draft-ietf-quic-transport-01

Changes from -00

- Use of network byte order instead of big-endian (consensus call done)
- Reworked description of packet and frame layout (editorial)
- Replaced DIVERSIFICATION_NONCE flag with KEY_PHASE flag
- Defined versioning
- Error code space is divided into regions for each component

Replacing DIVERSIFICATION_NONCE

- 1 bit in Flags field of packet header
- Required for QUIC Crypto, not needed with TLS 1.3

- KEY_PHASE allows a receiver to know which key to use for decrypting
  - avoids trial-decryption of received packets
  - 1-bit allows only two keys in use at any given time
    - Not enough during handshake
    - more discussion in draft-ietf-quic-tls discussion

Versioning

- QUIC versions are identified using a 32-bit value.
- Versions with the most significant 16 bits of the version number cleared are reserved for use in future IETF consensus documents.

- 0x00000000 is reserved to represent an invalid version.
- First RFC form is version 0x00000001
- IETF drafts are created by adding the draft number to 0xff000000.
  - draft-ietf-quic-transport-01 is version 0xff000001.
- Experimental versions of QUIC to be coordinated on github wiki

Error codes

- 32 bits long, with first two bits indicating the source of the error code
    - 0x0000-0x3FFF: App-specific error codes. Defined by app protocol.
    - 0x4000-0x7FFF: Reserved for host-local error codes. MUST NOT be sent to a peer, but MAY be used in API return codes and logs.
    - 0x8000-0xAFFF: QUIC transport error codes.
    - 0xB000-0xFFFF: Cryptographic error codes. Defined by crypto handshake protocol.
- Error codes from -00 renumbered.
- quic-transport-01 now has only transport error codes.