Lars Eggert

Firefox Networking

Browser meets network

- **HTTP:** H1, H2, H3
- **Transports:** TCP, TLS, UDP, QUIC
- **Naming:** DNS, DoH
- **Proxying:** SOCKS, MASQUE, OHTTP
- **Features:** ECH, WebSocket, WebTransport, PQC
- **Related:** Disk cache, cookies, WebRTC, WebPKI, TRR, Happy Eyeballs

Also: Security, privacy, operational aspects, performance, telemetry and OS interfaces for all of these.

smörgåsbord

Browser meets network 2025+

- HTTP: H1, H2, **H3**
- Transports: TCP, TLS, **UDP**, **QUIC**
- Naming: **DNS**, **DoH**
- Proxying: SOCKS, **MASQUE**, **OHTTP**
- Features: **ECH**, WebSocket, **WebTransport**, PQC
- Related: **Disk cache**, **cookies**, WebRTC, **WebPKI**, **TRR**, **Happy Eyeballs**

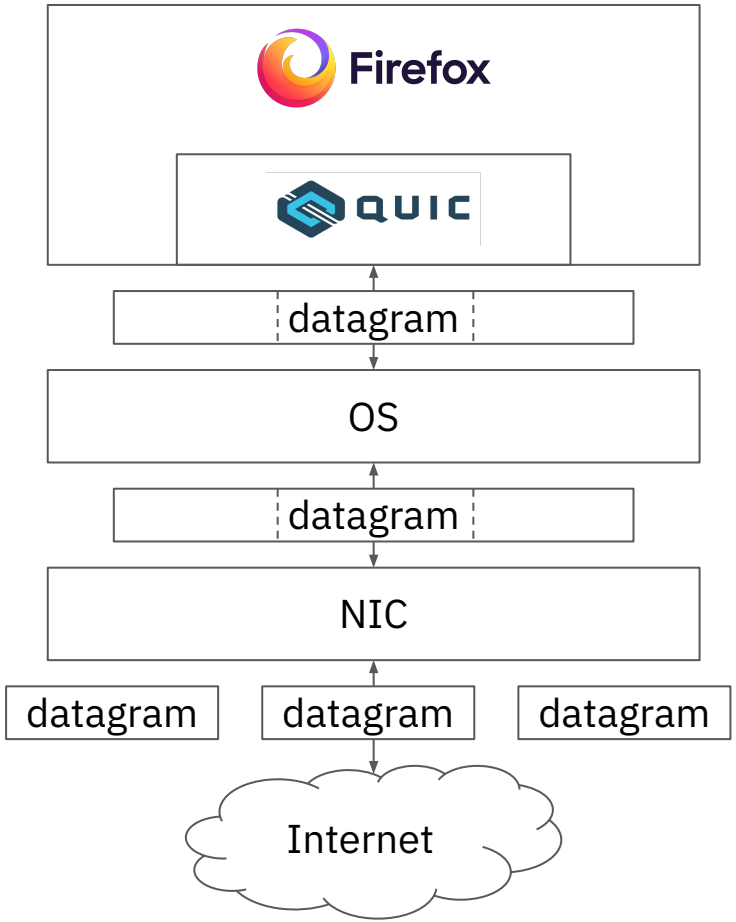
Also: **Security**, **privacy**, **operational aspects**, **performance**, **telemetry** and **OS interfaces** for all of these.

smörgåsbord

QUIC

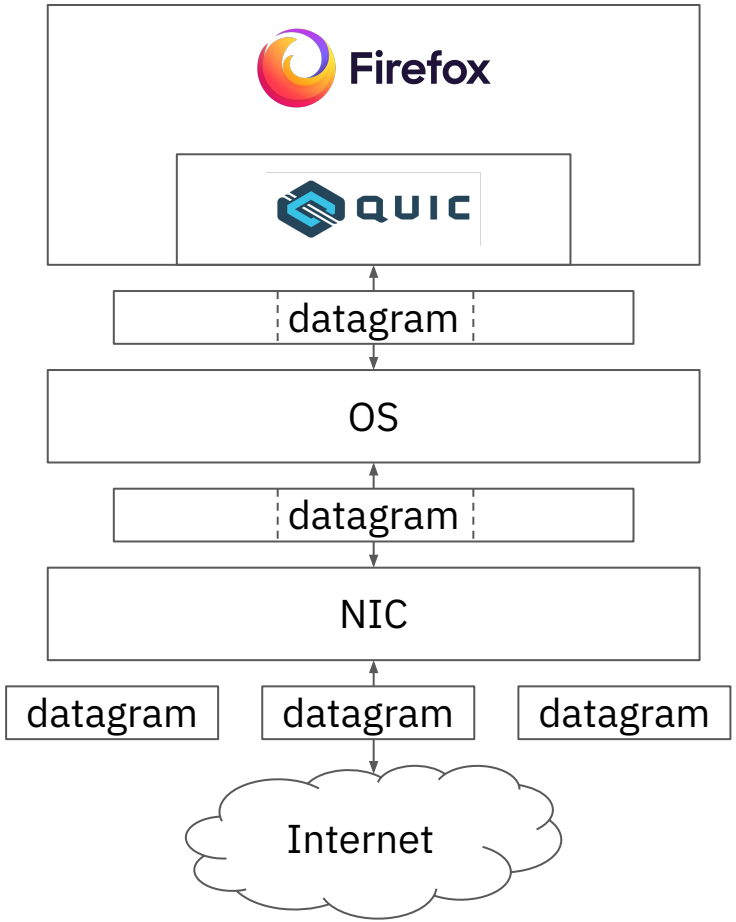
Fast UDP I/O

- **Spotty OS support**
  - Apple: no (official) multi-message
  - Windows: buggy GSO/GRO
- **Open questions**
  - Interactions with packet pacing
  - Tuning of constants
    (e.g., segment size)
  - Packet batch I/O
    (e.g., memory management)



PLPMTUD

- **Packetization Layer Path MTU Discovery for Datagram Transports**
  - RFC 8899
  - “PMTUD without ICMP”
  - 1280 vs. ~1500 matters
- **Open questions**
  - How to go 1280 → PMTU in min. number of tries, esp. miss-tries?
  - (Today and in the future)



QUIC ACK frequency

- **ACKing every 2nd packet @ 1 Gbps ~= 40k ACK/s**
  - 1 Gbps / 8 / 1500 / 2
  - It’s not quite that bad, most stacks drain RX before TX
- But still: ACK processing is expensive, esp. at server
- **Approach: sender proposes an ACK rate to receiver**
- **Open questions**
  - Relevance? Given segmentation offloading and pacing
  - Performance benefits? On high throughput connections
  - Downsides? ACK clocking, RTT sampling accuracy, ...

Congestion control

- **Slow start:** Classic, HyStart++, SEARCH or SUSS?
- **CC:** NewReno, CUBIC, BBR or else?
  - ECN with the above, or maybe L4S and Prague?
- **Open questions**
  - ^^^

Encrypted Client Hello

- TLS SNI is the last bit of plaintext
- ECH can encrypt that – but!
  - Low ECH adoption (only Cloudflare, basically)
  - Easy to block based on outer SNI
  - Needs DoH (or other encryption) to get ECH config
- **Open questions**
  - How do we get more ECH?
  - How do we get more DoH? (Or what instead of DoH?)

Anti-~~censorship~~bad firewalling

- Firewalls introduce (non-intended) breakage
  - (Insert war stories here)
- How can we make it harder to ship bad firewalls?
- GREASE, but more
- Shipped some things to force QUIC firewalls to be smarter
  - https://gfw.report/publications/usenixsecurity25/en/
- **Open questions**
  - What else can we do, ideally in a way that is always-on?

Proxying

Proxying today

- Plenty of protocols
  - SOCKS
  - HTTP CONNECT
  - ...
- How to proxy HTTP/3? UDP on top of TCP?
- **Send encrypted, congestion-controlled-but-still-unreliable datagrams** (with a fallback)

<table>
<tr><th>➡️ Inner
⬇️ Outer</th><th colspan="2">HTTP1</th><th colspan="2">HTTP2</th><th>HTTP3</th><th>WebRTC</th></tr>
<tr><td>HTTP1</td><td colspan="3" rowspan="2">now: HTTP CONNECT

future: connect-tcp with fallback to HTTP CONNECT</td><td rowspan="3">now: –

future: connect-udp via HTTP Capsules</td><td>now: –

future: connect-udp via HTTP Capsules and connect-udp-listen</td></tr>
<tr><td>HTTP2</td><td rowspan="2">now: –

future: connect-udp
• via HTTP Datagrams (if QUIC Datagram extension is available)
• or HTTP Capsules and connect-udp-listen</td></tr>
<tr><td>HTTP3</td><td colspan="3">now: –

future: connect-tcp with fallback to HTTP CONNECT</td></tr>
<tr><td>WebRTC</td><td colspan="5">never</td></tr>
</table>

MASQUE

- Single & two-hop proxy (c.f., iCloud Private Relay)
- Selective proxying (web trackers, FavIcon fetch, ...)
- MASQUE vs. OHTTP
  - MASQUE: replay defense, forward secrecy
  - OHTTP: request/response, unlinkability
- Double congestion control a problem in masque
- **Open questions**
  - Performance?
  - Privacy differential?

smörgåsbord

Getting off getaddrinfo

- Want: asynchronous resolution of multiple RRs
  - esp. relevant for Happy Eyeballs v3
- Want: HTTPS records on all platforms
  - Thus more QUIC
- Want: Bypass various OS bugs
- **Open questions**
  - Operating specific optimizations

Happy Eyeballs v3

- v1 in Firefox too easily falls back to H1/H2, less QUIC/H3
- New in v3
  - **Explicit design goal: prefer IPv6 and QUIC**
  - Support for HTTPS resource records
  - Discovery of alt. endpoints, protocols (H3), ECH configs
- **Open questions**
  - Impact on connection establishment latency
  - Constant tuning (e.g., *Connection Attempt Delay*)

DoH

- Improve Trusted Recursive Resolver (TRR) program
- Fallback via *Discovery of Designated resolvers*
- Rollout on Android
- Open questions
  - Performance impact of DoH
  - Global deployment
  - Optimizations (e.g., QUIC 0-RTT)

Open telemetry

We have lots of telemetry...

- ...and some of it is already open, and you can just use it: https://glam.telemetry.mozilla.org
- Much more can be made open or at least made available, please talk to us

- We care about privacy, so PII is stripped,
  and we enforce a resolution cap on SQL query results

Labeled Counter Active

DESCRIPTION

Number of paths known to be ECN capable or not-capable.

more info

AGGREGATION METHOD

sum

UNIT
n/a

EXPIRES
never

SEND IN PINGS
metrics

BUGS
bugzil.la/1902065

DATA REVIEWS
bugzil.la/1902065

NOTIFY
necko@mozilla.com
minden@mozilla.com

VIEW SQL QUERY

explore / networking.http_3_ecn_path_capability (GLEAN)

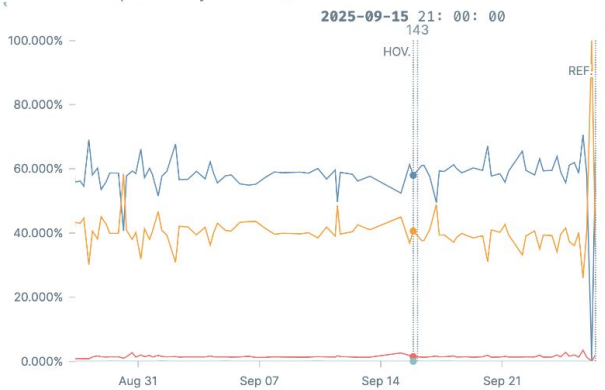
TIME HORIZON
WEEK | MONTH | QUARTER | ALL

CATEGORIES
CAPABLE | BLACK-HOLE | BLEACHING | RECEIVED-UNSENT-ECT-1

METRIC TYPE
PROPORTION | TOTAL CLIENTS

★ REFERENCE **2025-09-26** 09:00:00 570 clients 12,437 samples
● HOVERED **2025-09-15** 21:00:00 **27,208** clients **935,064** samples
(11 days before reference) +26,638 **(4673%)** +922,627 **(7418%)**

Proportions by Build ID



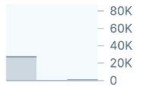
compare

Summary

CAT.	● HOV.	★ REF.	DIFF.
capable	57.97%	62.05%	-4.09%
bleaching	40.58%	35.98%	4.59%
black-hole	1.44%	1.96%	-0.52%
received-unsent-ect-1	0.01%	0.00%	

Client Volume by Build ID

Compare



Thank you

 https://github.com/mozilla/neqo

Lars Eggert, lars@eggert.org
 lars@social.secret-wg.org