEAD

DNS over QUIC: Motivation

	UDP	TCP	TLS	DTLS	QUIC
Transport efficiency					
Connection set up time	✓	✖	✖	✖	**0-RTT**
Head of queue blocking	✓	✖	✖	✓	✓
Retransmission efficiency	✖	✓	✓	✖	✓
Long messages (DNSSEC)	✖	✓	✓	✖	✓
Security					
Three ways handshake	✖	✓	✓	✓	✓
Encryption & Authentication	✖	✖	✓	✓	✓

QUIC over DNS: Scenarios

- Initial Scenario: Stub to Recursive Resolver
  - Similar to RFC 7858
- Future Scenario: Recursive Resolver to Authoritative Server
  - Motivated by Security + Performance
  - User Space implementation may have lower overhead than DNS/TLS
- Feedback?