# LISP RLOC Membership Distribution

draft-kouvelas-lisp-rloc-membership-00

Chris Cassar
Isidor Kouvelas
Johnson Leong
Darrel Lewis
Gregg Schudel

IETF 91

# Motivation – the VPN use case

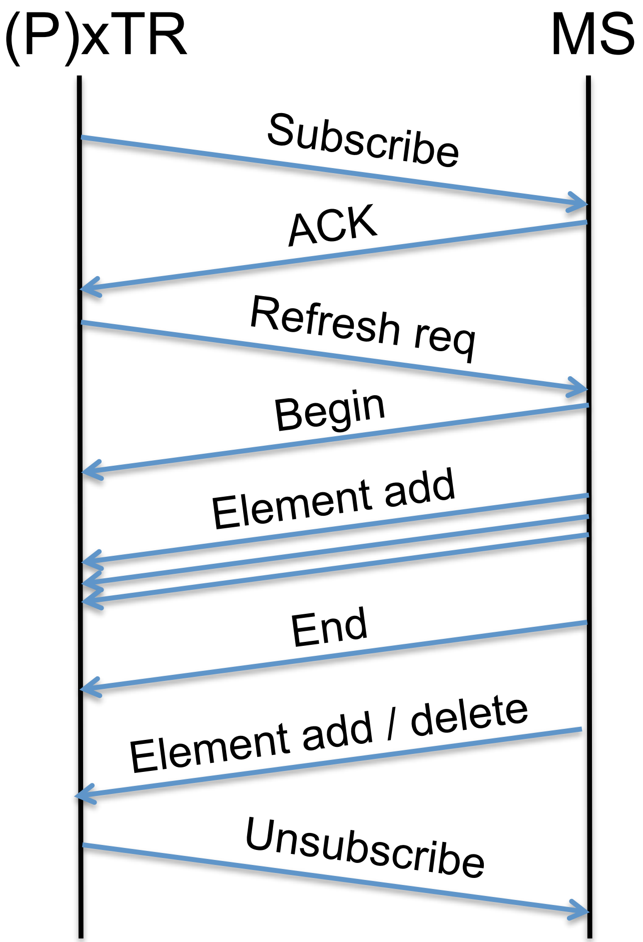
- Sites of a VPN want to prevent data insersion from non-VPN members
- Traditional methods (which work) use encryption to enforce this
- Some networks however have implemented strict uRPF checking on all Locators in their network
- Thus an access control like check on the outer header prior to decapsulation can provide some value
- The key issue then is how to create and maintain this ACL – this is what this draft discusses

# MS RLOC Membership View

- EID prefix registrations to the mapping system include the list of site RLOCs.
- Map-Servers that share authority for a LISP overlay hold between them the complete set of xTR RLOCs participating in the overlay.
- The RLOC membership set gleaned from mapping registrations can be pushed out to the member xTRs (including add/delete updates).
- An xTR can use the RLOC membership to filter decapsulated traffic or trigger map cache updates.

# Membership Distribution

- Separate RLOC membership gleaned and distributed for each EID instance and EID AF.
- Leverages xTR to MS reliable transport session (draft-kouvelas-lisp-reliable-transport)
- New session TLVs to subscribe, request full membership refresh and receive incremental updates.



# Applicability

- Practical in VPN use cases (draft-lewis-lisp-vpns) with limited membership size.
- MS RLOC membership synchronization mechanism needed to support overlays (IIDs) distributed across multiple map-servers.
- Membership gleaning at the map-server assumes symmetric ITR/ETR deployments.
  - Possible extension to allow the registration of RLOCs of (P)ITRs that do not register EID space.