QUIC-LB Open Issues

IETF 109

Martin Duke, F5 Inc.

Significant changes since draft-03

- Deleted Obfuscated CID algorithm after feedback here
- Reworked Shared-State Retry format
- Lots of editorial cleanup/clarification
- I open-sourced algorithm library: https://github.com/f5networks/quic-lb
- I open-sourced NGINX load balancer implementation: https://github.com/martinduke/nginx-quic-lb
- Ant Financial NGINX LB implementation: https://github.com/alipay/quic-lb

Feedback since IETF 108

- Ant Financial critiques of Retry Service addressed
- Request for UDP proxy protocol
- Ops area not all that interested
- 5 Open issues remain

#12 More Config Rotation Bits

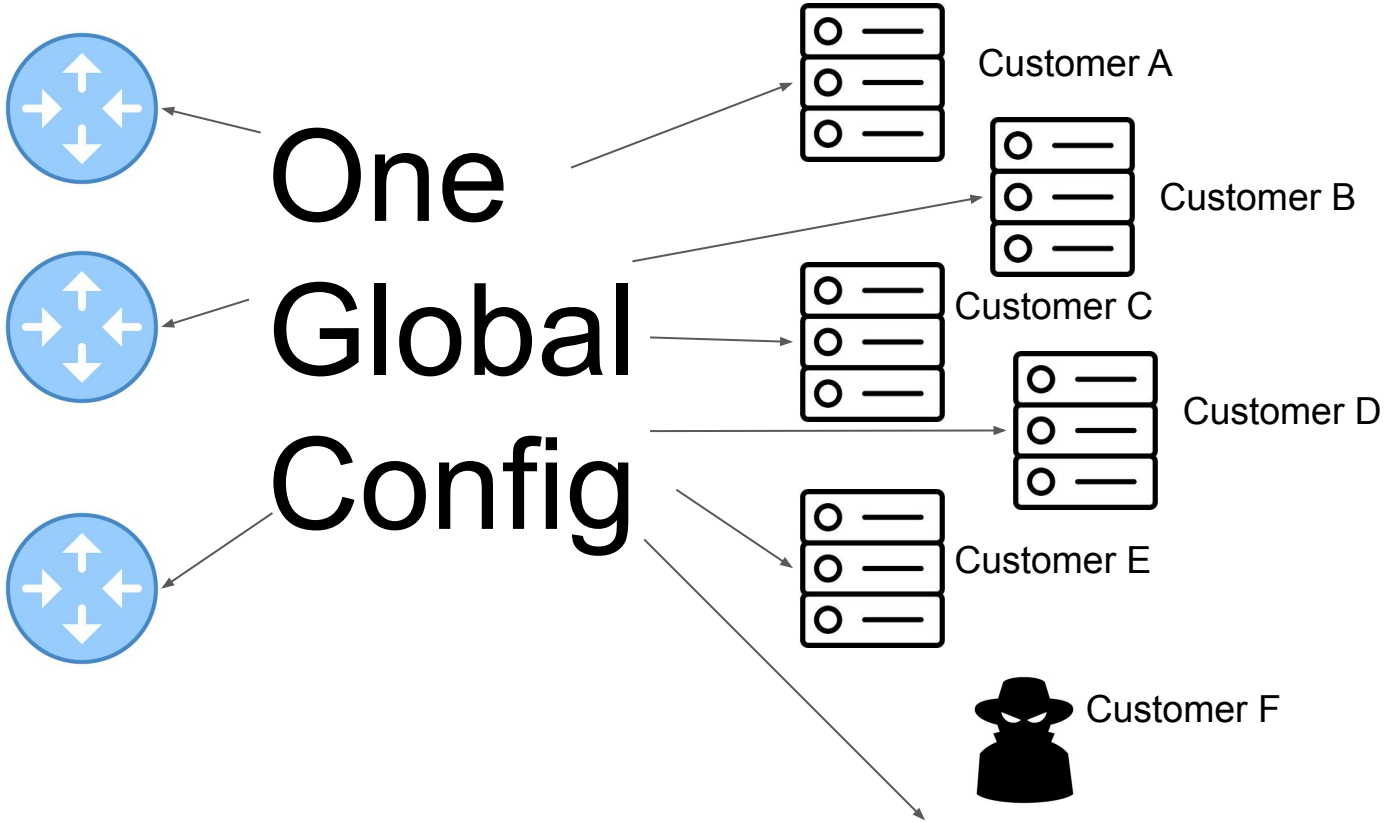
- We have two bits to allow gradual deployment of new configs (took one codepoint for something else)

Cfg Rotation (2)	CID Length (optional, 6 bits)

- Proposal to make it 3

Why more?

MegaCloudCorp



Separate server pool by...

- Load balancer instance
- Virtual IP/Port
- SNI (or similar)

We can…

- Assign CR bits, which means SNI is linkable across CIDs by everyone
- Make them share a config (limited server mapping exposure) <-

Discussion (#12)

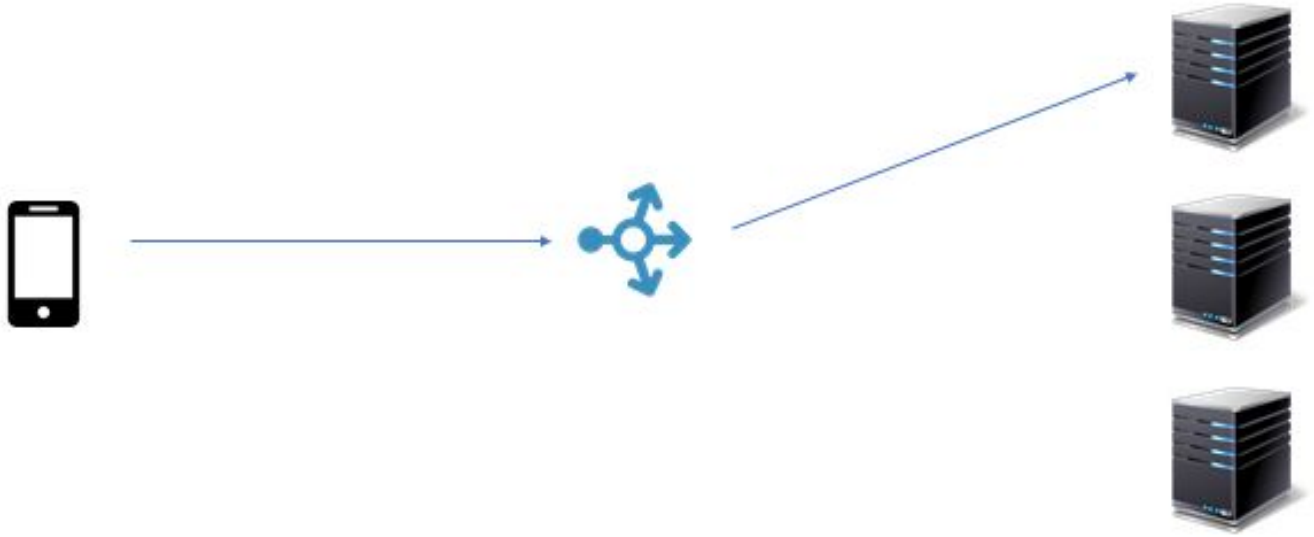
#8 Unguessable Connection IDs

quic-transport, sec 5.1:

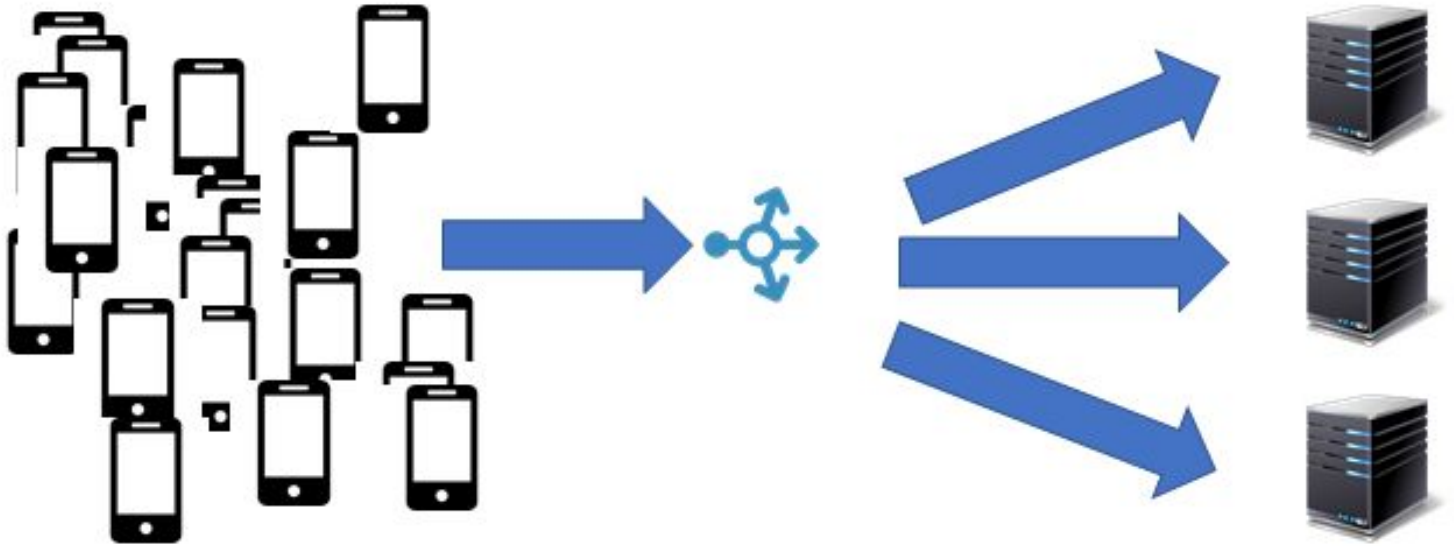
> Connection IDs MUST NOT contain any information that can be used by an external observer (that is, one that does not cooperate with the issuer) to correlate them with other connection IDs for the same connection.

Plaintext CID clearly violates this

Perfect Linkability



Perfect Unlinkability



#16 Giving the Client More Information

- Server chooses the encoding, client bears the linkability consequences
- disable_active_migration? then Plaintext Is just about NAT rebinding
- Add a transport parameter to communicate the compromises the server is making

Recommendation: Remove all restrictions, add a server TP that indicates unencrypted CID (see PR #58)

Discussion (#8 and #16)

#35 Shared-State Retry Token format

The encoding and encryption technique is simple but sacrifices some entropy.

We can do better; a PR would be welcome.

Configuration?

PRs welcome