Network Working Group
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

L. Ramanathan
R. Kovacina
M. Portoles
Cisco Systems

20 October 2025

SAVI in a LISP network
draft-ramanathan-lisp-savi-01

Abstract

This document specifies the procedures for Source Address Validation of LISP Endpoint Identifiers (EID). The implementation of these mechanisms provides endpoint detection, on-boarding and roaming support in LISP networks, while protecting against IP address spoofing.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 April 2026.

Copyright Notice

Table of Contents

1. Introduction

The LISP protocol [RFC9300] defines two numbering spaces, Endpoint Identifiers (EIDs) and Routing Locators (RLOCs) supporting an architecture to build network overlays. Mapping EIDs to RLOC-sets is accomplished with a Mapping Database System and the LISP control-plane [RFC9301] specifies procedures to learn and distribute these Mappings. Once EIDs are learned and on-boarded on a LISP network, the LISP architecture is flexible to extend subnets and routing domains with mobility and traffic optimization [I-D.ietf-lisp-eid-mobility].

With increased mobility support requirements and when operating LISP networks at scale, it becomes even more important to offer source address verification of EIDs and protect the system and endpoints against spoofing and duplication. This support needs to work across mobility events and routing domains.

To this end, Source Address Validation Improvements (SAVI) procedures have been specified to provide a set of mechanisms and state machines to verify Source Address ownership [RFC7039]. A SAVI instance enforces the EIDs to use legitimate IP source address and also verify the source address used in data packet actually belong to the originator of the packet.

This document describes the use of SAVI procedures to provide source address protection for IP addresses (both IPv4 and IPv6) in LISP networks. To perform Source Address Validation in a LISP network, the SAVI function is integrated with the LISP xTR. Only those EIDs validated by the SAVI instance will be detected and on-boarded by LISP, thereby protecting the integrity of EIDs distributed in the network. This integrated function does not require changes to the endpoint protocol stack.

2. SAVI LISP Architecture

Source Address Validation Improvement (SAVI) features are embedded into the LISP xTRs referenced as SAVI xTR. The SAVI xTR follows the mechanisms mentioned in [RFC7039] to perform source address validation of IP addresses used as EIDs. A SAVI instance monitors packets exchanged by endpoints and identify which IP source addresses are legitimate. SAVI creates a binding entry where the IP address (the EID) is bound to an immutable binding anchor. The binding entries have a state and lifetime which determines if the IP is valid and for how long. Once the EIDs are validated, they are treated as detected by a LISP xTR, added to the local Mapping Database and registered with the Mapping System.

2.1. SAVI Perimeter in LISP Network

The essential elements in a SAVI LISP deployment include one or more SAVI xTRs which belong to the RLOC space, endpoints which belong to the EID space and a LISP Mapping System which holds the EID to RLOC mappings. SAVI xTRs form a SAVI perimeter separating trusted and untrusted regions of a network. As specified in [RFC6620] and [RFC7513], only validated addresses can inject traffic over the trusted perimeter. This implies only SAVI validated endpoints can join the LISP network.

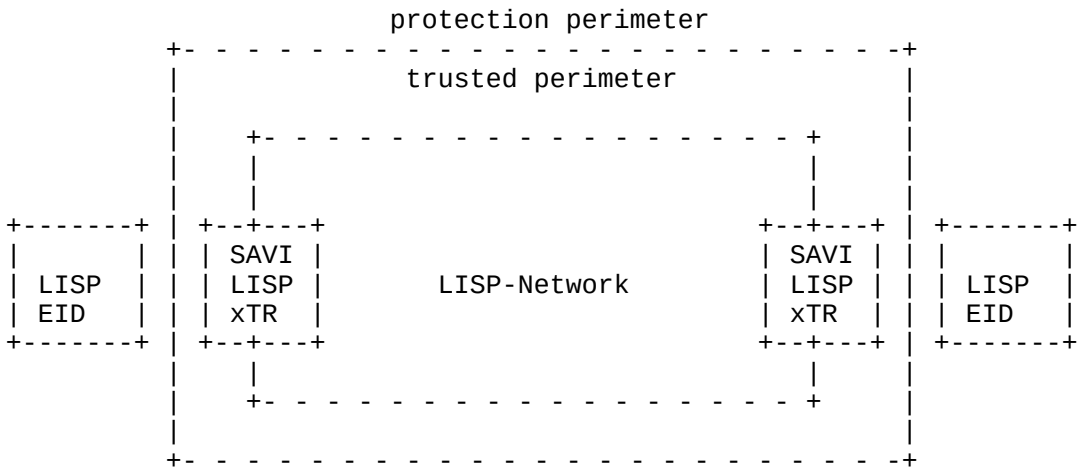

Figure 1: SAVI LISP perimeter

2.2. Binding Address

SAVI mainly follows packet exchanges used for address assignment to learn the source IP address of a host. As a consequence, the SAVI specification comes in multiple variants depending on the exchange used for address assignment. [RFC7513], describes a mechanism that provides Source Address Validation Improvements (SAVI) for addresses assigned by DHCPv6 or DHCPv4 server. [RFC6620] is another specification based on First Come First Serve (FCFS) principle, applicable to any IPv6 address including those assigned through IPv6 Neighbor Discovery and Stateless Address Autoconfiguration (SLAAC). While [RFC6620], does not explicitly mention IPv4, a very similar approach can be applied to IPv4 addresses when using ARP packets to learn and track a source address.

Following the above SAVI specifications, IP address can be validated by the SAVI instance on the SAVI xTR, and on-boarded as EIDs in the LISP network.

2.3. Binding Anchor

The SAVI instance creates a binding between the IP address and a binding anchor. As discussed in [RFC7039], a binding anchor is a physical or link layer property of an attached device. In SAVI LISP deployments, the Media Access Control (MAC) address is used as the binding anchor.

As a result, in a SAVI LISP environment, the IP address used as an EID is bound to a binding anchor which is the MAC address of the endpoint. This is referred as the binding entry present in the SAVI database.

2.4. Binding State

Following [RFC6620], every binding goes through multiple states before it reaches the "VALID" state. The binding entry in state "NO_BIND" or "TENTATIVE" are considered not validated by SAVI yet. When an IP is in one of these states, SAVI xTR does not detect it as an EID. An IP binding entry to moves to state VALID is on-boarded as an EID LISP Mapping Database.

If the binding entry moves from VALID state to the "TESTING_TP_LT" state, it remains as a detected EID in the LISP Mapping Database, while the state gets resolved. If the resolution leads the IP to NO_BIND state, the EID is removed from the LISP Mapping Database. On the contrary, if the TESTING_TP_LT state resolves to VALID state, the EID remains in the LISP Mapping Database.

A similar mechanism applies when using a DHCP based SAVI instance. In this case instead of "VALID", the host has to reach the "BOUND" state to be considered validated and on-boarded as an EID in the LISP Mapping Database.

For completeness, note also that during the IP validation process, the ARP Address Conflict Detection (ARP ACD) is used for an IPv4 address and the Duplicate Address Detection Neighbor Solicitation (DAD NS) message is used for IPv6 address.

3. Operation of SAVI in a LISP Network

3.1. IP Discovery

This section describes the endpoint discovery process in a SAVI xTR. The packet flow diagram in Figure 2 illustrates the sequence to validate and on-board the IP address of Host1 (IP1 in the figure) as an EID on the LISP network. Host1 uses MAC1 as its MAC address.

1. Data sourced with IP1 is received on the SAVI xTR. The SAVI instance snoops the packet and learns about IP1.

2. A Binding entry for Host1 is created with IP1 in NO_BIND state.

3. IP1 is bound to binding anchor MAC1. SAVI xTR generates a Map-Request querying the Mapping System about IP1 and moves the entry to TENTATIVE state. It starts a timer TENT_LT.

4. When the Mapping System does not have any registration for IP1, it sends a Negative Map-reply back to the SAVI xTR.

5. When the NMR is received with Action "Native Forward", the SAVI xTR broadcasts an ARP ACD/DAD NS to the rest of SAVI xTRs and starts the TENT_TL timer.

6. As the timer expires, this confirms the SAVI instance that IP1 is legitimate and is not present anywhere else in the LISP network.

7. The binding entry moves to VALID state and the SAVI instance starts a timer DEFAULT_LT

8. LISP on-boards IP1 as an EID and adds it to the local Database Mapping table on the xTR

9. The xTR sends a Map-Register with the Mapping <EID: IP1> -> <xTR RLOC> that is stored in the Mapping System.

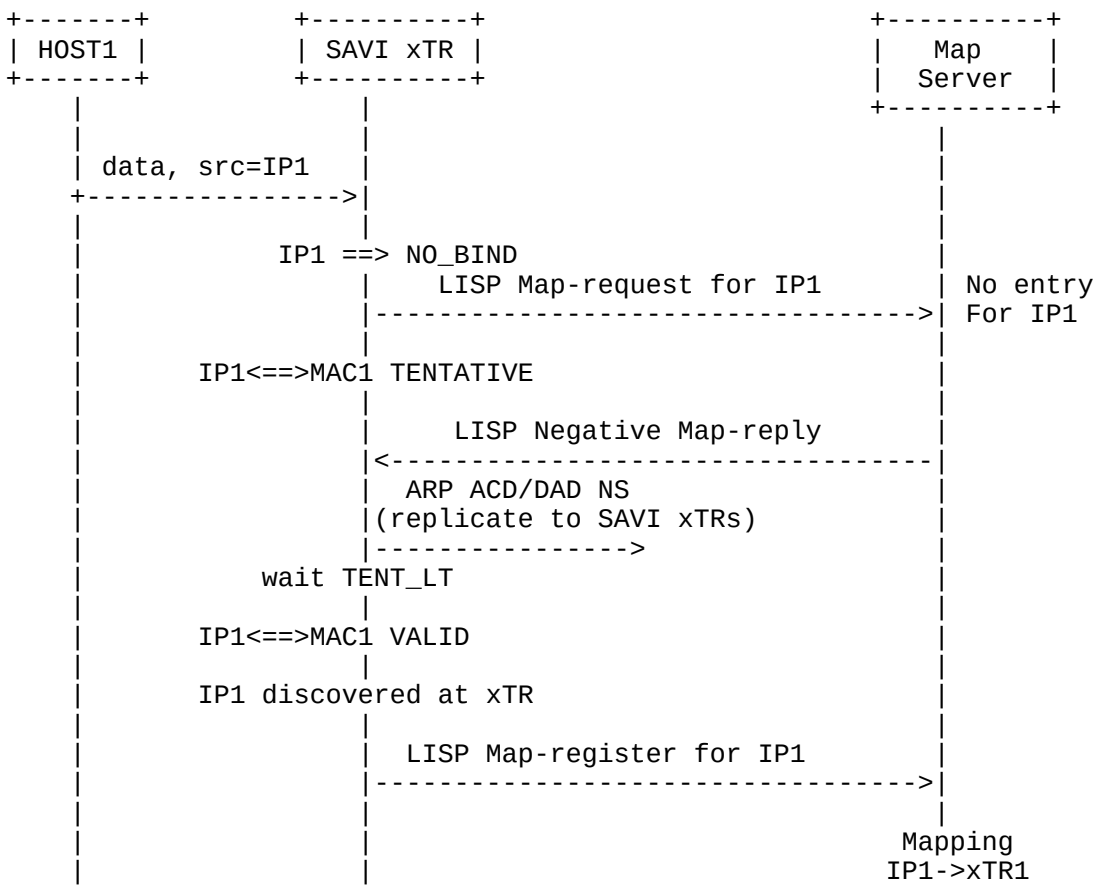

Figure 2: IP Discovery Flow

After host discovery, the SAVI binding entry is in VALID state and has a lifetime DEFAULT_LT. When the timer expires, the SAVI will probe the host to check for reachability. At any time, if Host1 leaves the network the reachability check fails and the binding entry will be removed from the database. Same applies if the binding entry is cleared for any reason.

The next sections discuss the case when the EID is already present in the LISP Mapping Database, and the Map-Resolution process initiated by the SAVI xTR resolves with a complete Mapping. In this case, there are two possible cases: the endpoint roamed to a new location or there is an attempt to spoof the IP address.

In instances where the LISP Network does no support silent EIDs and ARP/ND flooding suppression is possible, the onboarding of new EID can be sped up and optimized by suppressing the ACD/DAD packet broadcasted to all SAVI xTRs. In this case the Mapping System replies to the Map-Request with a Negative Map-Reply and Action Drop. This tells the SAVI xTR that the flooding of ACD/DAD is not required and it can proceed to onboard the EID.

3.2. Host Roaming and Duplicate Address Detection

Every IP address validated with SAVI is on-boarded in the LISP Database Mapping, at the xTR, and registered with the LISP Mapping System. At any point of time, the LISP Mapping System will have a registration for every IP validated in the SAVI LISP Network. To complete the interaction between SAVI and LISP, this section considers the behavior of the system when:

* An endpoint roams from a SAVI xTR to a new SAVI xTR.

* A rogue endpoint connected to a different SAVI xTR attempts to spoof an IP address already assigned to another endpoint.

3.2.1. Host Roaming

The packet flow in Figure 3 illustrates an example where a host (host1) initially connected to SAVI xTR1 roams to SAVI xTR2. The SAVI xTRs gather information from the LISP Mapping System to coordinate the old and new SAVI agents and support the roaming function. In this case the sequence works as follows:

1. Host1 is initially connected to SAVI xTR1. The IP1-MAC1 binding is considered VALID and IP1 is on-boarded as an EID in the LISP network. The Map-Server has a registration for the Mapping: <EID: IP1> -> <xTR1 RLOC>

2. Host1 roams to SAVI xTR2. When SAVI xTR2 sees data-traffic sourced with IP1, it creates a new entry for IP1 in NO_BIND state.

3. IP1 is bound to binding anchor MAC1. SAVI xTR2 sends a Map-Request for IP1 to the Mapping System. IP1 is moved to TENTATIVE state pending resolution. It starts a timer TENT_LT.

4. A Mapping exists in the Mapping System, so SAVI xTR2 receives a Map-Reply with the Mapping <EID: IP1> -> <xTR1 RLOC>

5. The IP1-MAC1 binding entry at SAVI xTR2 is moved to TESTING_TP_LT.

6. SAVI xTR2 sends ARP ACD/DAD NS request to the SAVI xTR1 using the RLOC address received in Map-Reply.

7. After receiving the message, SAVI xTR1 moves IP1 to TESTING_TP_LT state and starts a timer for TENT_LT.

8. Since the end point roamed there is no response and TENT_LT expires. SAVI xTR1 removes the binding entry for IP1-MAC1.

9. The binding entry for IP1 at SAVI xTR2 is moved to VALID state and added to the LISP Mapping Database.

10. A new Map-Register is finally sent to the Mapping System with the Mapping: <EID: IP1> -> <xTR2 RLOC>. This completes the protected roam process.

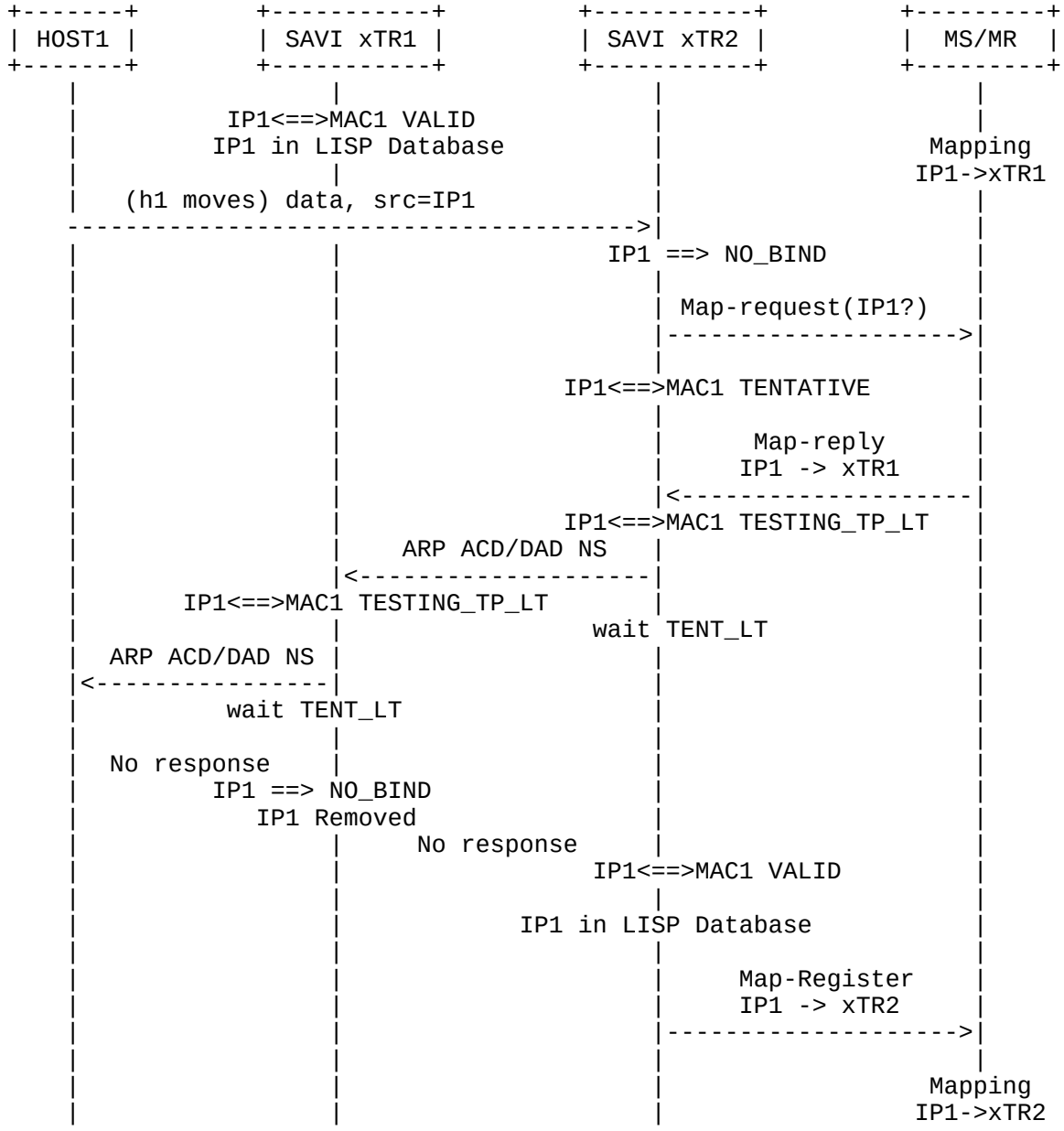

Figure 3: Host Roaming Flow

3.2.2. IP Theft Prevention

Alternatively, the packet flow in Figure 4 illustrates an example sequence where a misbehaving EID attempts to spoof IP1. The SAVI xTR gathers information from the LISP Mapping System to learn that IP1 is already assigned to another EID and blocks the spoofed IP address. The SAVI-LISP sequence to block spoofed addresses proceeds as follows:

1. Host1 is connected to SAVI xTR1. The IP1-MAC1 binding is considered VALID and IP1 is on-boarded as an EID in the LISP network. The Map-Server has a registration for the Mapping: <EID: IP1> -> <xTR1 RLOC>

2. SAVI xTR2 sees traffic activity from a misbehaving endpoint attempting to use IP1. It creates a new entry for IP1 in NO_BIND state.

3. SAVI xTR2 sends a Map-Request for IP1 to the Mapping System. IP1 is moved to TENTATIVE state pending resolution. It starts a timer TENT_LT.

4. A Mapping exists in the Mapping System, so SAVI xTR2 receives a Map-Reply with the Mapping <EID: IP1> -> <xTR1 RLOC>

5. The IP1-MAC1 binding entry at SAVI xTR2 is moved to TESTING_TP_LT.

6. SAVI xTR2 sends ARP ACD/DAD NS request to the SAVI xTR1 using the RLOC address received in Map-Reply.

7. After receiving the message, SAVI xTR1 moves IP1 to TESTING_TP_LT state and starts a timer TENT_LT.

8. Since the Host1 with IP1 is active behind SAVI xTR1, a response is received at SAVI xTR1 and the binding entry moves back to VALID state.

9. xTR1 sends the response to xTR2. This confirms that IP1 is hosted at SAVI xTR1 and reachable.

10. SAVI xTR2 removes the binding entry for IP1-MAC1, thereby blocking the endpoint and preventing IP theft.

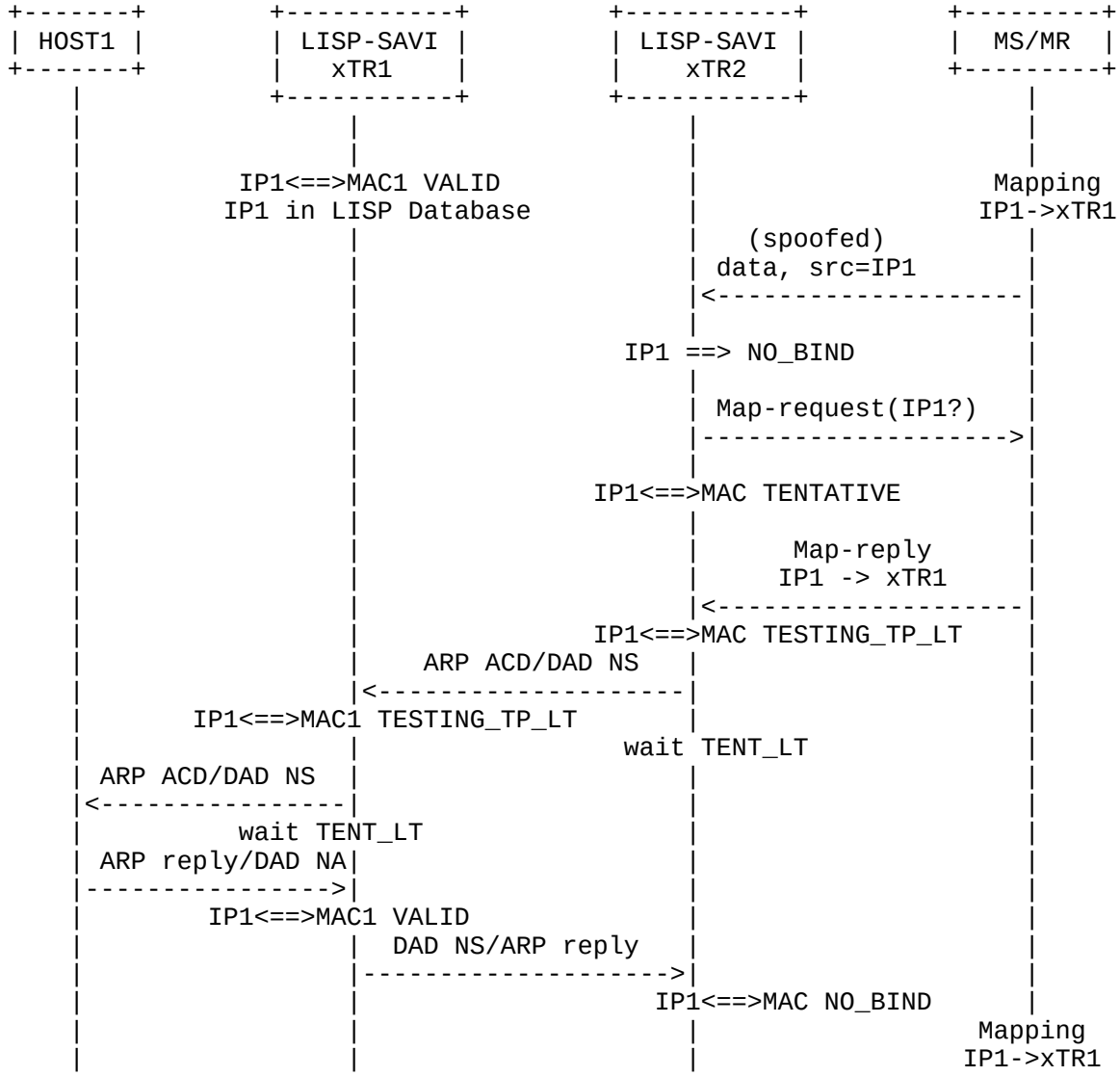

Figure 4: IP Theft Prevention

3.2.3. Fast Detection

This section describes a scenario where there is need for fast detection. The EID is on-boarded before considered valid by SAVI and the validation is done after on-boarding. The following example describes the sequence for fast detection in a SAVI-LISP environment.

1. Host1 is connected to SAVI xTR1. The IP1-MAC1 binding is considered VALID and IP1 is on-boarded as an EID in the LISP network. The Map-Server has a registration for the Mapping: <EID: IP1> -> <xTR1 RLOC>

2. Host1 roams to SAVI xTR2. When SAVI xTR2 sees data-traffic sourced with IP1, it creates a new entry for IP1 (and MAC1).

3. SAVI xTR2 sends a Map-Request for IP1 to the Mapping System and moves the entry to TENTATIVE state and starts timer TENT_LT

4. When fast detection is enabled, the IP1 is on-boarded as an EID at SAVI xTR2 even though it has not moved to VALID state yet. SAVI xTR2 sends a Map-Register for IP1. It is important to note that SAVI does not allow any control traffic from the host until it is validated.

5. SAVI xTR2 receives a Map-reply with the RLOC of SAVI xTR1 and sends ARP ACD/DAD NS request to SAVI xTR1.

6. On receiving this request, SAVI xTR1 moves the entry TESTING_TP_LT and starts a timer TENT_LT.

7. If a response is received, then binding entry at SAVI xTR1 moves back to VALID state and entry at SAVI xTR2 is removed, since this might be a host trying to spoof the IP address which is prevented now.

8. When no response is received, the binding entry at SAVI xTR1 is removed and the entry at SAVI xTR2 moves to VALID state.

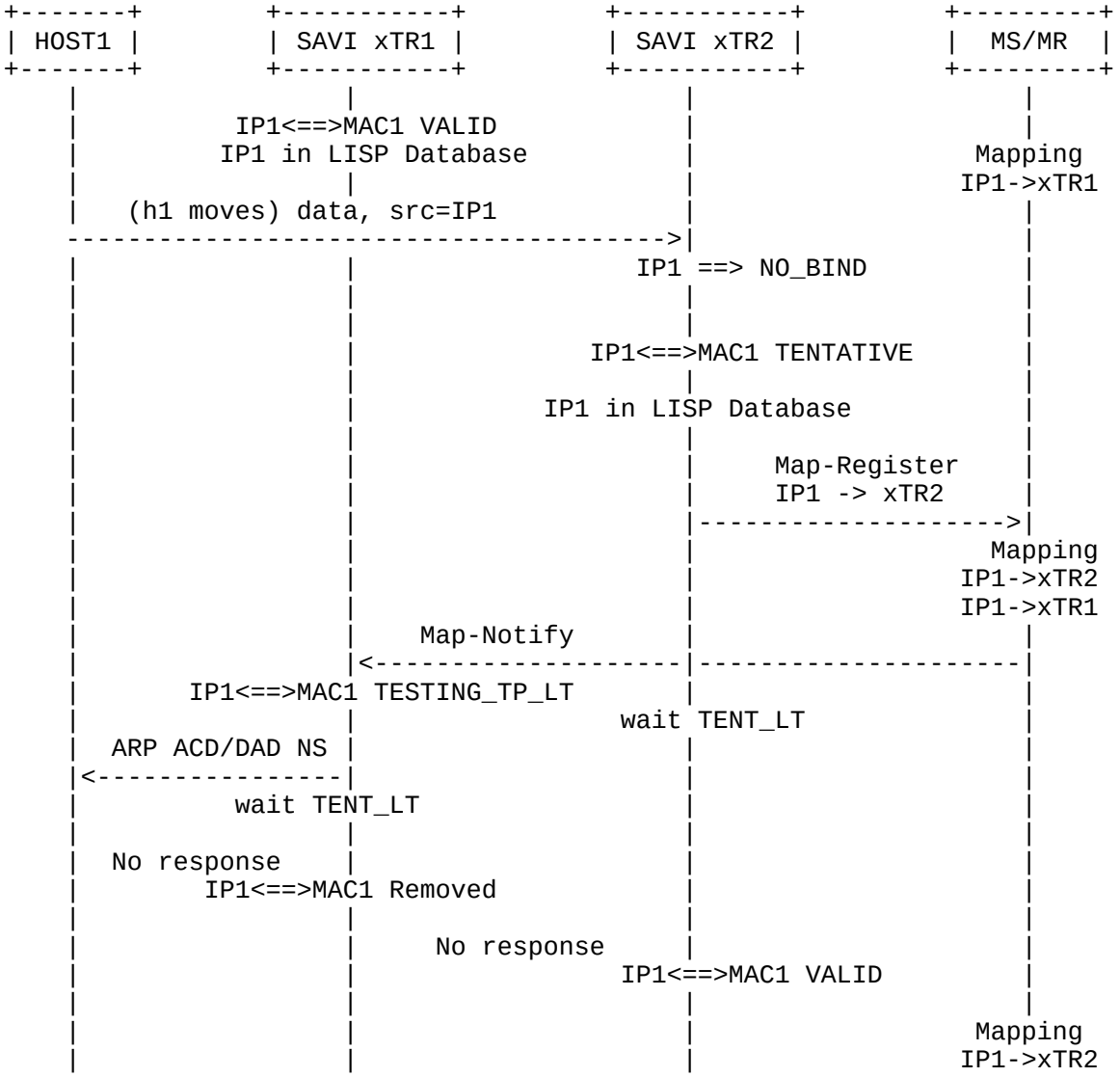

Figure 5: Fast detection

4. SAVI LISP and L2/L3 EID mobility models

The LISP control-plane offers the flexibility to support multiple overlay flavours. In particular [I-D.ietf-lisp-eid-mobility] describes mechanisms to support unified L2 and L3 overlays with mobility support. This section describes implementations options of the SAVI LISP function when different L2 and L3 EID mobility options are used.

4.1. L2-only overlay

In this case, intrasubnet traffic is encapsulated using the L2 overlay. EID detection and mobility with SAVI follows the mechanisms described in Section 3 When a SAVI xTR attempts to discover the location of an IP address and run the ARP ACD/DAD NS exchange, it uses the MAC location. The SAVI xTR resolves the location of the IP using an iterative Map-Resolution process (as described in [I-D.ietf-lisp-eid-mobility]):

* First it resolves the IP-MAC binding (following the ARP/ND resolution procedure)

* Second it resolves the MAC-RLOC binding to discover the candidate location of the endpoint and start the ARP ACD/DAD NS exchange.

4.2. L2 and L3 unified overlay

This model is a co-existence of both L2 and L3 overlay and follows the same interative sequence as the L2-only overlay described above.

4.3. L3-only overlay

In this case both intrasubnet and inter-subnet traffic are forwarded using the L3 overlay. IP detection and on-boarding using SAVI follows the sequence described in this document. In this case, the SAVI xTR resolves the candidate location of the IP endpoint using by resolving the IP-RLOC Mapping directly. The SAVI ARP ACD/DAD NS exchange is done using the RLOC resolved through IP Map-Resolution.

5. Considerations with Ephemeral EIDs

[I-D.ietf-lisp-eid-anonymity] describes the use of ephemeral EIDs to provide source anonymity for endpoints. Ephemeral EIDs are temporary, randomly-generated IP addresses that can change frequently. The integration of SAVI with LISP provides critical source address validation for ephemeral EIDs, ensuring that even short-lived addresses are properly authenticated before being on-boarded to the LISP network.

A key challenge with ephemeral EIDs is the risk of address collision when multiple endpoints independently generate random addresses. Through the procedures described in this document to protect against address duplication (see Section 3.1), SAVI xTRs can detect and validate ephemeral EIDs. This inherently provides source address validation and protection against spoofing attempts and ensures that the anonymity benefits of ephemeral EIDs are maintained without compromising network security or address integrity.

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6620] Nordmark, E., Bagnulo, M., and E. Levy-Abegnoli, "FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses", RFC 6620, DOI 10.17487/RFC6620, May 2012, <https://www.rfc-editor.org/info/rfc6620>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <https://www.rfc-editor.org/info/rfc7039>.

[RFC7513] Bi, J., Wu, J., Yao, G., and F. Baker, "Source Address Validation Improvement (SAVI) Solution for DHCP", RFC 7513, DOI 10.17487/RFC7513, May 2015, <https://www.rfc-editor.org/info/rfc7513>.

[RFC9300] Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", RFC 9300, DOI 10.17487/RFC9300, October 2022, <https://www.rfc-editor.org/info/rfc9300>.

[RFC9301] Farinacci, D., Maino, F., Fuller, V., and A. Cabellos, Ed., "Locator/ID Separation Protocol (LISP) Control Plane", RFC 9301, DOI 10.17487/RFC9301, October 2022, <https://www.rfc-editor.org/info/rfc9301>.

[I-D.ietf-lisp-eid-mobility]
Portoles-Comeras, M., Ashtaputre, V., Maino, F., Moreno, V., and D. Farinacci, "LISP L2/L3 EID Mobility Using a Unified Control Plane", Work in Progress, Internet-Draft, draft-ietf-lisp-eid-mobility-16, 8 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-eid-mobility-16>.

[I-D.ietf-lisp-eid-anonymity]
Farinacci, D., Pillay-Esnault, P., and W. Haddad, "LISP EID Anonymity", Work in Progress, Internet-Draft, draft-ietf-lisp-eid-anonymity-17, 19 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-eid-anonymity-17>.

7. Informative References

Authors' Addresses

Lakshmi Ramanathan
Cisco Systems
2000 Innovation Dr
Kanata, ON K2K 3E8
Canada
Email: laramana@cisco.com

Ratko Kovacina
Cisco Systems
2000 Innovation Dr
Kanata, ON K2K 3E8
Canada
Email: rkovacin@cisco.com

Marc Portoles Comeras
Cisco Systems
170 Tasman Drive
San Jose, CA 95134
United States of America
Email: mportole@cisco.com