Thoughts on QUIC

Lars Eggert

DE@NetApp, Chair@IETF

Genesis

- QUIC, a fast, secure, evolvable transport for Internet workloads
  - Long talk at https://eggert.org/talks/2021-quic-isi.pdf

- Originated with Google
- Brought to IETF in 2016, somewhat controversial BOF
- WG formed with mnot and me as initial chairs
- Modern GitHub-centric workflow for standards development
- Extremely quick pace of development for ~3 years
- Core set of RFCs published in 2021 (RFCs 8999-9002)

WG is nice and boring now

- This is a feature – want protocol stability
- Maintenance mode: key fixes and extensions
  - Potential outlier: multipath
- Other work on top of QUIC is underway
  - DNS (DOQ, also DOH/3)
  - Media (MOQ)
  - BGP
  - NFS (and SMB)
  - …

QUIC Privacy and Security

- Deployed QUIC is “IETF-QUIC“
  - “Google-QUIC” and gCrypto is dead
- Uses TLS1.3, inherits TLS1.3 privacy/security surface
- Immediately benefits from new TLS1.3 features, e.g., ECH
- Mostly two additional principles:
  - e2e authenticate and ideally e2e encrypt (or at least obfuscate) L4 metadata
  - Maximize greasing for all plaintext L4 codepoints

What more to do?

- For QUIC
- For TLS1.3
- Alternatives to TLS1.3?
- More