Stream: Internet Engineering Task Force (IETF)
RFC: 9735
Category: Standards Track
Published: February 2025
ISSN: 2070-1721
Authors: D. Farinacci *lispers.net*
L. Iannone, Ed. *Huawei*

RFC 9735
Locator/ID Separation Protocol (LISP) Distinguished Name Encoding

Abstract

This document defines how to use the Address Family Identifier (AFI) 17 "Distinguished Name" in the Locator/ID Separation Protocol (LISP). LISP introduces two new numbering spaces: Endpoint Identifiers (EIDs) and Routing Locators (RLOCs). Distinguished Names (DNs) can be used in either EID-Records or RLOC-Records in LISP control messages to convey additional information.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9735.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
2.1. Definition 3
2.2. Requirements Language 3
3. Distinguished Name Format 3
4. Mapping-System Lookups for DN EIDs 4
5. Example Use Cases 4
6. Name-Collision Considerations 5
7. Security Considerations 5
8. IANA Considerations 5
9. Sample LISP DN Deployment Experience 5
9.1. DNs to Advertise Specific Device Roles or Functions 5
9.2. DNs to Drive xTR Onboarding Procedures 6
9.3. DNs for NAT-Traversal 6
9.4. DNs for Self-Documenting RLOC Names 6
9.5. DNs Used as EID Names 7
10. References 7
10.1. Normative References 7
10.2. Informative References 7
Acknowledgments 8
Authors' Addresses 8

1. Introduction

LISP ([RFC9300] and [RFC9301]) introduces two new numbering spaces: Endpoint Identifiers (EIDs) and Routing Locators (RLOCs). To provide flexibility for current and future applications, these values can be encoded in LISP control messages using a general syntax that includes the Address Family Identifier (AFI).

The length of addresses encoded in EID-Records and RLOC-Records can easily be determined by the AFI field, as the size of the address is implicit in its AFI value. For instance, for AFI equal to 1, which is "IP (IP version 4)", the address length is known to be 4 octets. However, AFI 17 "Distinguished Name", is a variable-length value, so the length cannot be determined solely from the AFI value 17 [ADDRESS-FAMILY]. This document defines a termination character, an 8-bit value of 0, to be used as a string terminator so the length can be determined.

LISP DNs are useful when encoded either in EID-Records or RLOC-Records in LISP control messages. As EIDs, they can be registered in the Mapping System to find resources, services, or simply be used as a self-documenting feature that accompanies other address-specific EIDs. As RLOCs, DNs, along with RLOC-specific addresses and parameters, can be used as labels to identify equipment type, location, or any self-documenting string a registering device desires to convey.

The Distinguished Name field in this document has no relationship to the similarly named field in the Public-Key Infrastructure using X.509 (PKIX) specifications (e.g., [RFC5280]).

2. Terminology

2.1. Definition

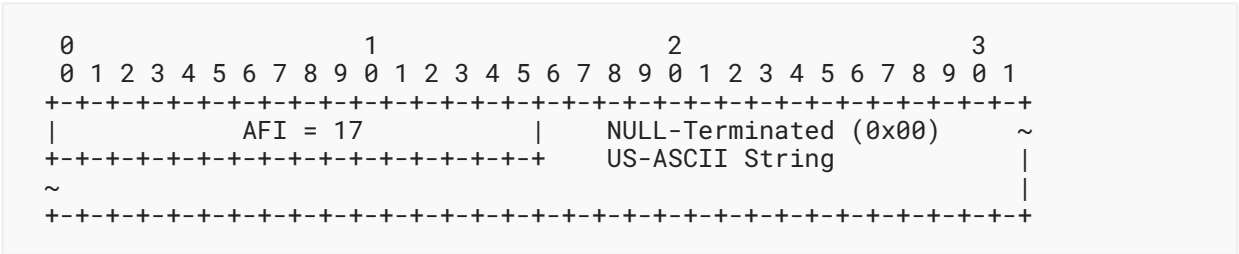
Address Family Identifier (AFI): a term used to describe an address encoding in a packet. An address family is currently defined for IPv4 or IPv6 addresses. See [ADDRESS-FAMILY] for details on other types of information that can be AFI encoded.

2.2. 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Distinguished Name Format

An AFI 17 "Distinguished Name" is encoded as:



The variable-length string of characters are encoded as a NULL-terminated (0x00) US-ASCII character set as defined in [RFC3629], where UTF-8 has the characteristic of preserving the full US-ASCII range. A NULL character **MUST** appear only once in the string and **MUST** be at the end of the string.

When DNs are encoded for EIDs, the EID Mask-Len length of the EID-Records, for all LISP control messages [RFC9301], is the length of the string in bits (including the NULL-terminated 0x00 octet).

Where DNs are encoded anywhere else (i.e., nested in LISP Canonical Address Format (LCAF) encodings [RFC8060]), an explicit length field can be used to indicate the length of the ASCII string in octets. The length field **MUST** include the NULL octet (0x00). The string **MUST** still be NULL-terminated (0x00). If a NULL octet (0x00) appears before the end of the octet field, i.e., the NULL octet (0x00) appears before the last position in the octet fields, then the string **MAY** be accepted and the octets after the NULL octet (0x00) **MUST NOT** be used as part of the octet string.

If the octet after the AFI field is the NULL octet (0x00), the string is a NULL string and **MUST** be accepted. That is, an AFI 17 "Distinguished Name" encoded string **MUST** be at least 1 octet in length.

4. Mapping-System Lookups for DN EIDs

When performing DN-EID lookups, Map-Request messages **MUST** carry an EID Mask-Len length equal to the length of the name string in bits. This instructs the Mapping System to do either an exact-match or a longest-match lookup.

If the DN EID is registered with the same length as the length in a Map-Request, the Map-Server (when configured for proxy Map-Replying) returns an exact-match lookup with the same EID Mask-Len length. If a less specific name is registered, then the Map-Server returns the registered name with the registered EID Mask-Len length.

For example, if the registered EID name is "ietf" with an EID Mask-Len length of 40 bits (the length of the string "ietf" plus the length of the NULL octet (0x00) makes 5 octets), and a Map-Request is received for EID name "ietf.lisp" with an EID Mask-Len length of 80 bits, the Map-Server will return EID "ietf" with a length of 40 bits.

5. Example Use Cases

This section identifies three specific use-case examples for the DN format: two are used for an EID encoding and one for an RLOC-Record encoding. When storing public keys in the Mapping System, as in [LISP-ECDSA], a well-known format for a public-key hash can be encoded as a DN. When street-location-to-GPS-coordinate mappings exist in the Mapping System, as in [LISP-GEO], the street location can be a free-form UTF-8 ASCII representation (with whitespace characters) encoded as a DN. An RLOC that describes an Ingress or Egress Tunnel Router (xTR) behind a NAT device can be identified by its router name, as in [LISPERS-NET-NAT]. In this case, DN encoding is used in NAT Info-Request messages after the EID-prefix field of the message.

6. Name-Collision Considerations

When a DN encoding is used to format an EID, the uniqueness and allocation concerns are no different than registering IPv4 or IPv6 EIDs to the Mapping System. See [RFC9301] for more details. Also, the use cases documented in Section 5 of this specification provide allocation recommendations for their specific uses.

It is **RECOMMENDED** that each use case register their DNs with a unique Instance-ID. Any use cases that require different uses for DNs within an Instance-ID **MUST** define their own Instance-ID and syntax structure for the name registered to the Mapping System. See the encoding procedures in [LISP-VPN] for an example.

7. Security Considerations

DNs are used in mappings that are part of the LISP control plane and may be encoded using LCAF; thus, the security considerations of [RFC9301] and [RFC8060] apply.

8. IANA Considerations

This document has no IANA actions.

9. Sample LISP DN Deployment Experience

Practical implementations of the LISP DN, defined in this document, have been running in production networks for some time. The following sections provide some examples of its usage and lessons learned out of this experience.

9.1. DNs to Advertise Specific Device Roles or Functions

In a practical implementation of [LISP-EXT] on LISP deployments, routers running as Proxy Egress Tunnel Routers (Proxy-ETRs) register their role with the Mapping System in order to attract traffic destined for external networks. Practical implementations of this functionality make use of a DN as an EID to identify the Proxy-ETR role in a Map-Registration.

In this case, all Proxy-ETRs supporting this function register a common DN together with their own offered locator. The Mapping System aggregates the locators received from all Proxy-ETRs as a common locator-set that is associated with this DN EID. In this scenario, the DN serves as a common reference EID that can be requested (or subscribed as per [RFC9437]) to dynamically gather this Proxy-ETR list as specified in the LISP Site External Connectivity document [LISP-EXT].

The use of a DN here provides descriptive information about the role being registered and allows the Mapping System to form locator-sets associated with a specific role. These locator-sets can be distributed on-demand based on using the shared DN as EID. It also allows the network admin and the Mapping System to selectively choose what roles and functions can be registered and distributed to the rest of the participants in the network.

9.2. DNs to Drive xTR Onboarding Procedures

Following the LISP reliable transport [LISP-MAP], ETRs that plan to switch to using reliable transport to hold registrations first need to start with UDP registrations. The UDP registration allows the Map-Server to perform basic authentication of the ETR and to create the necessary state to permit the reliable transport session to be established (e.g., establish a passive open on TCP port 4342 and add the ETR RLOC to the list allowed to establish a session).

In the basic implementation of this process, the ETRs need to wait until local mappings are available and ready to be registered with the Mapping System. Furthermore, when the Mapping System is distributed, the ETR requires having one specific mapping ready to be registered with each one of the relevant Map-Servers. This process may delay the onboarding of ETRs with the Mapping System so that they can switch to using reliable transport. This can also lead to generating unnecessary signaling as a reaction to certain triggers like local port flaps and device failures.

The use of dedicated name registrations allows driving this initial ETR onboarding on the Mapping System as a deterministic process that does not depend on the availability of other mappings. It also provides more stability to the reliable transport session to survive through transient events.

In practice, LISP deployments use dedicated DNs that are registered as soon as xTRs come online with all the necessary Map-Servers in the Mapping System. The mapping with the dedicated DN together with the RLOCs of each Egress Tunnel Router (ETR) in the locator-set is used to drive the initial UDP registration and also to keep the reliable transport state stable through network condition changes. On the Map-Server, these DN registrations facilitate setting up the necessary state to onboard new ETRs rapidly and in a more deterministic manner.

9.3. DNs for NAT-Traversal

At the time of writing, the open-source lispers.net NAT-Traversal implementation [LISPERS-NET-NAT] has deployed DNs for documenting xTRs versus Re-encapsulating Tunnel Routers (RTRs) as they appear in a locator-set for 10 years.

9.4. DNs for Self-Documenting RLOC Names

At the time of writing, the open-source lispers.net implementation [LISPERS-NET-NAT] has self-documented RLOC names in production and pilot environments for 10 years. The RLOC name is encoded with the RLOC address in DN format.

9.5. DNs Used as EID Names

At the time of writing, the open-source lispers.net implementation [LISPERS-NET-NAT] has deployed xTRs that are allowed to register EIDs as DNs for 10 years. The LISP Mapping System can be used as a DNS proxy for Name-to-EID-address or Name-to-RLOC-address mappings. The implementation also supports Name-to-Public-Key mappings to provide key management features in [LISP-ECDSA].

10. References

10.1. Normative References

[ADDRESS-FAMILY] IANA, "Address Family Numbers", <https://www.iana.org/assignments/address-family-numbers>.

[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>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

[RFC9437] Rodriguez-Natal, A., Ermagan, V., Cabellos, A., Barkai, S., and M. Boucadair, "Publish/Subscribe Functionality for the Locator/ID Separation Protocol (LISP)", RFC 9437, DOI 10.17487/RFC9437, August 2023, <https://www.rfc-editor.org/info/rfc9437>.

10.2. Informative References

[LISP-ECDSA] Farinacci, D. and E. Nordmark, "LISP Control-Plane ECDSA Authentication and Authorization", Work in Progress, Internet-Draft, draft-ietf-lisp-ecdsa-auth-13, 18 August 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-ecdsa-auth-13>.

[LISP-EXT] Jain, P., Moreno, V., and S. Hooda, "LISP Site External Connectivity", Work in Progress, Internet-Draft, draft-ietf-lisp-site-external-connectivity-01, 24 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-site-external-connectivity-01>.

[LISP-GEO] Farinacci, D., "LISP Geo-Coordinate Use-Cases", Work in Progress, Internet-Draft, draft-ietf-lisp-geo-09, 15 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-geo-09>.

[LISP-MAP] Venkatachalapathy, B., Portoles-Comeras, M., Lewis, D., Kouvelas, I., and C. Cassar, "LISP Map Server Reliable Transport", Work in Progress, Internet-Draft, draft-ietf-lisp-map-server-reliable-transport-05, 4 November 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-map-server-reliable-transport-05>.

[LISP-VPN] Moreno, V. and D. Farinacci, "LISP Virtual Private Networks (VPNs)", Work in Progress, Internet-Draft, draft-ietf-lisp-vpn-12, 19 September 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-vpn-12>.

[LISPERS-NET-NAT] Farinacci, D., "lispers.net LISP NAT-Traversal Implementation Report", Work in Progress, Internet-Draft, draft-farinacci-lisp-lispers-net-nat-09, 8 December 2024, <https://datatracker.ietf.org/doc/html/draft-farinacci-lisp-lispers-net-nat-09>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8060] Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", RFC 8060, DOI 10.17487/RFC8060, February 2017, <https://www.rfc-editor.org/info/rfc8060>.

Acknowledgments

The authors would like to thank the LISP WG for their review and acceptance of this document. A special thank you goes to Marc Portoles for moving this document through the process and providing deployment-experience samples.

Authors' Addresses

Dino Farinacci
lispers.net
San Jose, CA
United States of America
Email: farinacci@gmail.com

Luigi Iannone (EDITOR)
Huawei Technologies France S.A.S.U.
18, Quai du Point du Jour
92100 Boulogne-Billancourt
France
Email: luigi.iannone@huawei.com