

CoRE: Corr-Clar

2024-10-23 CoRE Interim 15

Plan: Work on issues via PRs

<https://github.com/core-wg/corrclar/issues?q=is%3Aissue+>

2024-10-14: [draft-ietf-core-corr-clar-00](#)

— 🙄 [core-wg/corrclar/issues/39](#), PR #40:
Source address validation, amplification, 0-RTT

👁️ issues/39: ORTT and other cryptographically unconfirmed situations (DTLS CIDs, OSCORE B.1.2)

Underlying observation: Source addresses (of a request):

- not trustworthy (can be spoofed)
- not stable (may need updates due to renumbering or NAT instability)
→
- operational instability when changing addresses
- DoS opportunities:
 - attacker may try confusing server on request address
 - attacker may want to use amplification via spoofed source

Is this a new problem?

No, essentially all UDP-based protocols have it.
A recent thorough discussion happened in [QUIC](#).

- QUIC defines "anti-amplification [upper] limit" (= 3) to mitigate amplification via source address spoofing

Previous work in CoAP in [RFC 9175](#): [Echo](#) Option

- CoAP-native form of return routability check (RRC)
- Compare secure form [RRC](#) in draft for DTLS (need negotiation)

PR #40: New Section 2.6

Discuss Problem, two subsections:

2.6.1: Amplification mitigation and return routability

- Define "amplification factor" (upper limit) of 3
 - uncertain request address OK wrt amplification
- Opt for Echo option as a default strategy where $af > 3$

2.6.2: Replay protection

2.6.2: Replay protection

Handling address changes may require setting up a new replay window.

DTLS forbids "0-RTT".

OSCORE enables it (need document about "early data").

OK if request is **cheap and safe**.

(**Possibly** OK even if not safe, e.g., due to idempotency.)

Warn: **safety** of a request is an **application concept**.