

DoS / Resource Protection Considerations for MoQT

Mike English (Cloudflare)

MoQ WG Boulder Interim
February 2026

BACKGROUND

Motivation

Security Considerations Requirements (BCP 72 / RFC 3552):

- 'Potential denial of service attacks MUST be identified.'
- 'There should be a clear description of the kinds of threats... due diligence in describing all known or foreseeable risks.'

Goal:

More complete coverage of resource exhaustion risks, including risks we've mitigated to prevent regressions.

Current State

Already in the Draft:

Resource Exhaustion section:

- Stream limits and flow control
- MAX STREAM count limits
- Priority starvation guidance

Relay Security Considerations:

- PUBLISH_NAMESPACE / SUBSCRIBE_NAMESPACE flooding
- Short prefix amplification

Missing:

Threat model, rapid request cycles, slow subscribers / join time buffering, flow control limitations, documentation of load-bearing mitigations.

Proposal Summary

To Resource Exhaustion section:

- Threat model (subscriber/publisher/relay profiles)
- Rapid request cycles (Rapid Reset parallel)
- Update coalescing guidance
- Slow subscribers / join time buffering
- Flow control limitations (intra-session vs. cross-session)
- Cost tracking guidance
- Load-bearing mitigations

To Relay Security Considerations:

- Resource isolation
- Upstream load protection (fan-in from downstream sessions)
- Relay topology considerations (ref: [#556](#))

QUESTIONS FOR THE WG

Q1: Direction

Is this direction useful? Should I open a PR?

- Draft text available for review: [Google Doc](#)
- Complements Magnus's PR #1455 (trust model, auth, media security)

Q2: Specificity

How prescriptive should the text be?

Option A: Include suggested numbers

- 'Implementations might consider starting points such as 1000 announcements per connection.'

Option B: Guidance only, no numbers

- 'Implementations **SHOULD** impose limits on announcements accepted per connection.'

Note: Numbers could be deployment-dependent; but concrete starting points may help implementers.

Q3: Load-Bearing Mitigations

Should we document which mechanisms are load-bearing for DoS prevention?

Option A: Yes, keep in final RFC

- Helps implementers understand security relevance (e.g., MAX_REQUEST_ID).

Option B: No, don't include

- Too meta / not appropriate for the spec itself.

Option C: Compromise

- Include now (useful for evaluating PR #1389 tradeoffs), remove before final publication.

Wrap-up

Summary:

- Draft text available: [Google Doc](#)
- Complements Magnus's PR [#1455](#)
- Looking for WG signal on direction

Related Issues:

[#374](#), [#869](#), [#1389](#), [#1404](#), [#1455](#)

Next Steps:

- Open PR with proposed text
- Continue discussion on list / issues
- Adjust approach based on feedback