LISP Working Group
Internet-Draft
Updates: 6830 (if approved)
Intended status: Experimental
Expires: March 30, 2018

A. Rodriguez-Natal
Cisco Systems
A. Cabellos-Aparicio
Technical University of Catalonia
V. Ermagan
F. Maino
Cisco Systems
S. Barkai
Fermi Serverless

September 26, 2017

MS-originated SMRs
draft-rodrigueznatal-lisp-ms-smr-04

Abstract

This document extends [RFC6830] to allow Map Servers to send SMR messages.

This extension is intended to be used in some SDN deployments that use LISP as a southbound protocol with (P)ITRs that are compliant with [RFC6830]. In this use-case mapping updates do not come from ETRs, but rather from a centralized controller that pushes the updates directly to the Mapping System. In such deployments, Map Servers will benefit from having a mechanism to inform directly (P)ITRs about updates in the mappings they are serving.

Table of Contents

1. Introduction

The Locator/ID Separation Protocol (LISP) [RFC6830] splits current IP addresses in two different namespaces, Endpoint Identifiers (EIDs) and Routing Locators (RLOCs). LISP uses a map-and-encap approach that relies in two entities, the Mapping System and the Tunnel Routers. The Tunnel Routers are deployed at LISP sites edge points and perform encapsulation and decapsulation of LISP data packets. The Mapping System is a distributed database that stores and disseminates EID-RLOC bindings across different Map-Servers. LISP Tunnel Routers keep a cache of EID-RLOC mappings pulled from the Mapping System.

There are several ways to keep this cache updated as described in [RFC6830]. Among them, the Solicit Map-Request (SMR) message allows to explicitly signal (P)ITRs to let them know that some of their cached mappings may be outdated. However, vanilla LISP as described in [RFC6830] only considers SMR messages to be sent by an ETR. This document extends [RFC6830] to cover the case where SMRs can be sent also by a Map Server (MS).

This document introduces changes in the MS specification allowing them to send SMR messages, however it does not require any modification in the (P)ITRs. This document is backwards compatible and enables upgraded MS to interoperate via SMRs with legacy (P)ITRs that only implement [RFC6830].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Map Server extension

This document enables MS to generate and send SMR messages towards (P)ITRs. SMRs originated in a MS follow the same format described in [RFC6830]. Besides the fact that they are sent from a MS, there is no difference between an SMR originated in an ETR and one originated in a MS.

When a MS generates an SMR, it uses as source-EID the EID-prefix it wants the (P)ITR to send the SMR-invoked Map-Request for. The EID included in the EID-record field is the one belonging to the (P)ITR the MS sends the SMR towards. As source locator for the SMR message, the MS uses one of its available locators. This has implications in the processing of the SMR at the (P)ITR as described in Section 4

When the MS has to send an SMR is implementation specific. However, as specified in [RFC6830] and noted in Section 7, SMRs MUST be rate-limited. It must be noted as well that, as described in Section 3, a MS that sends an SMR may not receive the SMR-invoked Map-Request that the (P)ITR generates as response to the SMR.

3. Interoperability with legacy (P)ITRs

This document introduces no changes in the specification of (P)ITRs and thus it is backwards compatible with legacy equipment only compliant with [RFC6830]. However, since SMRs were designed to be sent by ETRs, and legacy (P)ITRs expect to receive SMRs only from ETRs, the implications of sending SMRs from a MS are discussed in this section.

As indicated in Section 2, the MS generates the SMR message using one of its locators as source locator. However, this locator will not be present in the Locator-Set cached for that EID-prefix at the (P)ITR. Following [RFC6830], upon receiving the SMR message, the (P)ITR will check if the source locator is in the Locator-Set cached for that EID-record. Since it is not, the (P)ITR will send the SMR-invoked

Map-Request always to the Mapping System and never to the source locator of the SMR message. This means that a MS can not force an SMR-invoked Map-Request to be sent directly towards itself. However, it is possible that the Mapping System in use is instantiated (even partially) by the MS originator of the SMR. In that case, it may be that the SMR-invoked Map Request will eventually reach the MS, either directly or after being internally forwarded through the Mapping System.

4. Deployment considerations

The extension defined in this document may be useful in scenarios where the MS wants to signal (P)ITRs about changes on mappings it is serving. For instance, when the MS is keeping track of the (P)ITRs that are requesting its mappings and wants to inform them intermediately whenever a mapping is updated.

SDN deployments that use LISP as a southbound protocol are particularly suitable to take advantage of this extension. On the SDN scenario, mapping updates will unlikely come from ETRs, but rather from a centralized entity that pushes the updates directly to the Mapping System. In such deployments, Map Servers will benefit from having a mechanism to inform directly (P)ITRs about updates in the mappings they are serving.

Due to scalability and security concerns, it is RECOMMENDED that this extension is only applied in intra-domain scenarios where all LISP devices are within a single administrative domain.

To limit the impact of the extension and to ease its integration with the rest of LISP signaling and operation, it is RECOMMENDED that the MS only sends SMR messages for those mappings it is proxy-replying for.

5. Acknowledgments

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

As described in [RFC6830], the SMR messages and the SMR-invoked Map-Request MUST be rate-limited. This does not change with the extension proposed in this document.

The (P)ITRs receiving SMRs from the MS will send Map-Request messages to the Mapping System to retrieve authoritative mappings. It is

RECOMMENDED that the security mechanism described in [I-D.ietf-lisp-sec] and [RFC8111] are in place to secure the mapping retrieval and protect against unsolicited messages or hijacking attacks.

8. Normative References

[I-D.ietf-lisp-sec]
Maino, F., Ermagan, V., Cabellos-Aparicio, A., and D. Saucez, "LISP-Security (LISP-SEC)", draft-ietf-lisp-sec-13 (work in progress), September 2017.

[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>.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <https://www.rfc-editor.org/info/rfc6830>.

[RFC8111] Fuller, V., Lewis, D., Ermagan, V., Jain, A., and A. Smirnov, "Locator/ID Separation Protocol Delegated Database Tree (LISP-DDT)", RFC 8111, DOI 10.17487/RFC8111, May 2017, <https://www.rfc-editor.org/info/rfc8111>.

Authors' Addresses

Alberto Rodriguez-Natal
Cisco Systems
170 Tasman Drive
San Jose, CA
USA

Email: natal@cisco.com

Albert Cabellos-Aparicio
Technical University of Catalonia
Barcelona
Spain

Email: acabello@ac.upc.edu

Vina Ermagan
Cisco Systems
170 Tasman Drive
San Jose, CA
USA

Email: vermagan@cisco.com

Fabio Maino
Cisco Systems
170 Tasman Drive
San Jose, CA
USA

Email: fmaino@cisco.com

Sharon Barkai
Fermi Serverless
CA
USA

Email: sharon@fermicloud.io