SeND for 6lo

draft-sarikaya-6lo-cga-nd-02

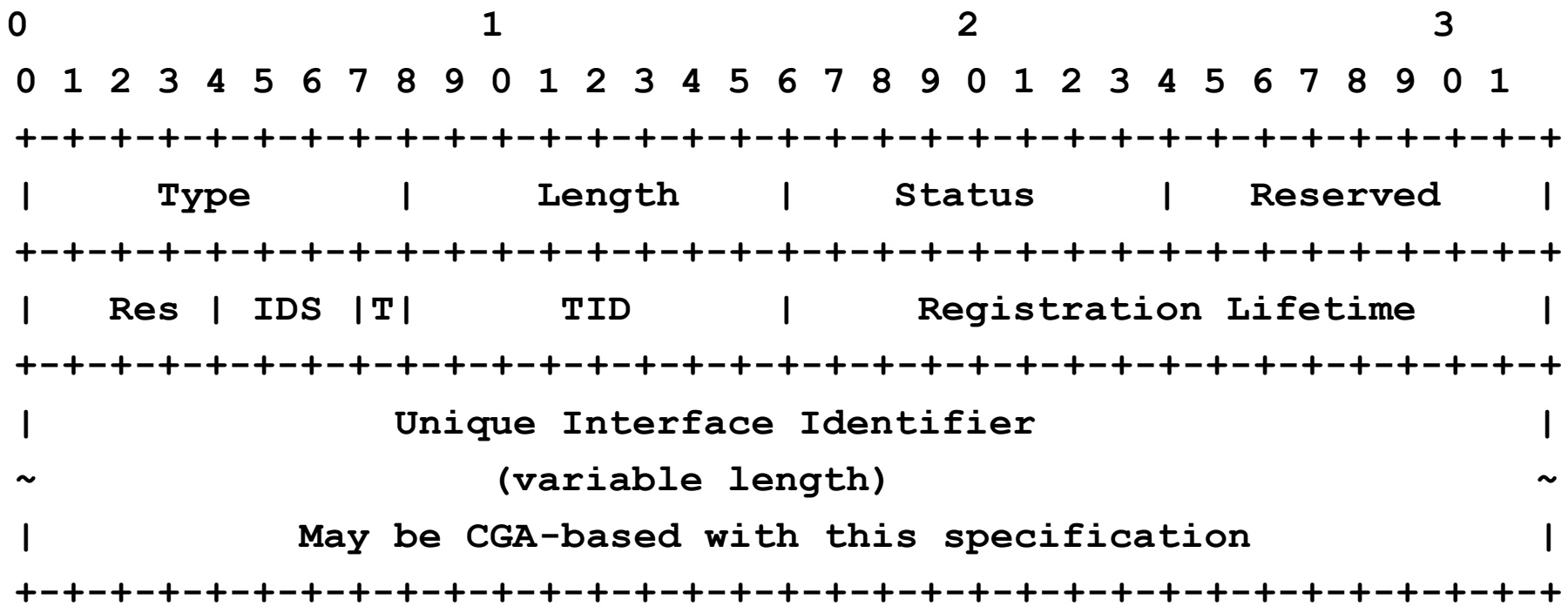
Requirements

- Extend 6LoWPAn ND RFC 6775
  - Extend the Address Registration Option
  - Small packet size and memory footprint
  - Public key and signature size minimized
  - Lightweight signature calculation
- Applicable to all LLN links
  - for which a 6lo "IPv6 over foo" specification exists,
  - as well as Low- Power Wi-Fi.
- Provide a mechanism to compute a unique Identifier
  - Suitable for the formation of a site-local address that follows the security recommendations from [RFC7217].

draft-sarikaya-6lo-cga-nd-02

draft-sarikaya-6lo-cga-nd-02 ARO

- Extends Efficient ND, new *IDS* * for CGA unique IID

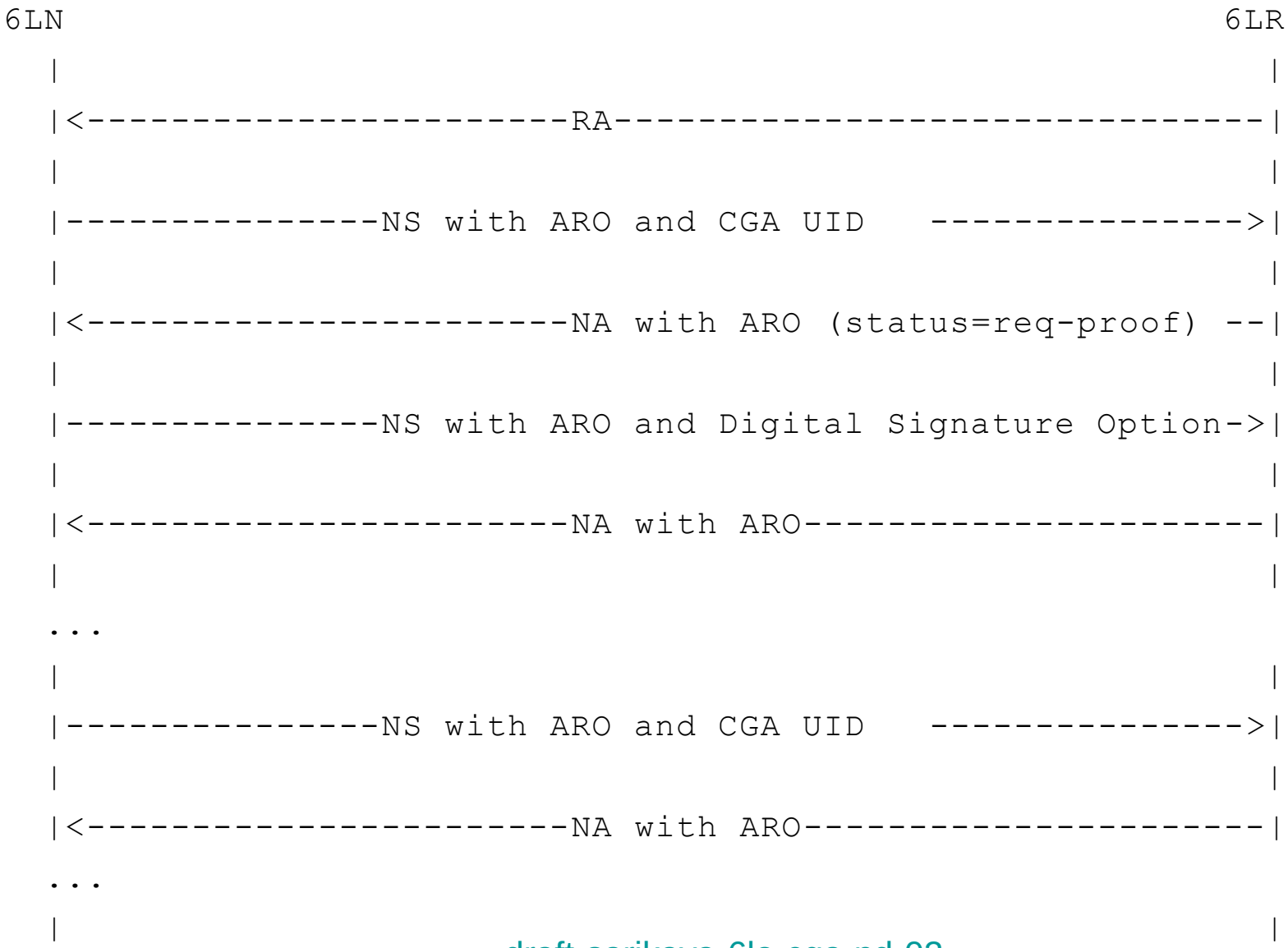


** Identifier Name Space.*

draft-sarikaya-6lo-cga-nd-02

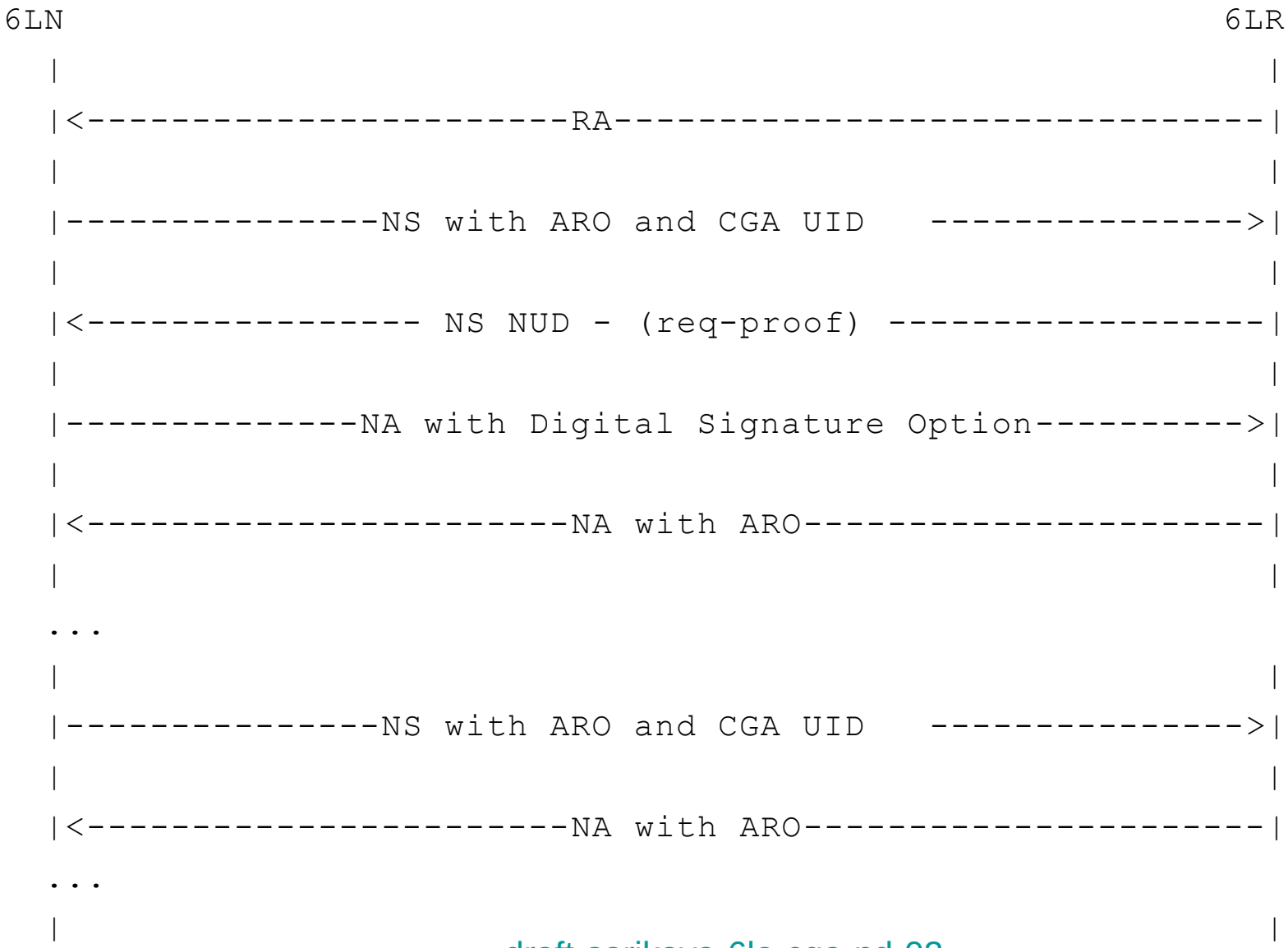
- Use CGA to compute the ARO Unique Interface ID
- Ownership checked by the 6LR at 1st registration
  - And then on demand eventually
- CGA UID stored in 6LR and 6LBR
- 6LR and 6LBR protect ownership
  - CGA parameters between node and 6LR only
  - And only once (Could be avoided per Suresh's proposal)
  - 6LBR trusts 6LR (else need to pass proof to 6LBR)
  - 6LR indicates that CGA proof was performed
  - CGA proof required to allow state update

Possible flow



draft-sarikaya-6lo-cga-nd-02

Alternate flow



draft-sarikaya-6lo-cga-nd-02

Author's Suggestions

- Alternate Flow has better role separation
- Use CGA or MAC for IID to form a link local address
- No DAD for such LLA, can source NS(ARO) with it
- Use any IID to form other IPv6 addresses
- Correlate/prove all addresses with a single CGA UID

- Additionally (controversial?)
  - Use CGA LLA as source to register other addresses
  - But then, register NS target as opposed to the source

draft-sarikaya-6lo-cga-nd-02

Questions to the group

- Flow 1 or flow 2 ?
- Register NS source or target ?
- Recommendation for forming LLA ?

draft-sarikaya-6lo-cga-nd-02

Thank you!