

# Using onion routing with CoAP

`draft-amsuess-t2trg-onion-coap`

*Christian Amsüss, Marco Tiloca, Rikard Höglund*

IETF118 Prague, T2TRG, 2023-11-03

# Essence of the document

CoAP proxying, OSCORE (with proxy support) and EDHOC give us building blocks that allow Tor-like REST operations, even on constrained devices.

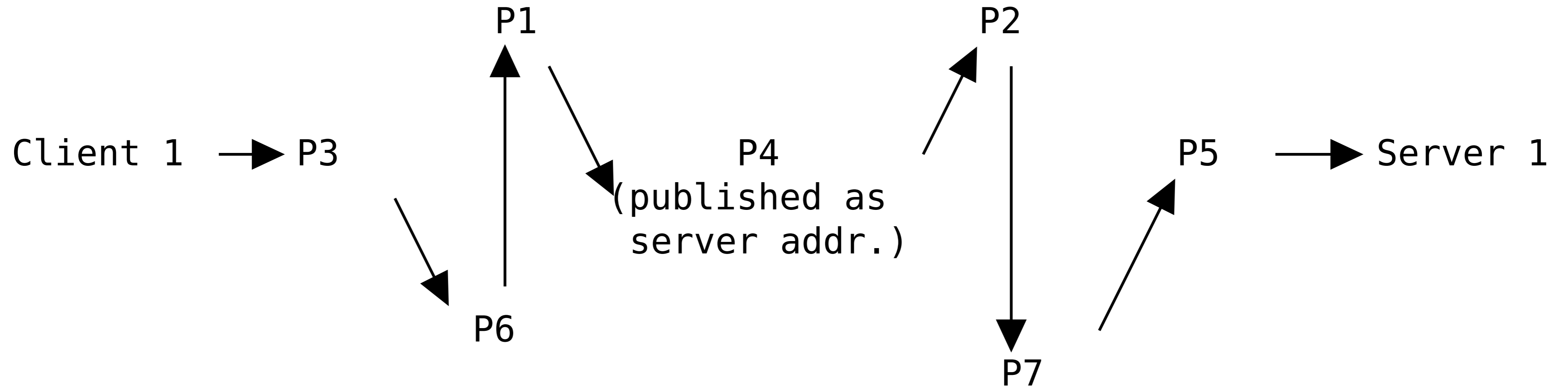
We “just” need a little glue: proxy (chain) discovery and setup, and names (see also Non-IP Cluster).

# This builds on...

- CoAP RFC 7252, OSCORE RFC 8613, EDHOC draft [ietf-lake-edhoc](#)
- OSCORE capable proxies draft [tiloca-core-oscore-capable-proxies](#)
- Transport Indication draft [ietf-core-transport-indication](#)
- Cryptographic identifiers as names and their discovery draft [amsuess-t2trg-rdlink](#)
- ...and some building blocks that may be generic enough to pull out of the current sketches (e. g. setup of reverse proxies)

# Plot, plot, networks, baby, figure 1 will be amazing<sup>1</sup>

An example network graph of many proxies



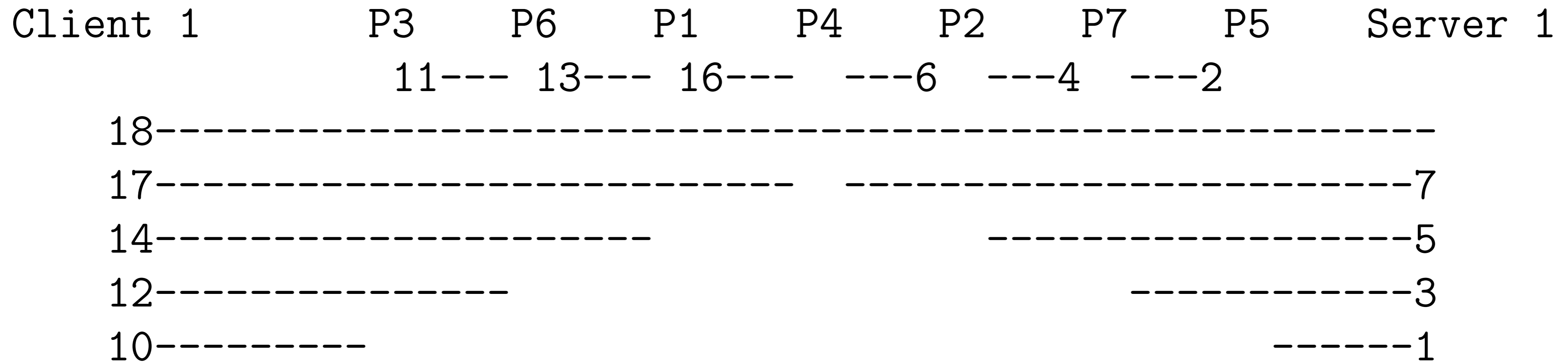
Arrow directions indicate direction of request.

---

<sup>1</sup>To the tune of [Bad Project / Bad Romance](#). Note the future form of the auxiliary.

# Figure 2

Peeling the onion's layers



Numbers at the initiator's side indicate the sequence of established network security contexts. Steps 8 and 9 (address announcements) and 15 (client looks up hidden service, finds P4 to be the announced address).

# It's just a choice

Opt-in by both parties.

If nobody decides to be hidden, it's plain CoAP.

(Or EDHOC, if server chooses cryptographically generated name).

# State of the draft

Broad strokes – who talks to whom. Collection of ideas.

Big missing topics:

- Naming – current state assumes something like [draft amsuess-t2trg-rdlink](#), which needs updating
- Announcement of names – as with names
- Announcement of proxies – drawing from Tor

# Advancing Onion CoAP

- Do we lose security properties compared to Tor? Right now: Most certainly. How far can we get while still supporting constrained devices?
- Run as an experiment: 3-4 operators – too few for actual anonymity, enough to gather some experience.
- Is T2TRG a good place for this?