Changes on draft-ietf-lisp-rfc6830bis draft-ietf-lisp-rfc6833bis

IETF 103 Bangkok

November 2018

Scope of Applicability

- Added new section 1.1 for both 6830bis and 6833bis:

> *As such, the design and development of LISP has changed so as to focus on these use cases. The common property of these uses is a large set of* ***cooperating entities seeking to communicate over the public Internet or other large underlay IP infrastructures, while keeping the addressing and topology*** *of the cooperating entities* ***separate from the underlay and Internet topology, routing, and addressing****.*

- Removed the term *global* from both specs

LISP-SEC is Mandatory to Implement

- The LISP Control Plane has the following security assumptions:
  1. The Mapping System is secure and trusted
  2. ETRs have pre-configured trust relationship with the Mapping System
  3. **LISP-SEC MUST be implemented**

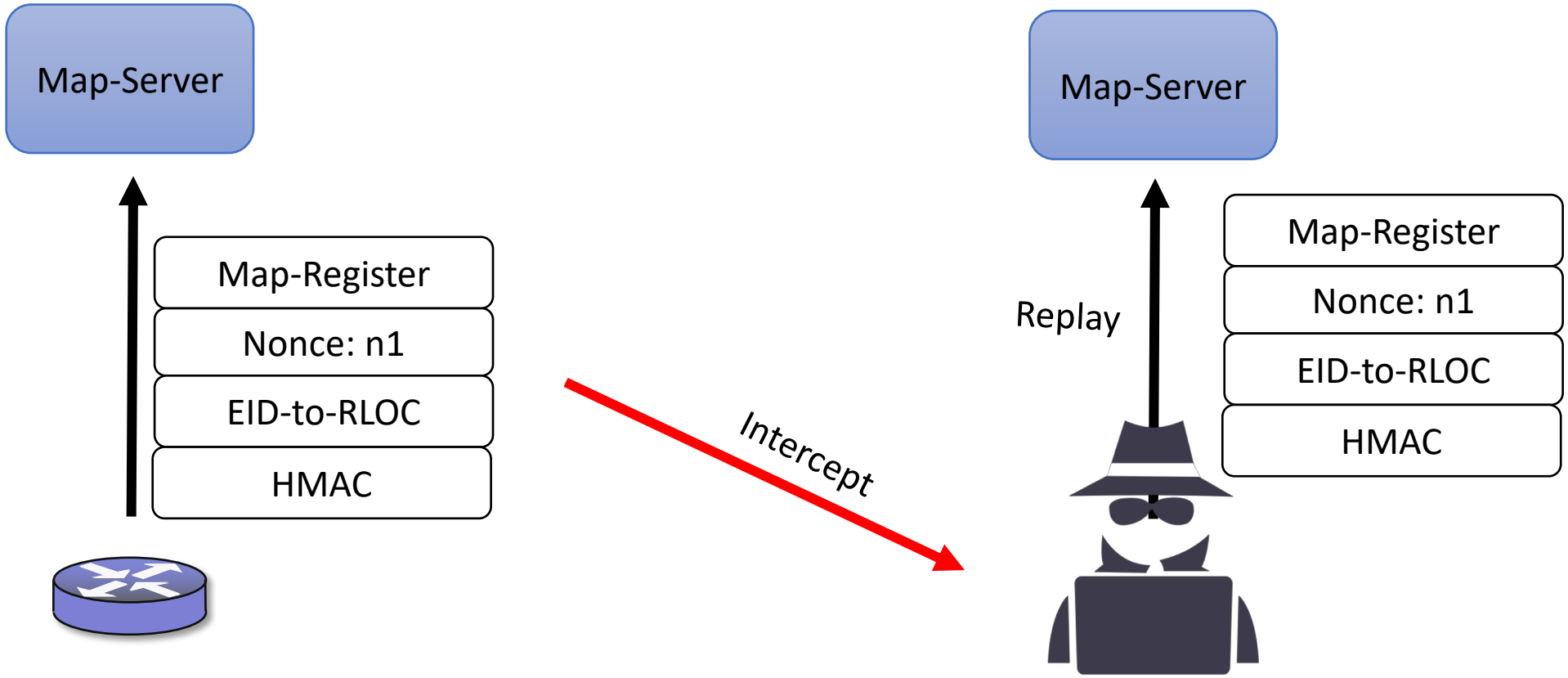
LISP-SEC is Mandatory to Implement

- The LISP Control Plane has the following security assumptions:
  1. The Mapping System is secure and trusted
  2. ETRs have pre-configured trust relationship with the Mapping System
  3. **LISP-SEC MUST be implemented**

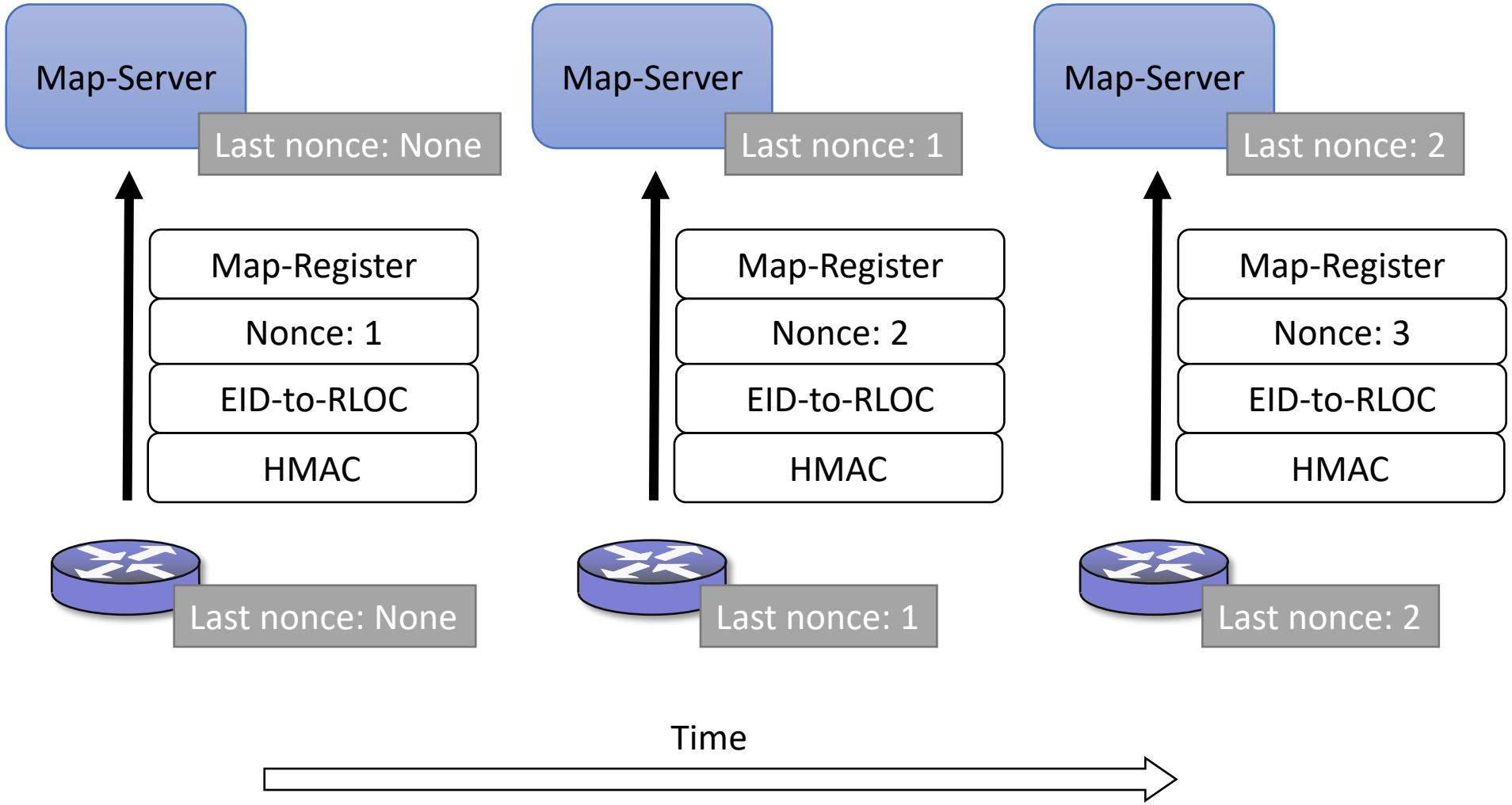
- Deployments concerned about manipulations of Map-Request and Map-Reply messages, and malicious ETR EID prefix overclaiming **MUST drop LISP Control Plane messages that do not contain LISP-SEC material (S-bit, EID-AD, OTK-AD, PKT-AD)**

Not posted yet

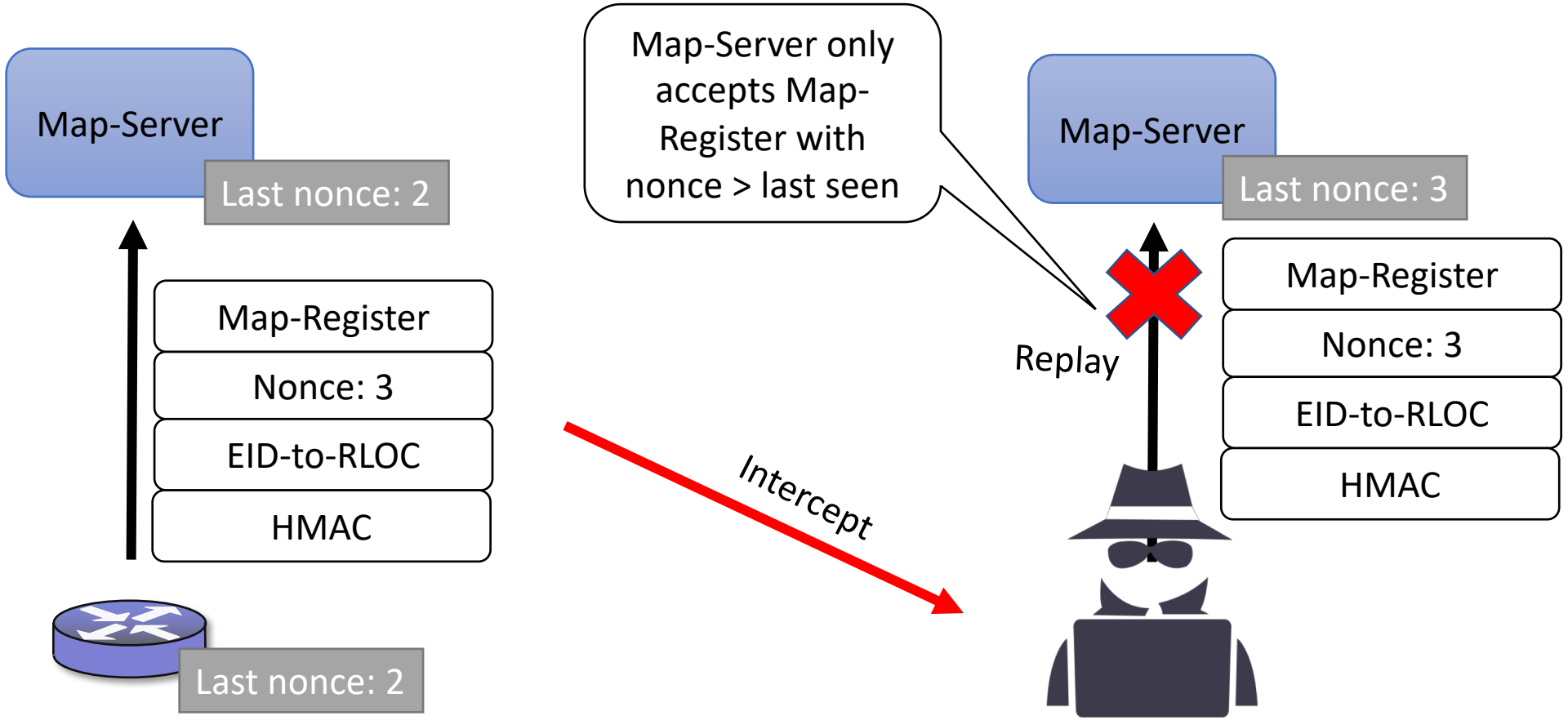
Anti-Replay attack for Map-Register



Anti-Replay protection for Map-Register



Anti-Replay protection for Map-Register



Anti-Replay protection for Map-Register

- Anti-Replay attacks for Map-Register message
  - Nonce is auto-incremented in each Map-Register
  - Nonce is returned in Map-Notify messages
  - ETRs/Map-Server must store in persistent storage the last nonce (indexed by xTR-ID)
  - If state is lost entities need to rekey
  - If Map-Register is received with a nonce <= stored then MS drop-logs message.

UDP and Congestion Control

- Follow guidelines from RFC8085 “*UDP Usage Guidelines*”
- Data-Plane:
  - Congestion Control for LISP Data-Packets
  - UDP Checksum
- Control-Plane
  - Transmission of Map-Request
  - Congestion Control and reliability for unsolicited Map-Notify
  - Rate-limiting of SMRs
  - Maximum size of LISP Control-Plane messages

draft-ietf-lisp-rfc6830bis

- Since IETF102 from -14 to -25
- Current (11/4/18) status

TSVART Telechat Review (of -19): Ready with Nits
SECDIR Telechat Review (of -18): Has Issues
GENART Telechat Review (of -16): Ready with Nits
OPSDIR Last Call Review (of -16): Ready
TSVART Last Call Review (of -15): Ready with Issues
SECDIR Last Call Review (of -15): Has Issues
RTGDIR Last Call Review (of -14): Ready

Overall/Introduction

- Removed the term *global* when referring to EIDs or RLOCs
- Scope of Applicability (see slide 2)
- Reactions to LSB are rate-limited by ETRs

UDP

- Implementors are encouraged to follow RFC8085 “*UDP Usage Guidelines*” on:
  - Congeston control when sending LISP Packets
  - Optional UDP checksum guidelines when it´s desirable to protect the UDP or LISP headers

ETR/PETR Decapsulation

- The inner TTL/Hop-Count MUST (as opposed to SHOULD) be copied from the outer header.
- It is RECOMMENDED that implementations follow RFC6040 “Tunnelling of Explicit Congestion Notification” when dealing with the Explicit Congestion Notification field.
  - Before copied from the outer to the inner header

Security Considerations

- Stated that off-path attackers able to spoof the RLOC and/or nonce can take advantage of LSB, Nonce-Present and Echo-nonce to declare false RLOC reachability information.
- Added a specific example of such attacks:
  - Off-path attacker
  - Sending echo-nonce packets with random nonces
  - Added mitigation techniques (uRPF BCP 38 or specific detection techniques)

Other

- In load-sharing scenarios the source port SHOULD be the same for all the packets of the same flow
- Minor edits

draft-ietf-lisp-rfc6833bis

- Since IETF102 from -10 to -21
- Current (11/4/18) status

GENART Telechat Review (of -15): Ready
GENART Last Call Review (of -13): Ready with Nits
TSVART Last Call Review (of -13): On the Right Track
RTGDIR Last Call Review (of -13): Ready
SECDIR Last Call Review (of -12): Ready
OPSDIR Last Call Review - due: 2018-08-31

Overall/Introduction

- Removed the term *global*
  - Example: Mappings are propagated across the mapping system (not globally)
- Added Scope of Applicability (verbatim from 6830bis, see slide 2)
- Recommend to follow the guidelines of RFC8085 “UDP Usage Guidelines” regarding the maximum size of LISP Control Plane messages.

Congestion Control

- Map-Request SHOULD be transmitted following the recommendations from RFC8085 “UDP Usage Guidelines”
- Unsoliticed Map-Notify follows Congestion Control and Reliability guidelines specified in RFC8085
- Specified retransmissions and timeouts for (solicited) Map-Notify messages
- SMRs are rate-limited according to the procedures of RFC8085

Nonce

- Anti-Replay attacks for Map-Register message
  - Nonce is auto-incremented in each Map-Register
  - Nonce is returned in Map-Notify messages
  - ETRs/Map-Server must store in persistent storage the last nonce (indexed by xTR-ID)
  - If state is lost entities need to rekey
  - If Map-Register is received with a nonce <= stored then MS drop-logs message.
- Specify that the nonce is a 64-bit value
- Stated that the nonce MUST (as opposed to SHOULD) be generated by a proper random source

xTR-ID

- Specified that in Map-Register message when the I-bit is set:
  - xTR-ID field 128-bit uniquely identifies the xTR
  - Site-ID 64-bit uniquely identifies the site where the xTR is attached
- We need to specify xTR-ID/SiteID in 6833bis to index the nonce for anti-replay protection

Security Considerations

- Considering the Scope of Applicability, the following assumptions hold:
  1. The Mapping System is secure and trusted
  2. ETRs have pre-configured trust relationship with the Mapping System
  3. LISP-SEC MUST be implemented
- Stated DoS and amplification attacks that can be done exploiting the Map-Request/Map-Reply message exchange
- How LISP-SEC provides origin authentication, integrity, anti-replay protection, and prevention of 'man-in-the-middle' and 'prefix overclaiming' attacks for Map-Request/Map-Reply message exchange.
- ETRs can overclaim the EID-prefix it owns

Privacy Considerations

- Privacy in LISP depends greatly on the specific deployment and use-case
- LISP uses long-lived identifiers that bind to the topological location of the node
- This information is publicly accessible via Map-Request
- Deployments concerned about this should use:
  - ACL or authentication mechanisms to control who has access to mapping information
  - Use ephemeral EIDs

Other

- Simplified Abstract
- Stated that LISP Control Plane Message type 7 is ”Not Assigned”. Not assigned values can be assigned following RFC8126 procedures.
- Added captions to figures of IPv4/IPv6 UDP LISP Control Messages
- Bits “m” (LISP-MN bit) and “I” (xTR-ID bit) are now reserved in Map-Request
- Bit “m” (LISP-MN bit) is now reserved in Map-Register
- Stated that RLOC-probe Map-Request MUST not be sent to the Mapping System
- Several instances of MAY to may (editorial)
- Examples using IPv6 addresses
- Specified that several fields of Map-Register, Map-Notify and Map-Notify-Ack are “dual-use”
- Minor edits