# QUIC Multiplexing and Peer-to-Peer

draft-aboba-avtcore-quic-multiplexing-02
IETF 103, Banghok

Bernard Aboba – Microsoft
Peter Thatcher – Google
Colin Perkins – University of Glasgow

# Recapping the Problem...

- QUIC is potentially attractive as a transport for peer-to-peer data transfer in WebRTC applications.
  - Reliable transport (defined in draft-ietf-quic-transport)
    - Potential scenario: file transport friendly with audio/video
  - Unreliable transport
    - Potential scenario: fire and forget updates (such as for games), media
      - Unreliable datagram extension: https://tools.ietf.org/html/draft-pauly-quic-datagram
- WebRTC applications (almost always) multiplex SRTP/SRTCP/STUN/DTLS on the same socket, as described in RFC 7983.

# Recap: Requirements for a solution

- STUN: Multiplexing of QUIC with STUN is REQUIRED for all usage scenarios
  - Without this, an equivalent mechanism will need to be reinvented to support P2P.
- DTLS, SRTP, SRTCP: Multiplexing of QUIC with these protocols is REQUIRED to enable QUIC to be used alongside audio/video interoperable with the WebRTC protocol stack specified by the IETF RTCWEB WG.
  - Joint use of QUIC and the SCTP/DTLS/UDP datachannel is a side benefit.

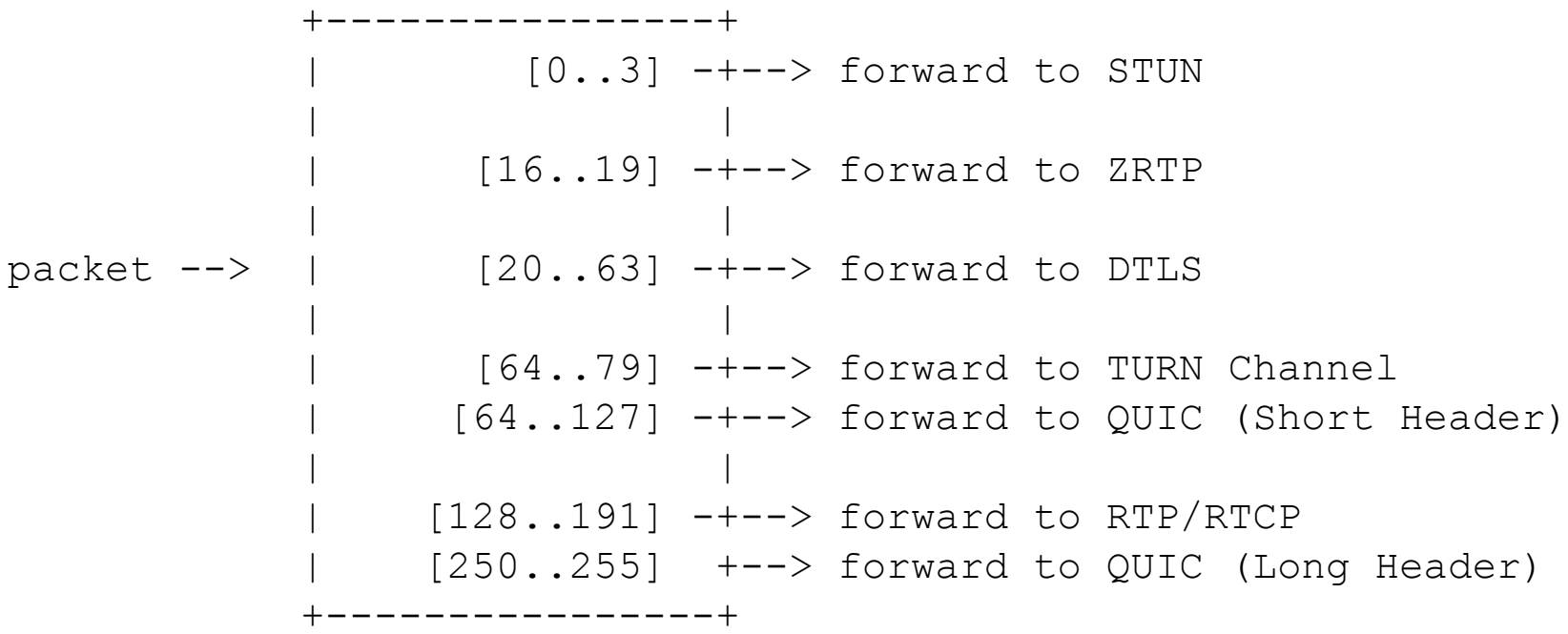
# Recap: Non-Requirements

- TURN channels
  - An optimization not supported in WebRTC implementations, where data packets are exchanged with a 4 octet prefix instead of the standard 36 octet STUN overhead.
- ZRTP: an alternative key exchange mechanism not supported by WebRTC implementations.

# A Brief Recap of Past Events...

- March 30, 2017: Colin Perkins and Lars Eggert first notice the incompatibility of QUIC transport with RFC 7983, and file an Issue against the QUIC transport specification:
  - https://github.com/quicwg/base-drafts/issues/426
- November 16, 2017: Colin Perkins presents to AVTCORE at IETF 100:
  - https://datatracker.ietf.org/meeting/100/materials/slides-100-avtcore-quic-multiplexing-with-rtp-03
- November 29, 2017: Solution proposed to AVTCORE WG proposed as a PR and merged into draft-ietf-quic-transport-08:
  - PR: https://github.com/quicwg/base-drafts/pull/956
- December 18, 2017: PR to undo the changes rejected:
  - https://github.com/quicwg/base-drafts/pull/995

# Recap: Demultiplex Proposed at IETF 100



# (D)TLS Content-Type Field

## TLS ContentType

**Registration Procedure(s)**
Standards Action
**Reference**
[RFC8446][RFC7983]
**Available Formats**

csv

- Content-Type 25 assigned for DTLS 1.3.

| Value | Description | DTLS-OK | Reference |
|---|---|---|---|
| 0-19 | Unassigned (Requires coordination; see [RFC7983]) | | [RFC5764][RFC7983] |
| 20 | change_cipher_spec | Y | [RFC8446] |
| 21 | alert | Y | [RFC8446] |
| 22 | handshake | Y | [RFC8446] |
| 23 | application_data | Y | [RFC8446] |
| 24 | heartbeat | Y | [RFC6520] |
| 25-63 | Unassigned | | |
| 64-255 | Unassigned (Requires coordination; see [RFC7983]) | | [RFC5764][RFC7983] |

# Since Then:  Increasing Traction

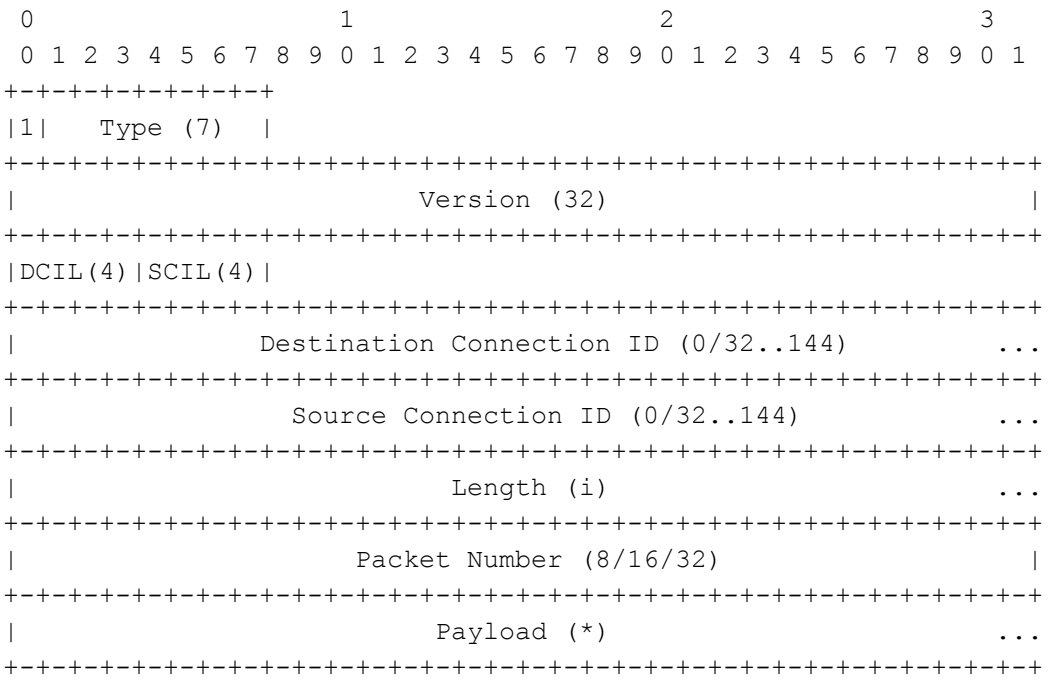
- JS API specification under active development in W3C: https://w3c.github.io/webrtc-quic/
  - Specification has matured from implementation experience
  - Compatibility with recent QUIC drafts, and support for recently added QUIC features (e.g. unidirectional streams).
- Initial implementations coming...
  - May 2018: Chrome Intent to Implement: https://groups.google.com/a/chromium.org/forum/#!topic/Blink-dev/iRJ3as8AYy4
  - Potential experimentation with media scenarios: https://chromium.googlesource.com/external/webrtc/+/lkgr/api/media_transport_interface.h
  - https://mailarchive.ietf.org/arch/msg/quic/tUMYPmNce6XDkingYKkRiTkUdN4

# Why Can’t We Declare Victory Yet?

- History shows that undocumented agreements have a low probability of working out.
  - No documentation of requirements in IANA registries
  - Undocumented algorithms likely to exhibit interoperability problems.
- With trials approaching, we are rapidly approaching an inflexion point:
  - Given current popularity of multiplexing, implementations likely to ***depend*** on it.
  - Multiplexing one of the **major** features motivating adoption of the IETF standard.
  - WebRTC a potentially powerful force for deployment of the QUIC standard: in use by more than 700+ applications, and 1.5+ billion users worldwide.
- Problems with multiplexing support would have **consequences**.
- For these reasons, RFC 7983bis is needed.

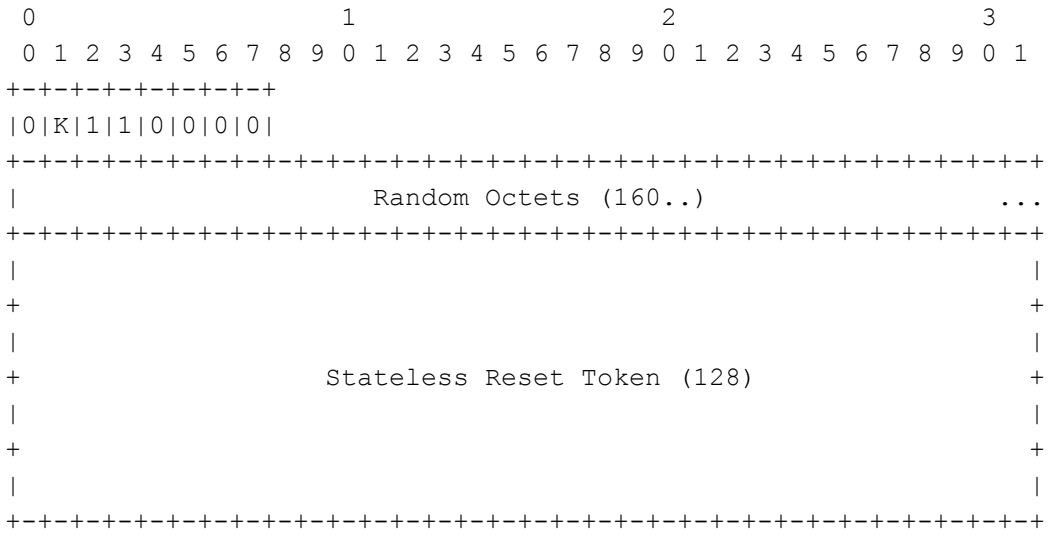
# Evaluation of draft-ietf-quic-transport-16

- Long Header (Section 17.2) and Type field values (0x7C-0x7F) unchanged.  Values 250-255 in first octet can be demultiplexed. Good!



# Concerns about draft-ietf-quic-transport-16

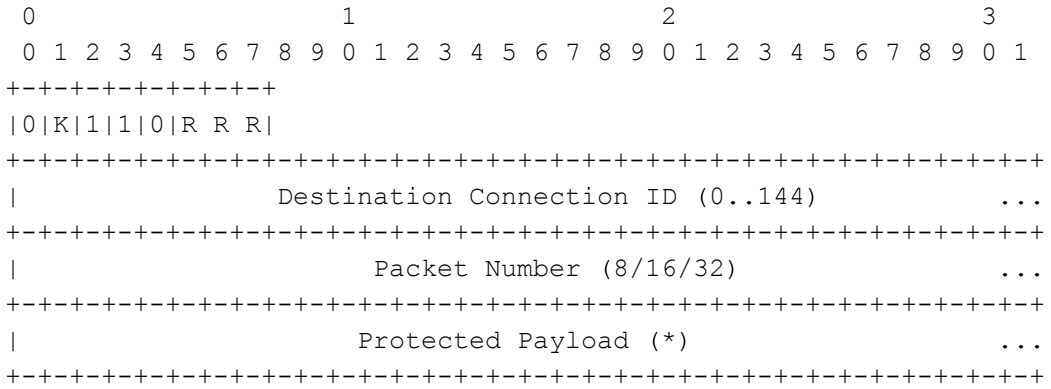
- Stateless Reset Packet (Section 10.4)




Keyphase bit initially set to zero and inverted with each key update.
K = 0 (Value of 48 potential overlap with DTLS)
K = 1 (Value of 112 not an issue)

# Concerns about draft-ietf-quic-transport-16 (cont'd)

- Short header packet (Section 17.3)



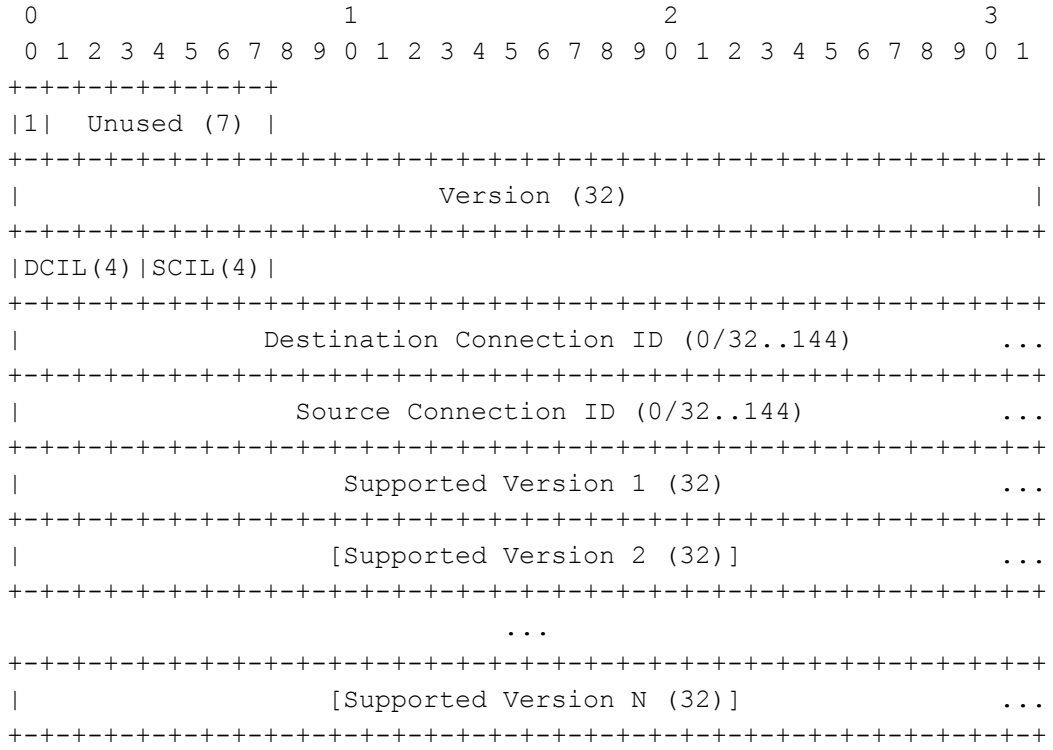

R bits are set randomly.

K = 0 (Values 48-55, potential overlap with DTLS)

K = 1 (Values of 112-119, not an issue)

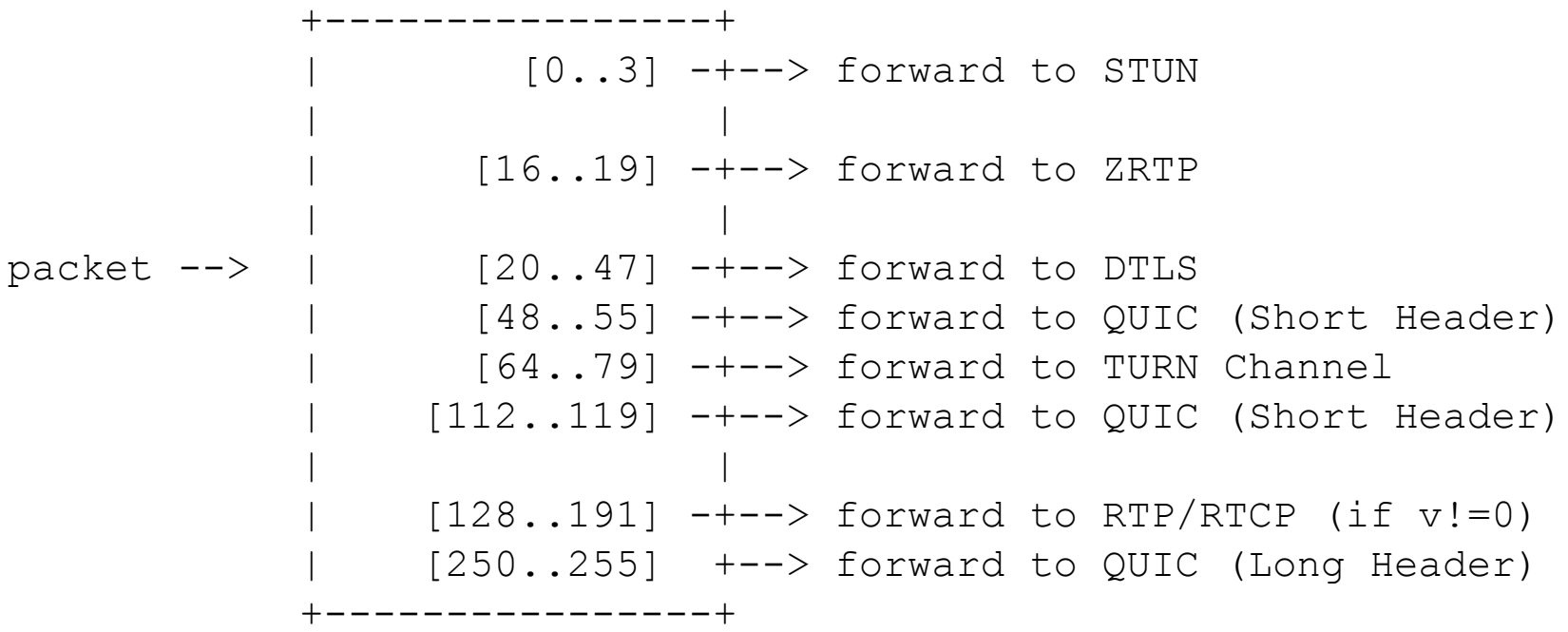
# Concerns about draft-ietf-quic-transport-16 (cont'd)

- Version negotiation packet (Section 17.4)




- Unused bits selected randomly by the server.
- Values 128 - 255 overlap with RTP/RTCP
- Need to check version field, set to zero.

# Revised Demultiplex Proposal



# Call to Action

- Documentation of QUIC multiplexing in RFC 7983bis.
- Additional advice beyond original proposal:
  - Values of 48-55 forwarded to QUIC
  - For values of 128-255, check if value of next 32 bits is set to zero (if so, forward to QUIC)
- Potential change to TLS Content-Type IANA registry:
  - Values 48-55 require coordination (RFC 7983bis)