QUIC-LB Open Issues

Significant changes since draft-02

- New Stream Cipher Algorithm with better security properties (thanks Christian)
- Tweaked design to improve version invariance and listed assumptions
- More security considerations

Feedback since IETF 107

- Reviews from Martin T and Christian (thanks!) are reflected in Issues/PRs
- Outreach to cloud providers has largely failed to date
- One provider is extremely reluctant to implement anything besides the plaintext algorithm
- request early review from ops area?
- 3 Open issues remain

#12 More Config Rotation Bits

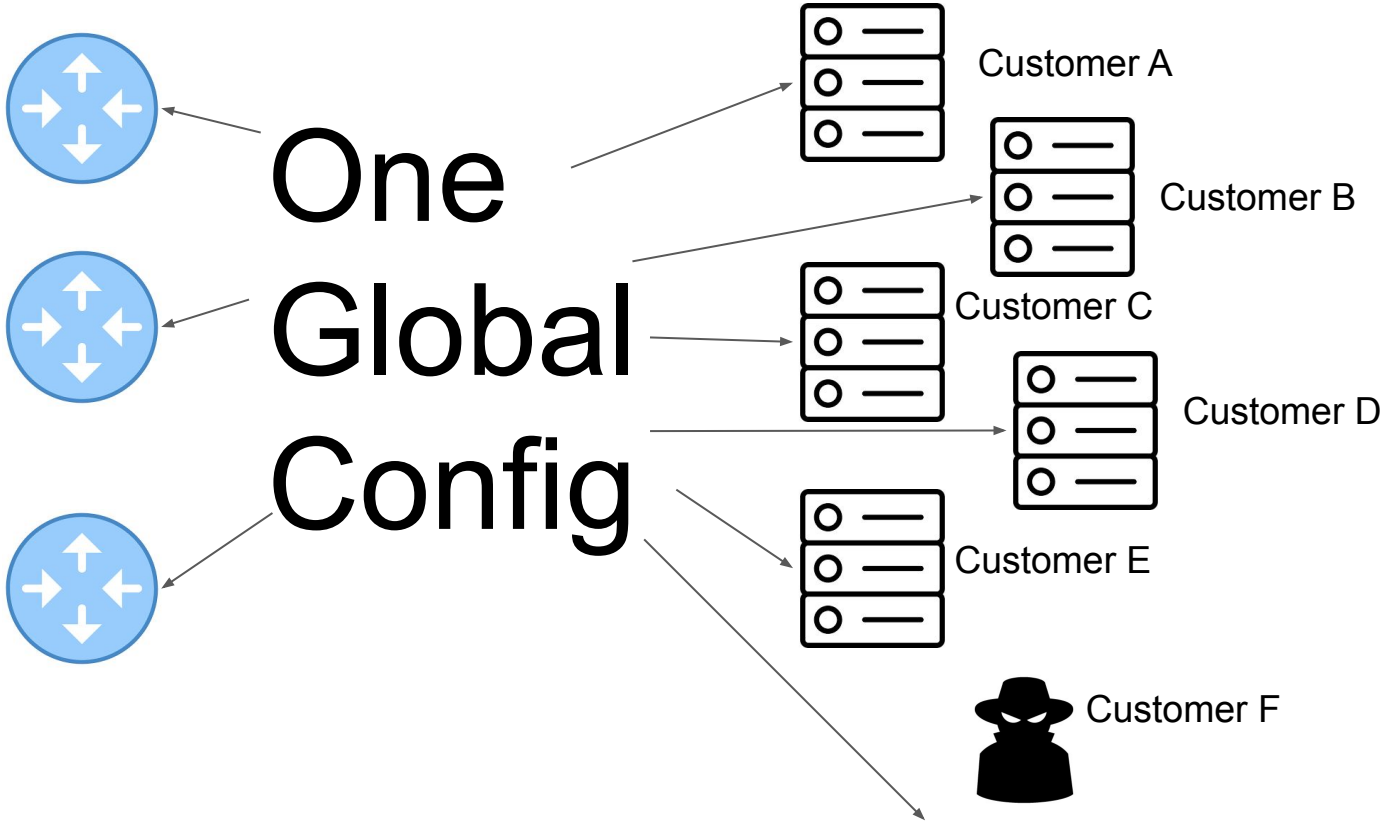
- We have two bits to allow gradual deployment of new configs (took one codepoint for something else)

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

- Proposal to make it 3

Why more?

MegaCloudCorp



Separate Config by...

- Load balancer instance
- Virtual IP/Port
- or more config rotation bits? (if e.g. SNI switched)

BUT this leaks information

Discussion (#12)

#8 Unguessable Connection IDs

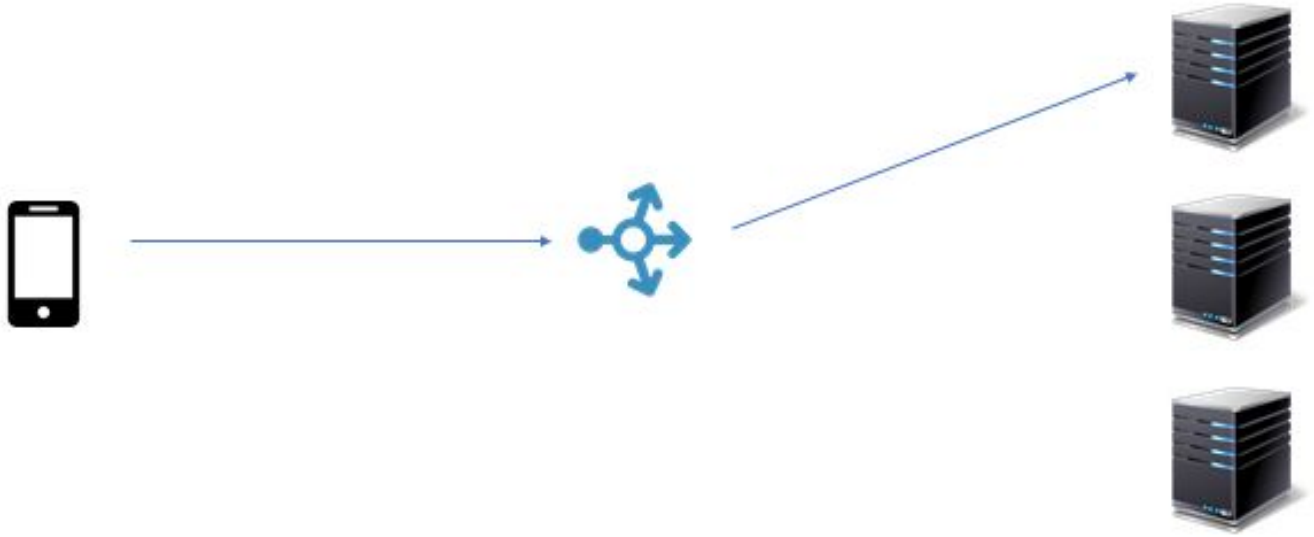
quic-transport, sec 5.1:

> 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.

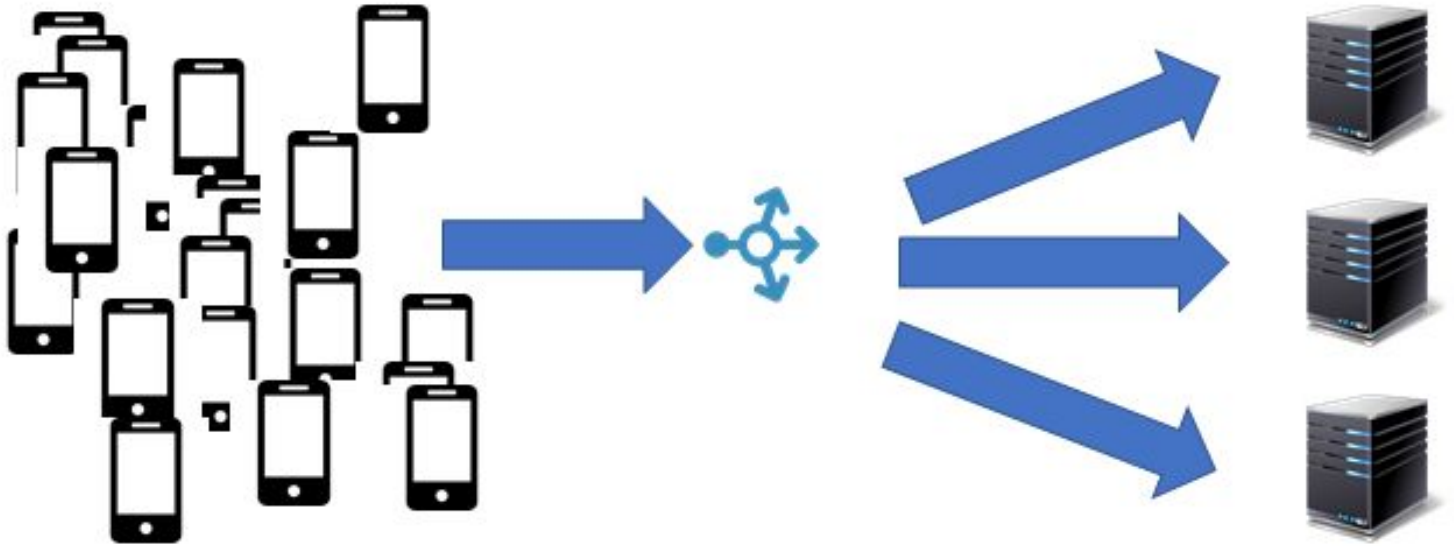
Plaintext CID clearly violates this

Obfuscated CID maybe does

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

Discussion (#8 and #16)