-06 to -07

AEAD_AES_128_GCM “protection” for cleartext packets

1-RTT long header is gone

Closing changes from interim (see next slide)

Moved stateless reset token to the end

ACK timestamps removed
Closing (partly in -07)

Three termination modes:

- timeout - determined by idle_timeout
- immediate - APPLICATION_CLOSE/CONNECTION_CLOSE
- stateless reset

Two states prior to termination, these share a timer (3RTO)

- draining - can’t send anything, just absorb packets
- closing - as draining, but allowed to resend closing frame

Can transition from closing to draining
Closing - Timeout

Exchange Packets

idle_timeout

draining (3RTO)

A

Exchange Packets

idle_timeout

draining (3RTO)

B
Closing - Immediate

- error detected OR graceful shutdown complete
- closing (3RTO)
- closing becomes draining after confirming that a peer is closing
- draining (3RTO)
Closing - Stateless Reset

C

Packets

Stateless Reset

no state

S

draining (3RTO)
Unidirectional and Bidirectional

We decided to do both plan A and plan B

Unidirectional streams have \( \text{stream}_\text{id} \& 2 == 2 \)

Bidirectional streams have \( \text{stream}_\text{id} \& 2 == 0 \)

Client streams have \( \text{stream}_\text{id} \& 1 == 0 \)

Server streams have \( \text{stream}_\text{id} \& 1 == 1 \)

New state machines coming
Integers

Before, we had a mix of integer encodings

- 8 bit
- 16 bit
- 32 bit
- 64 bit
- 8/16/24/32 bit
- 8/16/32/64 bit
- 0/16/32/64 bit
- bespoke 16-bit floating point

Now just one

2 bits for size (8/16/32/64)

Remainder big endian

- 6 bit: 0x12 = 0x12 = 18
- 14 bit: 0x4567 = 0x567 = 1383
- 30 bit: 0x9abcdef0 = 0x1abcdef0
- 62 bit: 0xe0123456789abcdf = 0x20123456789abcdf

Used in HTTP mapping too
Misc

MAX_STREAM_DATA is octets

PONG frame (for address validation post-handshake)

Renamed packet types and removed client/server split

  Initial, Retry, Handshake, 0-RTT (1-RTT uses short header)