Building QUIC Multipath

Floris Bruynooghe

number 0

https://mastodon.social/@flub

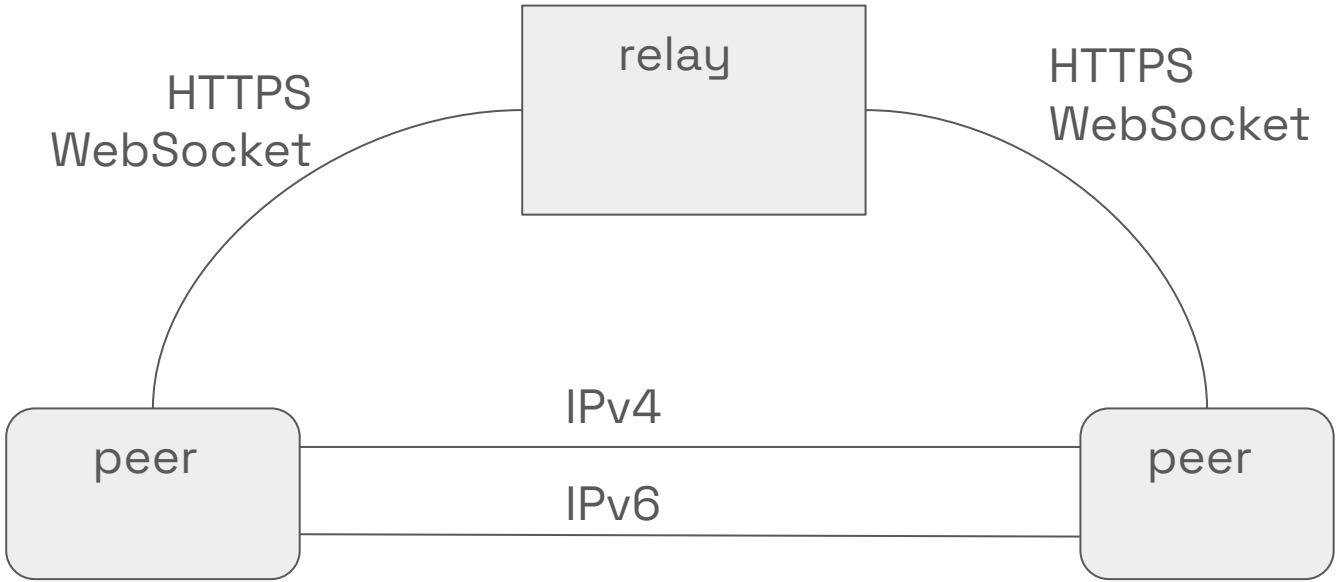
https://mastodon.social/@n0iroh

fast, efficient, reliable connections

iroh

 p2p & holepunching

relay path



direct IP paths

Managing multiple paths for QUIC connections

draft-ietf-quic-multipath-19

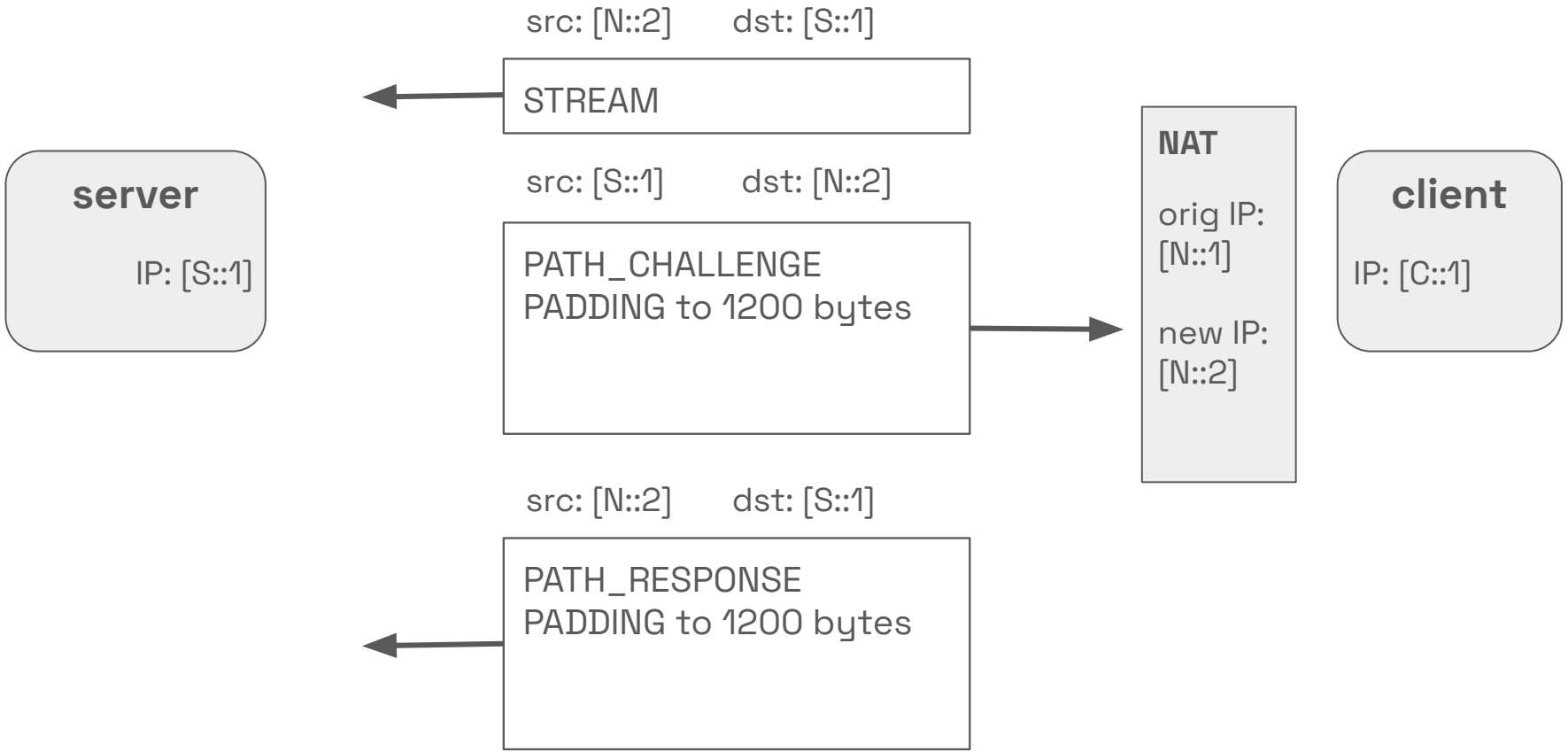
Paths in RFC9000

clients can migrate

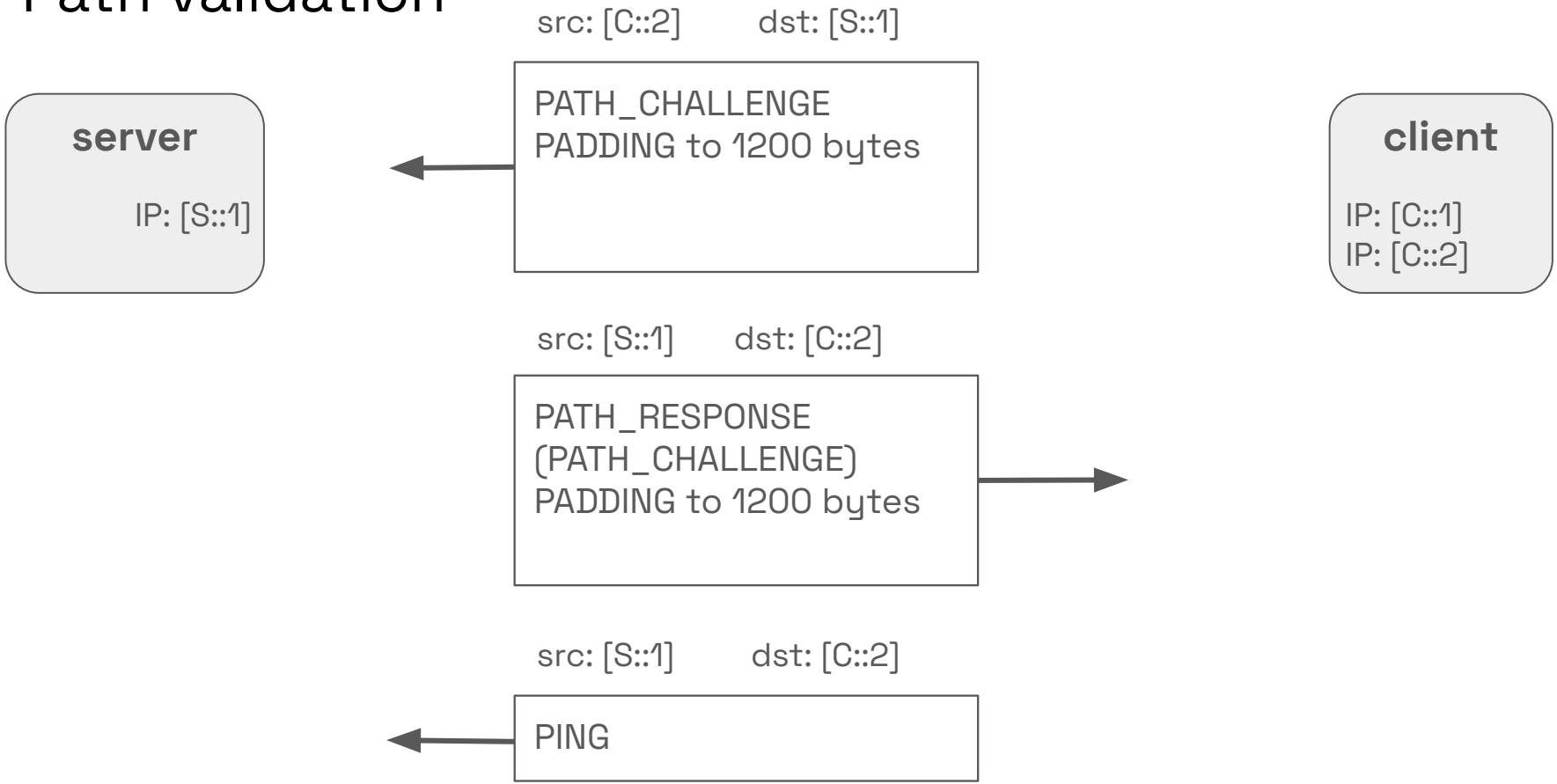
- path probing with PATH_CHALLENGE
- path switching with non-probing packets
  - **only one active path**

involuntary migration: NAT rebindings

Path validation (involuntary migration)



Path validation



Packet Number Spaces

RFC9000

- Initial
- Handshake
- Data

Crypto Nonce: PN

Multipath

- Initial
- Handshake
- Data
  - Path ID 0
  - Path ID 1
  - Path ID 2
  - ...

Crypto Nonce: PN + PathId

Space & Path State

Before Multipath

Per Connection:

- PathData
  - Congestion controller, ...
- Prev PathData

Per Space:

- crypto keys
- pending data
- PNs, sent packets, ...

Multipath

Initial, Handshake & Data Space:

- crypto keys
- pending data

Per Path ID:

- PNs, sent packets
- PathData
- Prev PathData
- pending data

Connection Identifiers

Where are packets from?

- Packet headers unchanged
- CIDs
- At ~fixed offset in header
- *Issued by peer*

  `NEW_CONNECTION_ID` → `PATH_NEW_CONNECTION_ID`

  - Multipath: per path ID
  - CIDs are now fallible!

Managing Paths

Path open

- Only clients
- Send or Receive
  any packet on PathID
- To **use** a path it must be validated
  → PATH_CHALLENGE

Path close

- Client or server
- PATH_ABANDON
- Peer *should* confirm
- Drain in-flight packets

Packet Scheduling

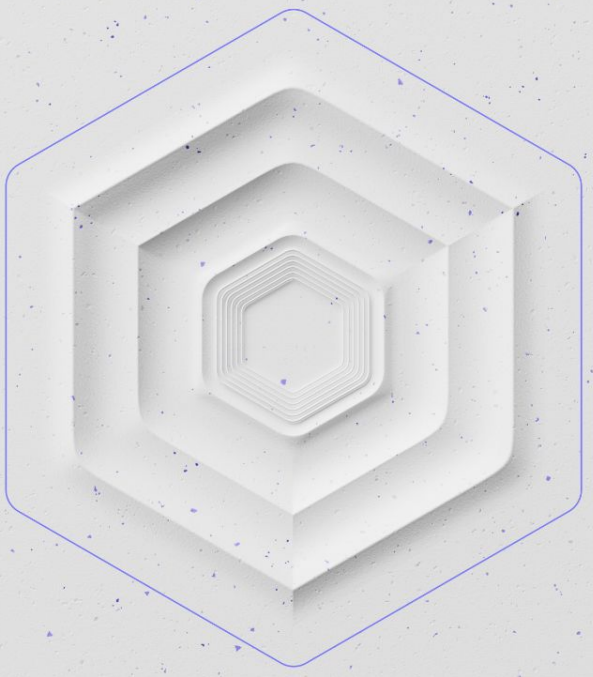
What path do you send on?

- PATH_STATUS_BACKUP / PATH_STATUS_AVAILABLE
- You need:
  - Validated path
  - CID
  - Congestion control window & pacing

QUIC NAT Traversal (iroh version)

- QUIC extension
- Requires multipath
- Use PATH_CHALLENGEs for holepunching
- Server address candidates: ADD_ADDRESS
- Initiate round with REACH_OUT
- Clients probes on new PathID
- Server probes off-path

Thanks!



https://iroh.computer