QUIC-LB Update

When last we met...

- Too many choices
- Not many implementations, no interop

Progress!

- Improved the (misnamed) Stream Cipher algorithm -- thanks Christian
- Consistent nomenclature across algorithms
- Abandoned Dynamic SID allocation -- reached consensus it’s too cute
- Inkling of more implementations out there

My Preferred Path

1. Await crypto review of Stream Cipher Algorithm
2. Delete Block Cipher
3. Split load balancer and retry service drafts
4. Editorial Pass
5. Profit!

Backup

Why Block CID?

Stream CID has similar security properties (?)

Longer CIDs

Use case for block CID is:

- OK with long CIDs
- Fine with doing an encryption pass
- Not fine with doing three encryption passes

Is encryption per-packet or per-4tuple?

Splitting the Documents

BOTH RELATE TO MIDDLEBOX COORDINATION, BUT OTHERWISE DISTINCT

Version Independent (ish)

Focused on Connection IDs

Version-dependent

No dependencies outside Retry

One of many potential offloads