Packet Number Space(s)

Christian Huitema

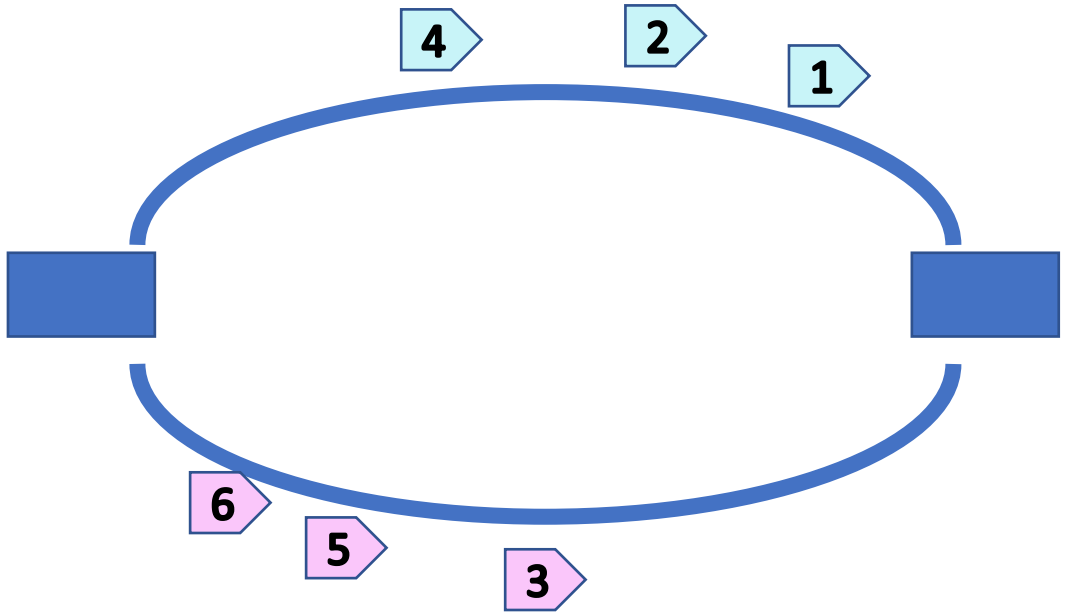
October 18, 2021

Why two options for numbering packets?

Numbering packets

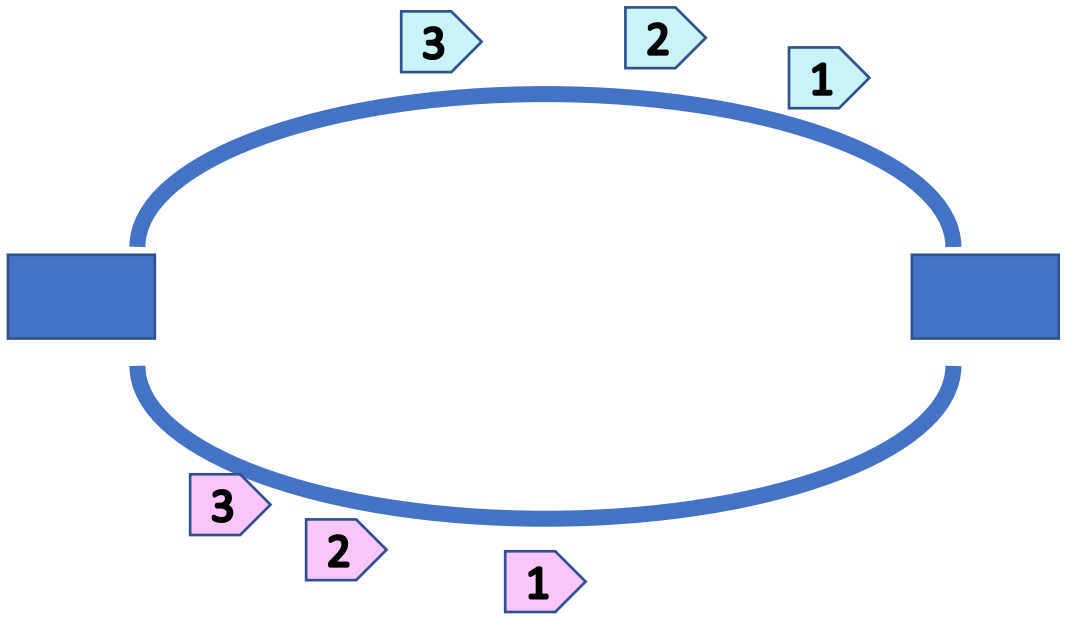
- Two options
  - Single number space (draft-huitema)
  - One number space for each path (draft-liu, draft-deconinck)
- There are pros and cons in each approach

Single Number Space



- Packets are numbered in sequence, as they are sent
- Same as QUIC V1
- Same ACK format as QUIC V1
- Sender keeps track of which packet went on what path
- Out of sequence delivery common if paths have different latencies

Multiple Number Space

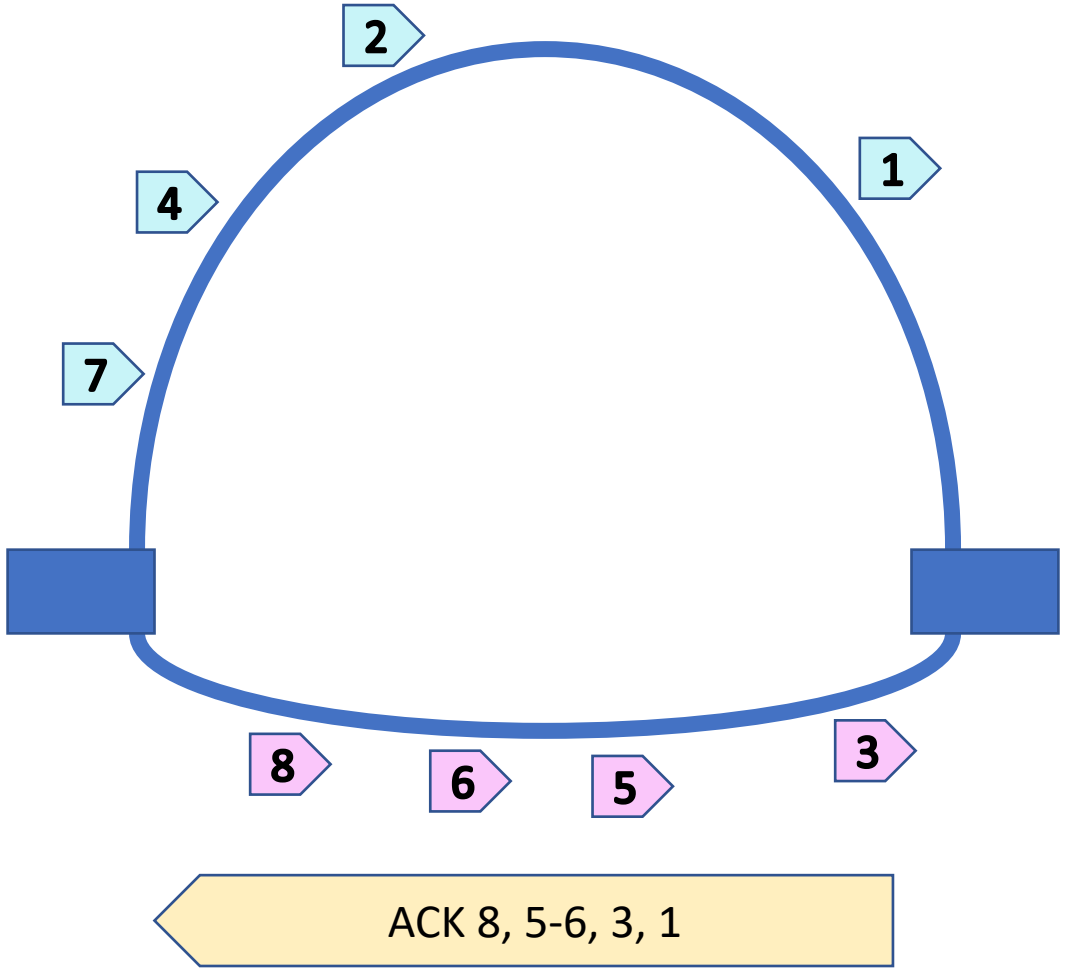


- On packet sequence per path
- Sender maintains separate list of packets waiting for acknowledgements per path
- New “per path” acknowledgement frame
- Requires changes in packet encryption/decryption

Encryption-decryption issue (Multiple spaces)

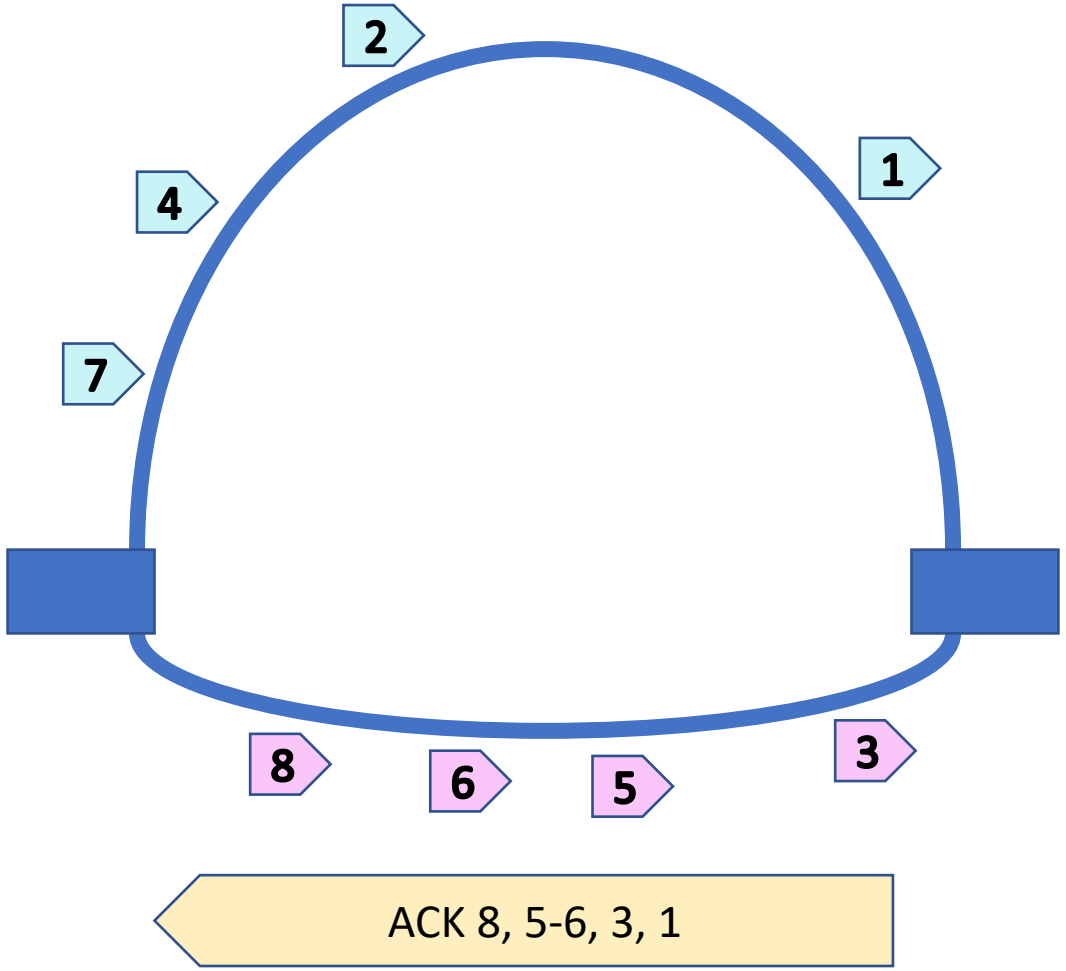
- Default behavior:
  - AEAD Nonce = IV + 64 bit packet number
- But same PN on multiple path means same nonce
  - Not compatible with AEAD, same nonce means same encryption
- Solution: 96 bit AEAD nonce
  - AEAD Nonce = IV + (32 bit CID sequence number | 64 bit packet number)
  - Supported by several TLS stacks
- Not possible if using NULL CID

ACK Ranges issue (single space)



- Paths with different latencies
  - Out of order deliveries
  - Large number of ACK ranges
  - Case of CWIN = 10,000 packets?
- Mitigate requires smarts
  - Send in batches (GSO)
  - Limit number of ranges in ACK
  - Limit number of ACK per range
  - ACK horizon
  - ACK of ACK

Loss recovery issue (single space)



- RFC 9002 specifies RACK
  - Assumes approximate in order delivery
  - Multipath breaks that
- Mitigation
  - Remember send path of packet
  - Perform RACK logic “within a single path”

Pros and cons

Single space

- Support for NULL CID
  - Minimal transmission overhead
- Fewer code changes
  - Lots of code assumes single packet number space
- Does not require 96 bit nonce
  - Fewer crypto stack requirements
- Allows implementation trade-offs
  - Complexity vs efficiency

Multiple spaces

- No worries about ACK ranges
  - Works well, even if large CWIN
- Simple logic
  - Per path version of RFC 9002 algorithms
- Does not require implementation trade-offs

Decision so far: just specify both options

- Allow for negotiation during handshake
  - Chose one, or other, or none.