Building Peer-to-Peer QUIC

Floris Bruynooghe

number 0

https://mastodon.social/@flub

https://mastodon.social/@n0iroh

Why p2p QUIC

Iroh: connect any two devices

- Empower user agency
- Works today

QUIC Transport Protocol

- TLS encrypted
- Multiple, cheap streams
- Unreliable datagrams
- 0-RTT
- Built on top of UDP

Iroh's Architecture

Priorities

- 100% reliable
- Fast time to first byte
- Low-latency direct connections

Iroh Relay Server

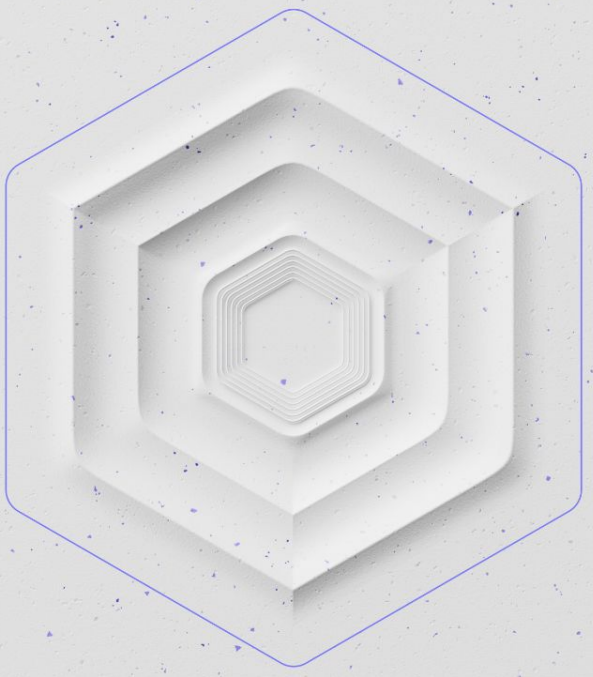
- A very ordinary HTTPS server
- HTTP 1.1 connection upgrade
  - Blind datagram forwarding
- STUN

Dial by NodeId

- An ed25519 key for every Endpoint
- Public key is *identity* and *address*
- Integrated into TLS

Practical addressing:

- NodeId + (Relay URL || UDP addr)
- Node discovery via DNS, …



IETF Drafts

Iroh today

- Works *besides* QUIC
- QUIC grease bit
- Multiple paths inside socket

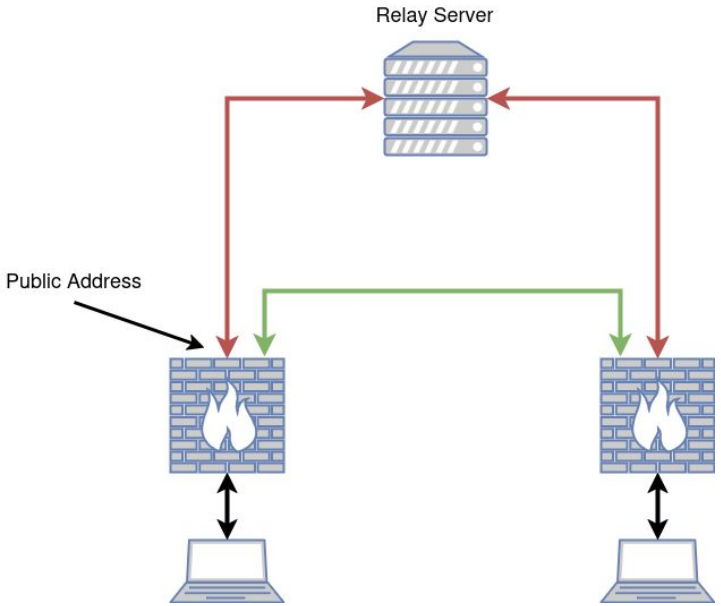
Soon™

QUIC Multipath

QUIC Address Discovery

QUIC NAT traversal

QUIC Address Discovery



Replaces STUN

- Encrypted
- Reliable
- Negotiated with transport parameters
- OBSERVED_ADDRESS frames
  - Events

draft-seemann-quic-address-discovery-04

Using QUIC to traverse NATs

Multipath variation

- Server sends ADD_ADDRESS frames
- Client initiates holepunching
- Both probe paths using PATH_CHALLENGE frames

draft-seemann-quic-nat-traversal-02

Multipath Extensions for QUIC

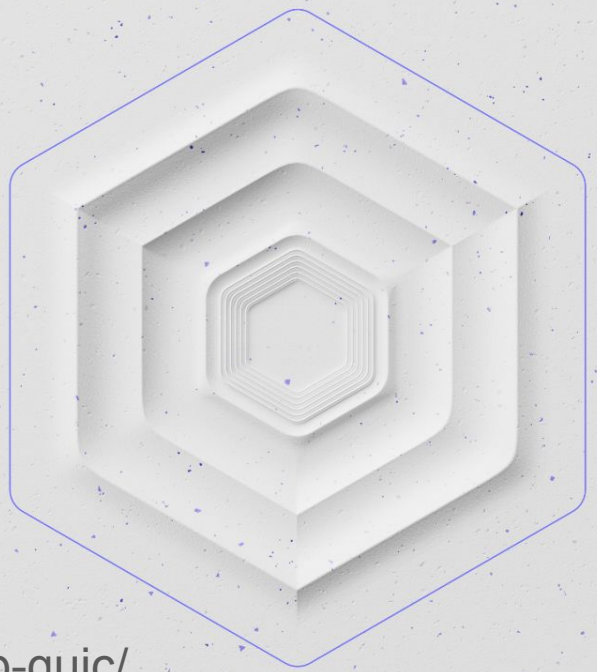
- Several IP paths between endpoints
- Each path has:
  - Congestion controller
  - MTU
- Path preferences
  - PATH_STANDBY
  - PATH_AVAILABLE

draft-ietf-quic-multipath-12

Acknowledgements

Christian Huitema

Martin Seemann



https://seemann.io/posts/2024-10-26---p2p-quic/