LISP subscription: analysis and discussion

Alberto Rodriguez-Natal
Dino Farinacci

With help from:
Vina Ermagan, Albert Cabellos, Sharon Barkai,
Darrel Lewis, Fabio Maino

About this document

- Summary of ideas/opinions/proposals/options
  - Baked during months of discussion
  - Rough consensus on some points
  - Some issues remain open

- Indented to drive broader discussion within the WG

- When several options to choose from, listed as A, B, C, etc.
- When relevant, includes references to recent draft-boucadair-lisp-subscribe-00

Subscription request

- A: Implicit
  - All Map-Requesters subscribed
- B: Extend Map-Request message
  - One bit per EID-record?
  - One bit in the header?
  - Both?

- draft-boucadair-lisp-subscribe-00
  - New message (Map-Subscribe)

Subscription acknowledgment

- A: No ack at all
- B: Implicit
  - Map-Reply received
- C: Extend Map-Reply
  - Bit(s) per EID-record?
  - Bit(s) in the header?
  - Both?

- Errors
  - A: One bit
    - Successful/Unsuccessful
  - B: Several bits
    - Different error types
    - More than one error at once?

- draft-boucadair-lisp-subscribe-00
  - New message (Map-Subscribe-Ack) with 7 bits for errors

Unsubscribe

- Time-out
  - A: Use mapping TTL
  - B: Subscription specific time-out
    - Signaling?
  - C: Hardcoded time-out
- Requested by subscriber (via Map-Request)
  - A: No bit in header, bits unset in EID records
    - Indistinguishable from legacy messages?
  - B: Bit set in header, bits unset in EID-records

- draft-boucadair-lisp-subscribe-00
  - New message (Map-Subscribe) with expiry time = 0

Announce updates to subscribers

- A: SMR message
  - Pro: Compatible with legacy equipment
  - Con: No security field. Easy to exploit
- B: Map-Notify
  - Pro: Security field. LISP-SEC with two OTK?
  - Con: Requires upgrading the subscribers

- draft-boucadair-lisp-subscribe-00
  - Unsolicited Map-Reply

Identifying subscribers

- A: Map Request's source locator
  - Pro: Suitable for all approaches
  - Con: Subscriber may move
- B: ITR-RLOC field on Map-Request
  - Pro: Already available in RFC6830
  - Con: May not reflect the subscriber's locator
- C: xTR-ID
  - Pro: Unique per subscriber
  - Con: Not present in RFC6830

State at Map Server(s)

- Disable Map-Resolver caching/replying
  - Requests always arrive to Map Server(s)
- State synchronization
  - A: Disable load balancing of Map-Requests
    - ALL requests to ALL Map Servers
  - B: Off-band synchronization mechanism
    - To ensure same state on all Map Servers
- State persistence
  - Time-out based eviction of subscribers
- Map Server going down?

Non-proxy reply

- A: Not allowed

- B: Two Map-Replies to subscriber
  - Subscription acknowledgment from Map-Server
    - Without mapping data (empty locators sets)
  - Mapping data from authoritative ETR

  - Subscribers will receive two Map-Replies with the same nonce
  - Negative Map-Reply indistinguishable from subscription acknowledgment
    - Use ACT field to distinguish?

Mitigation of amplification attacks

- Rate-limit
  - Mapping updates
  - Update notifications to subscribers
- White/black-lists
  - Subscribers
  - Mappings that support subscription
  - Who can update mappings with subscribers

- Only ONE update notification per subscription request
- Only ONE EID-record in the subscription request

Others

- When there is an update of a more specific mapping
  - Subscribers of less specific mappings should be notified as well
- When a subscriber is notified of an update
  - It should verify it through the Mapping System
- When a Map-Register goes to several Map Servers
  - Subscribers may receive multiple notifications for the same mapping update