Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-ietf-lisp-name-encoding-07
Published: 14 May 2024
Intended Status: Standards Track
Expires: 15 November 2024
Authors: D. Farinacci
lispers.net

LISP Distinguished Name Encoding

Abstract

This draft defines how to use the AFI=17 Distinguished Names in LISP.

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 [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 15 November 2024.

Copyright Notice

Table of Contents

1. Introduction

The LISP architecture and protocols [RFC9300] introduces two new numbering spaces, Endpoint Identifiers (EIDs) and Routing Locators (RLOCs) which are intended to replace most use of IP addresses on the Internet. To provide flexibility for current and future applications, these values can be encoded in LISP control messages using a general syntax that includes Address Family Identifier (AFI) [RFC3232].

The length of the value field is implicit in the type of address that follows. For AFI 17, a Distinguished Name can be encoded. A name can be a variable length field so the length cannot be determined solely from the AFI value 17. This draft defines a termination character, an 8-bit value of 0 to be used as a string terminator so the length can be determined.

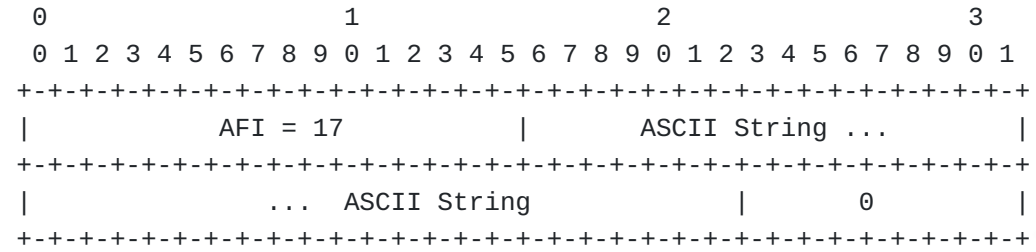
LISP Distinguished Names are useful when encoded either in EID-Records or RLOC-records in LISP control messages. As EIDs, they can be registered in the mapping system to find resources, services, or simply used as a self-documenting feature that accompany other address specific EIDs. As RLOCs, Distinguished Names, 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.

2. Definition of Terms

Address Family Identifier (AFI): a term used to describe an address encoding in a packet. An address family currently defined for IPv4 or IPv6 addresses. See [IANA-ADDRESS-FAMILY-REGISTRY] and [RFC3232] for details on other types of information that can be AFI encoded.

3. Distinguished Name Format

An AFI=17 Distinguished Name is encoded as:



The string of characters are encoded in the ASCII character-set definition [RFC0020].

When Distinguished Names are encoded for EIDs, the EID-Prefix length of the EIDs as they appear in EID-Records for all LISP control messages is the length of the string in bits (include the null 0 byte). Where Distinguished Names are encoded anywhere else (i.e. nested in LCAF encodings), then any length field is the length of the ASCII string including the null 0 byte in units of bytes.

4. Mapping System Lookups for Distinguished Name EIDs

Distinguished Name EID lookups MUST carry as an EID-Prefix length equal to the length of the name string. This instructs the mapping system to do either an exact match or longest match lookup.

If the Distinguished Name 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-Prefix length. If a less specific name is registered, then the Map-Server returns the registered name with the registered EID-Prefix length.

For example, if the registered EID name is "ietf" with EID-prefix length of 40 bits (the length of string "ietf" plus the null byte is 5 bytes), and a Map-Request is received for EID name "ietf.lisp" with an EID-prefix length of 80 bits, the Map-Server will return EID "ietf" with length of 40 bits.

5. Example Use-Cases

This section identifies three specific use-cases examples for the Distinguished Name format. Two are used for an EID encoding and one for a RLOC-record encoding. When storing public keys in the mapping system, as in [I-D.ietf-lisp-ecdsa-auth], a well known format for a public-key hash can be encoded as a Distinguished Name. When street location to GPS coordinate mappings exist in the mapping system, as in [I-D.ietf-lisp-geo], the street location can be a free form ASCII representation (with whitespace characters) encoded as a Distinguished Name. An RLOC that describes an xTR behind a NAT device can be identified by its router name, as in [I-D.farinacci-lisp-lispers-net-nat], uses a Distinguished Name encoding. As well as identifying the router name (neither an EID or an RLOC) in NAT Info-Request messages uses Distinguished Name encodings.

6. Name Collision Considerations

When a Distinguished Name 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-case documents specified in Section 5 provide allocation recommendations for their specific uses.

It is RECOMMENDED that each use-case register their Distinguish Names with a unique Instance-ID. For any use-cases which require different uses for Distinguish Names within an Instance-ID MUST define their own Instance-ID and structure syntax for the name registered to the Mapping System. See the encoding procedures in [I-D.ietf-lisp-vpn] for an example.

7. Security Considerations

There are no security considerations.

8. IANA Considerations

The code-point values in this specification are already allocated in [IANA-ADDRESS-FAMILY-REGISTRY].

9. Sample LISP Distinguished Name (DN) Deployment Experience

Practical implementations of the LISP Distinguished Name specification have been running in production networks for some time. The following sections provide some examples of its usage and lessons gathered out of the experience.

9.1. DNs to Advertise Specific Device Roles or Functions

In a practical implementation of [I-D.ietf-lisp-site-external-connectivity] on LISP deployments, routers running as 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 Distinguished Name 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 Distinguished Name 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 to this DN EID. The Distinguished Name in this case 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.

The use of a Distinguished Name in this case provides descriptive information about the role being registered and allows the Mapping System to form locator-sets associated to 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 On-Boarding Procedures

Following the LISP reliable transport [I-D.ietf-lisp-map-server-reliable-transport], ETRs that plan to switch to using a reliable transport to hold registrations first need to start with traditional UDP registrations. The UDP registration allows the Map-Server to perform basic authentication of the ETR and create the necessary state to permit the reliable transport session to go through (e.g., establish a passive open of 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. Even more, when the mapping system is distributed, the ETR requires to have 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 a 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 on-boarding 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 Distinguished Names 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 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 eRs rapidly and in a more deterministic manner.

9.3. DNs for NAT-Traversal

The open source lispers.net NAT-Traversal implementation [I-D.farinacci-lisp-lispers-net-nat] has had 10 years of deployment experience using Distinguished Names for documenting xTRs versus RTRs as they appear in an locator-set.

9.4. DNs for Self-Documenting RLOC Names

The open source lispers.net implementation has had 10 years of self-documenting RLOC names in production and pilot environments. The

RLOC name is encoded with the RLOC address in Distinguished Name format.

9.5. DNs used as EID Names

The open source lispers.net implementation has had 10 years of deployment experience allowing xTRs to register EIDs as Distinguished Names. 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 [I-D.ietf-lisp-ecdsa-auth].

10. References

10.1. Normative References

[IANA-ADDRESS-FAMILY-REGISTRY] IANA, "IANA Address Family Numbers Registry", https://www.iana.org/assignments/address-family-numbers/, December 2023.

[RFC0020] Cerf, V., "ASCII format for network interchange", STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, <https://www.rfc-editor.org/info/rfc20>.

[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>.

[RFC3232] Reynolds, J., Ed., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, DOI 10.17487/RFC3232, January 2002, <https://www.rfc-editor.org/info/rfc3232>.

[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

[I-D.farinacci-lisp-lispers-net-nat]
Farinacci, D., "lispers.net LISP NAT-Traversal Implementation Report", Work in Progress, Internet-Draft, draft-farinacci-lisp-lispers-net-nat-07, 22 December 2023, <https://datatracker.ietf.org/doc/html/draft-farinacci-lisp-lispers-net-nat-07>.

[I-D.ietf-lisp-ecdsa-auth] Farinacci, D. and E. Nordmark, "LISP Control-Plane ECDSA Authentication and Authorization", Work in Progress, Internet-Draft, draft-ietf-lisp-ecdsa-auth-12, 19 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-ecdsa-auth-12>.

[I-D.ietf-lisp-geo] Farinacci, D., "LISP Geo-Coordinate Use-Cases", Work in Progress, Internet-Draft, draft-ietf-lisp-geo-06, 6 May 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-geo-06>.

[I-D.ietf-lisp-map-server-reliable-transport]
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-04, 21 April 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-map-server-reliable-transport-04>.

[I-D.ietf-lisp-site-external-connectivity] Jain, P., Moreno, V., and S. Hooda, "LISP Site External Connectivity", Work in Progress, Internet-Draft, draft-ietf-lisp-site-external-connectivity-00, 27 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-site-external-connectivity-00>.

[I-D.ietf-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>.

Appendix A. Acknowledgments

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

Appendix B. Document Change Log

B.1. Changes to draft-ietf-lisp-name-encoding-07

*Submitted May 2024.

*Changed document status to "Proposed Standard" and some rewording per Alberto for the pETR use-case section.

B.2. Changes to draft-ietf-lisp-name-encoding-06

*Submitted April 2024.

*Add Deployment Experience section for standards track requirements.

*Update references.

B.3. Changes to draft-ietf-lisp-name-encoding-05

*Submitted December 2023.

*Update IANA AFI reference.

B.4. Changes to draft-ietf-lisp-name-encoding-04

*Submitted December 2023.

*More comments from Alberto. Change to standard spellings throughout.

*Add RFC 2119 boilerplate.

*Update reference RFC1700 to RFC3232.

B.5. Changes to draft-ietf-lisp-name-encoding-03

*Submitted December 2023.

*Address comments from Alberto, document shepherd.

*Update references.

B.6. Changes to draft-ietf-lisp-name-encoding-02

*Submitted August 2023.

*Update references and document expiry timer.

B.7. Changes to draft-ietf-lisp-name-encoding-01

*Submitted February 2023.

*Update references and document expiry timer.

*Change 68**.bis references to proposed RFC references.

B.8. Changes to draft-ietf-lisp-name-encoding-00

*Submitted August 2022.

*Move individual submission to LISP WG document.

B.9. Changes to draft-farinacci-lisp-name-encoding-15

*Submitted July 2022.

*Added more clarity text about how using VPNs (instance-ID encoding) addresses name collisions from multiple use-cases.

*Update references and document expiry timer.

B.10. Changes to draft-farinacci-lisp-name-encoding-14

*Submitted May 2022.

*Update references and document expiry timer.

B.11. Changes to draft-farinacci-lisp-name-encoding-13

*Submitted November 2021.

*Update references and document expiry timer.

B.12. Changes to draft-farinacci-lisp-name-encoding-12

*Submitted May 2021.

*Update references and document expiry timer.

B.13. Changes to draft-farinacci-lisp-name-encoding-11

*Submitted November 2020.

*Made changes to reflect working group comments.

*Update references and document expiry timer.

B.14. Changes to draft-farinacci-lisp-name-encoding-10

*Submitted August 2020.

*Update references and document expiry timer.

B.15. Changes to draft-farinacci-lisp-name-encoding-09

*Submitted March 2020.

*Update references and document expiry timer.

B.16. Changes to draft-farinacci-lisp-name-encoding-08

*Submitted September 2019.

*Update references and document expiry timer.

B.17. Changes to draft-farinacci-lisp-name-encoding-07

*Submitted March 2019.

*Update referenes and document expiry timer.

B.18. Changes to draft-farinacci-lisp-name-encoding-06

*Submitted September 2018.

*Update document expiry timer.

B.19. Changes to draft-farinacci-lisp-name-encoding-05

*Submitted March 2018.

*Update document expiry timer.

B.20. Changes to draft-farinacci-lisp-name-encoding-04

*Submitted September 2017.

*Update document expiry timer.

B.21. Changes to draft-farinacci-lisp-name-encoding-03

*Submitted March 2017.

*Update document expiry timer.

B.22. Changes to draft-farinacci-lisp-name-encoding-02

*Submitted October 2016.

*Add a comment that the distinguished-name encoding is restricted to ASCII character encodings only.

B.23. Changes to draft-farinacci-lisp-name-encoding-01

*Submitted October 2016.

*Update document timer.

B.24. Changes to draft-farinacci-lisp-name-encoding-00

*Initial draft submitted April 2016.

Author's Address

Dino Farinacci
lispers.net
San Jose, CA
United States of America

Email: farinacci@gmail.com