LISP Working Group
Internet-Draft
Intended status: Informational
Expires: October 1, 2025

S. Barkai
Oterra.ai
B. Fernandez-Ruiz
Nexar Inc.
R. Tamir
Ariga.io
A. Rodriguez-Natal
F. Maino
Cisco Systems
A. Cabellos-Aparicio
J. Paillisse-Vilanova
Universitat Politecnica de Catalunya
D. Farinacci
lispers.net

April 1, 2025

Geo-Intelligence Network Based On H3 and LISP
draft-ietf-lisp-nexagon-55.txt

Abstract

Lisp-Nexagon is a geospatial intelligence network protocol designed to support physical-world applications such as transportation, public safety, and logistics. It combines the Locator/ID Separation Protocol (LISP) with the H3 spatial indexing system to enable distributed agents to report, aggregate, and disseminate geospatial state information.

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 October 1,2025.

Copyright Notice

Table of Contents

1. Introduction

Lisp-Nexagon is a geospatial intelligence network protocol designed to support physical-world applications such as transportation, public safety, and logistics. It combines the Locator/ID Separation Protocol (LISP) with the [H3] spatial indexing system to enable distributed agents to report, aggregate, and disseminate geospatial state information.

The system models geospatial data flow and control after the management planes found in digital infrastructure. Geospatial intelligence is organized by H3 tiles at varying resolutions. High-resolution (small-area) tiles are used to represent specific environmental and infrastructural conditions such as road status, vegetation coverage, fire activity, weather, and physical obstructions. Data for these tiles is produced by interoperating sources and collected by geo-aggregation agents.

Each aggregation agent is assigned a low-resolution (large-area) H3 tile that defines its jurisdiction. This jurisdiction is associated with a LISP Endpoint Identifier (EID), which acts as the routing and addressing point for intelligence updates. Agents receive input from data sources within their jurisdiction and provide processed information or notifications to clients authorized to query or subscribe to state data.

Lisp-Nexagon provides a framework for structured, addressable, and jurisdiction-based geospatial coordination using existing LISP mechanisms and H3 spatial semantics.

The network requires a formal provisioning step for sources, clients, and agents. For sources and destinations, this step involves an authentication, authorization, and accounting (AAA) procedure through which endpoints request and renew EIDs and LISP tunnel-routers (XTR) to interact through.

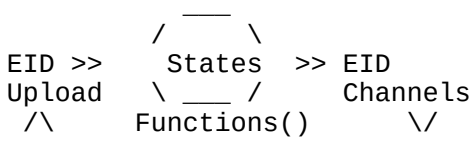

Figure 1:H3-LISP Agents

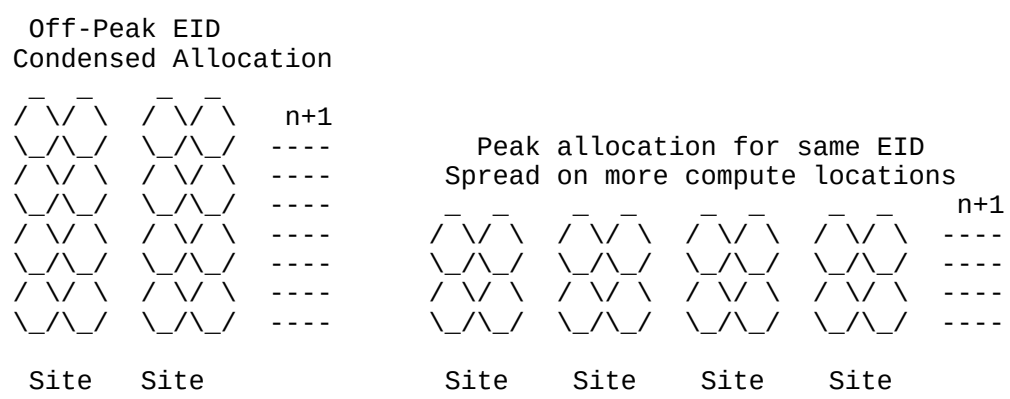

Figure 2: Dynamic allocation per activity

2. Definition of Terms

Based on [RFC9300][RFC9301]

H3AgentEID: H3AgentEID is an EID-addressable Geolocation agent, also known as a nexagon. It serves as a designated destination for Geolocation aggregation and an (S,G) source of multicast themed channels. It has a LISP data-plane stack to encapsulate packets via ServerXTR.

ServerXTR: ServerXTR is a data-plane only LISP protocol stack implementation that is co-located with the H3AgentEID process. It encapsulates and decapsulates packets to and from EdgeRTRs.

MobilityClient: MobilityClient is an application that may be a part of a driving system or mobility application, It has a LISP data-plane stack to encapsulate packets via ClientXTR.

MobilityClientEID: MobilityClientEID is the IPv6 EID used by Mobility Clients. The destination of such packets are H3AgentEIDs. The EID is assigned as part of the MobilityClient network AAA.

ClientXTR: ClientXTR is a data-plane only LISP protocol stack implementation co-located with the Mobility Client application. It encapsulates and decapsulates packets to and from EdgeRTRs.

EdgeRTR: The EdgeRTR network is responsible for connecting Mobility Clients to Agents and managing MobilityClientEIDs multicast registrations [RFC8378]. The network achieves this by using encapsulation to aggregate Mobility Clients and Geolocation Agents, making it easier to access the mobility network from hosting providers and mobile providers.

The RTRs within the EdgeRTR network re-encapsulate packets from ClientXTRs, ServerXTRs, and remote RTRs. During packet decapsulation, EdgeRTRs glean H3 agent EIDs and MobilityClientEIDs and store them along with route locations (RLOCs) in map-caches. These mappings are then registered to the LISP mapping system [RFC9301] and are provisioned when Geolocation Agents are assigned to EdgeRTRs.
It’s key to note that EdgeRTRs do not register MobilityClientEIDs. Enterprises can provide their own EdgeRTRs to protect the geo-privacy.

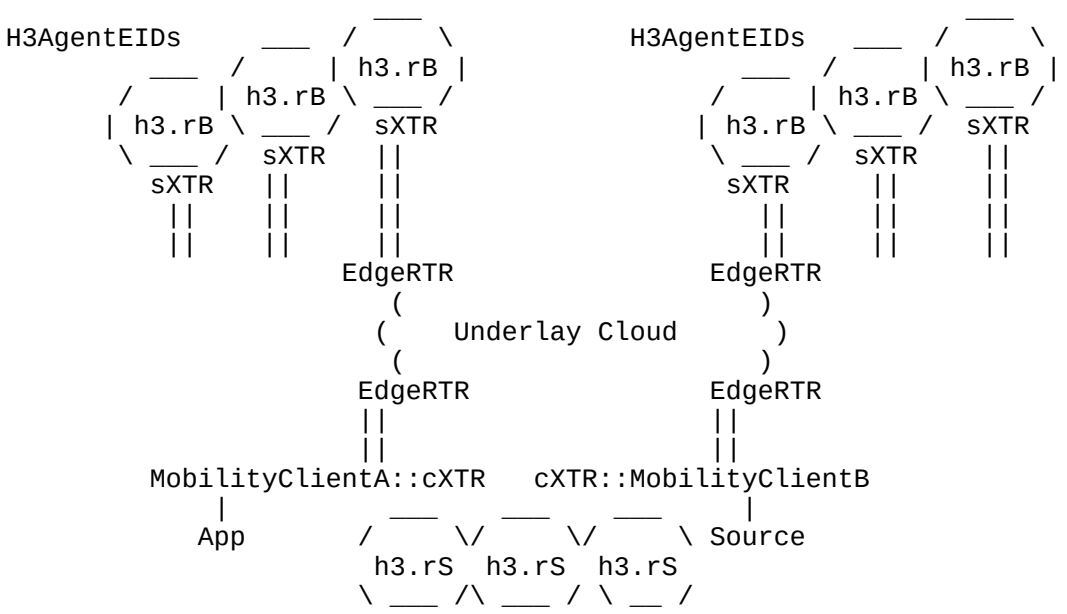

Figure 3: H3-LISP Network

- MobilityClientA source detections used by MobilityClientB app
- Sources share information only through the Geolocation agents
- ClientXTR (cXTR):encapsulates packets over access to EdgeRTR
- ServerXTR (sXTR):encapsulates packets over metro area to EdgeRTR
- Notifications: from Geolocation agents replicated by EdgeRTRs

3. Deployment Assumptions

The authorization of Mobility Clients to the mobility network is renewed while driving. The AAA procedure described below can be used as an example for obtaining EIDs and EdgeRTRs, and for enabling the use of the network. Diameter [RFC6733] based AAA can be used:

1) obtain the address of the mobility-network AAA using DNS
2) obtain MobilityClientEIDs and EdgeRTRs from AAA procedure
3) renewed periodically from AAA while using the network

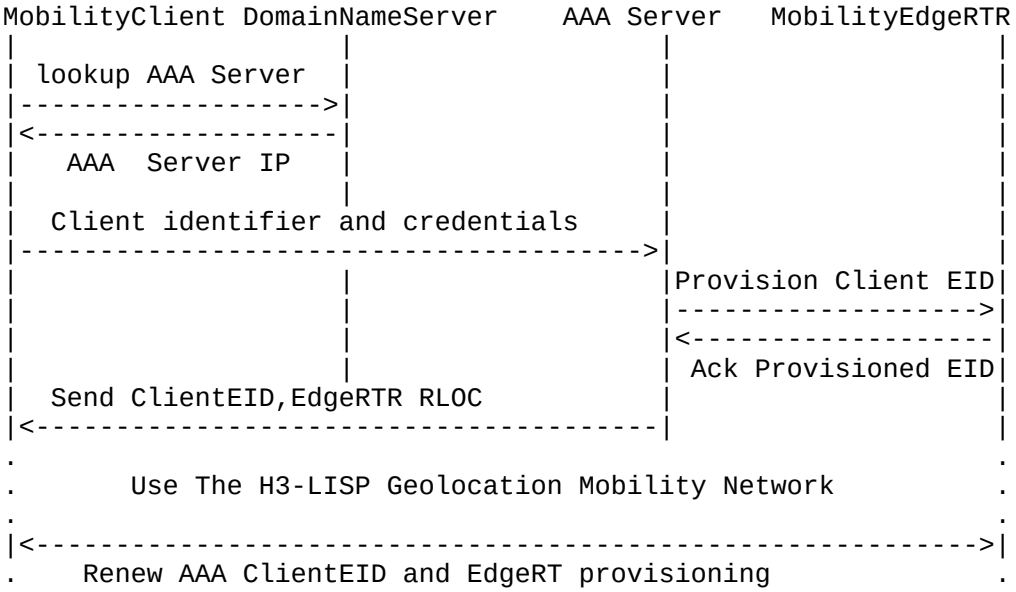

Figure 4: Example AAA procedure for mobility clients

Detections are enumerated in 16 fields x 16 enumerations. Nibbles named using hexadecimal index according to the position where most significant nibble has index 0. Enumerations defined in section 8.

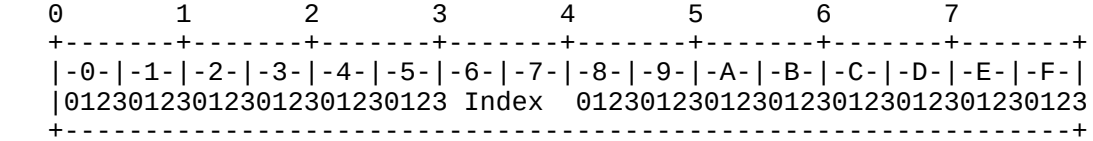

Figure 5: Nibble based detection enumeration

4. Clients-Agents Networking

The mobility network functions as a standard LISP overlay that delivers unicast and multicast packets across data plane XTRs, which are used in the stack of each mobility client and server. ClientXTRs and ServerXTRs are associated with EdgeRTRs, which allows MobilityClients to "show up" at any location within the mobility network, regardless of the network provider or network address translation domain. This structure also enables any H3 agent EID to be instantiated, delegated, or failed over to any compute location. In this specification, we assume a semi-random association between ClientXTRs and EdgeRTRs assigned by the AAA procedure, with a pool of EdgeRTRs, which can be dynamically allocated, distributing the load of MobilityClients within a given metro area. We also assume that EdgeRTRs are topologically equivalent and use LISP to encapsulate traffic to and from other EdgeRTRs. It is possible for there to be more than one ClientEID in the same process using the same ClientXTR. The implementation of such multiplexing is not specified.

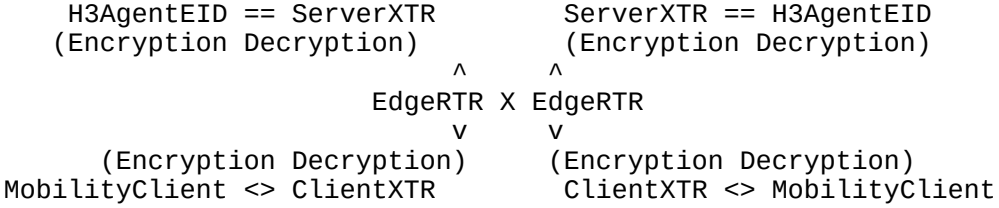

Figure 6: LISP network connecting MobilityClients and H3AgentEIDs

Encode HID to EID:

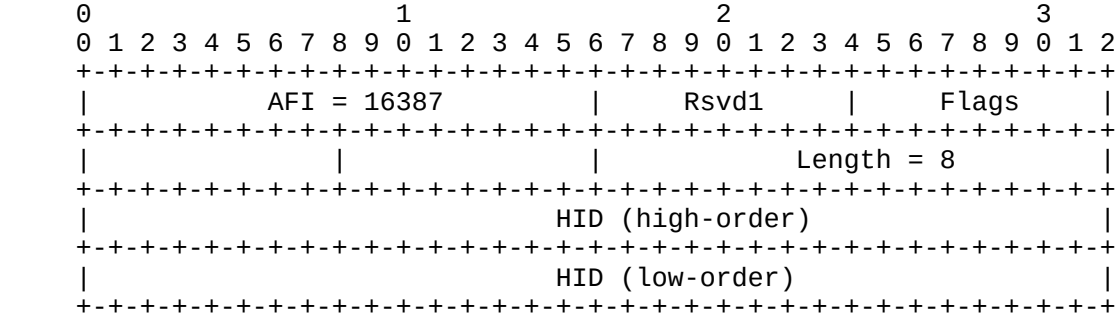

Figure 7: Encoding HIDs in H3AgentEIDs

5. Mobility Unicast and Multicast

The day in a life of unicast road-segment mapping upload:

1. A client detects condition of interest using AI camera
2. The client uses its GPS to establish its h3.rS location
3. It then estimates the h3.rS location of the detection
4. Detection h3.rS center is used to calculate h3.rB => H3ServerEID
5. Client sends (encrypted) location-detection via its ClientXTR

   Outer Header src/dest: ClientXTR RLOC, EdgeRTR RLOC
   Inner Header src/dest: ClientEID, H3AgentEID

6. EdgeRTR gleans and caches ClientEID and ClientXTR RLOC
7. EdgeRTR resolves RLOC of remote EdgeRTR, and re-encapsulates:

   Outer Header src/dest: EdgeRTR RLOC, remote EdgeRTR RLOC
   Inner Header src/dest: ClientEID, H3AgentEID

8. Remote EdgeRTR lookups H3ServerEID ServerXTR RLOC,
   re-encapsulates:

   Outer Header src/dest: EdgeRTR RLOC, ServerXTR RLOC
   Inner Header src/dest: ClientEID, H3AgentEID

9. ServerXTR delivers ClientEID message to H3AgentEID

The detection message headers consist of the following fields:

- Outer headers size = 40 (IPv6) + 8 (UDP) + 8 (LISP) = 56
- Inner headers size = 40 (IPv6) + 8 (UDP) + 4 (Nexagon Header) = 52
- 1500 (MTU) - 56 - 52 = 1392 bytes of effective payload size

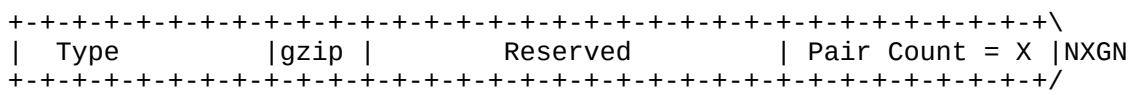

Figure 8: Nexagon header format

Nexagon Header allows for key-value (kv) tuples or value-key,key ..(vkkk) using the same formats of key and value outlined bellow:

```
 Nexagon Header Type 0:reserved (*)
 Type 1:key-value, key-value.. 1392 / (8 + 8) = 87 pairs
 Type 2:value, key,key,key.. (1392 - 8) / 8 = 173 h3.rS IDs
 Type 3-255: unassigned
 Nexagon Header GZIP field: 0x000 no compression, or(**) GZIP version.
 Nexagon Header Reserved bits
  Nexagon Header key and value count (in any format kv or vkkk)

(*)  Reserved fields are specified as being set to 0 on transmission,
       ignored when received.
(**) GZIP refers to entire kv or vkkk payload and major GZIP version,
       packets with unsupported GZIP version are dropped
```

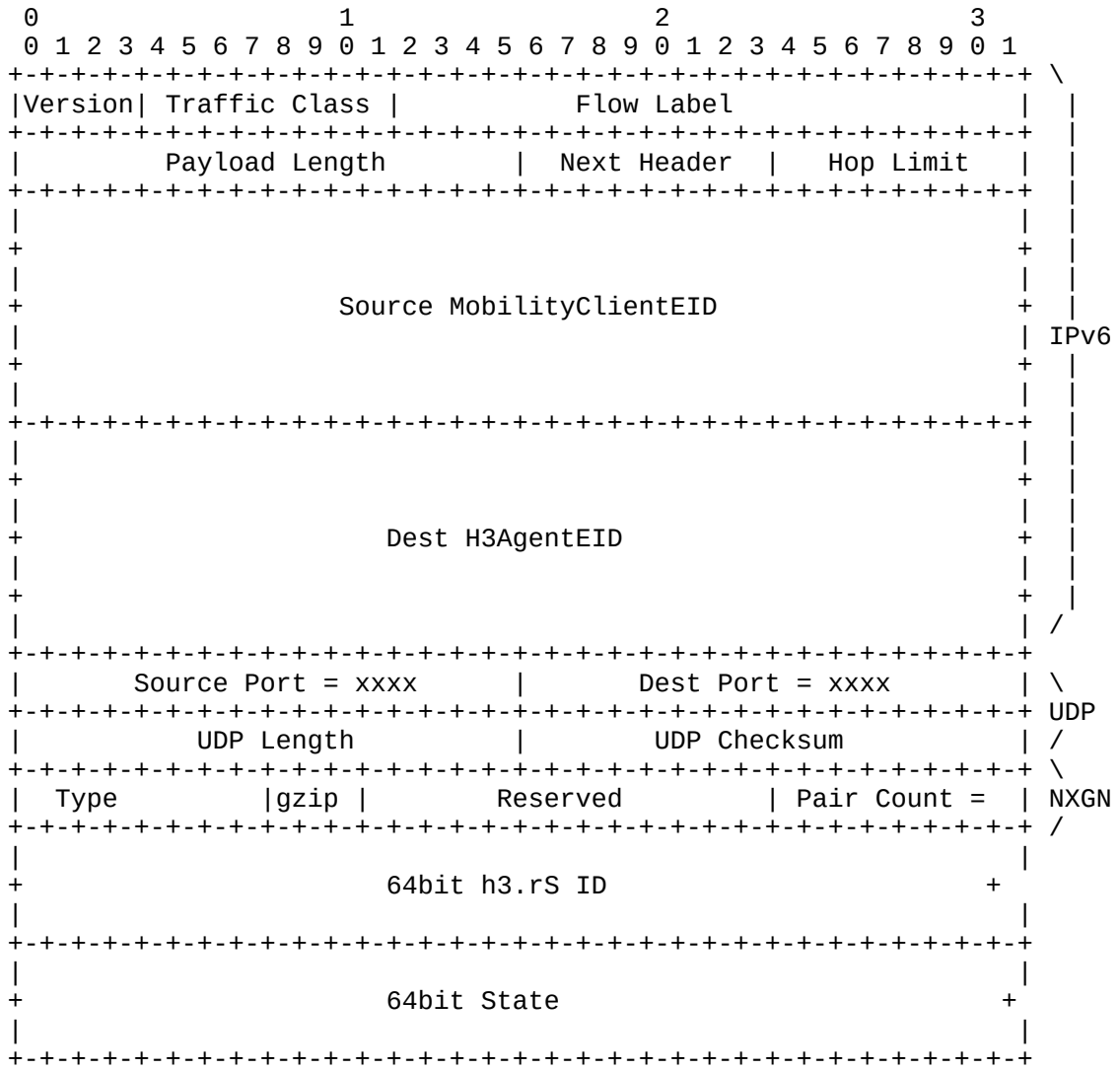

Figure 9: Uploaded detections packet format

Each H3Agent is also an IP Multicast Source used to update subscribers on the state of the h3.rS tiles in the h3.rB area. We use [RFC8378] signal-free multicast to implement overlay channels. Mobility-networks have many channels with thousands subscribers each. MobilityClients driving through/subscribing to an h3.rB area issue group address report based on any mechanism supported by [RFC8378]. Example report formats are specified in [RFC4604]. It is advised that clients establish a ring of objects on their areas of interest. Report messages are encapsulated between ClientXTRs and EdgeRTRs.

The day in a life of multicast notification update:

1. H3AgentEID determines change or timing requiring an update

2. H3AgentEID sends (S,G) update message via its ServerXTR

    Outer Header src/dest: ServerXTR RLOC, EdgeRTR RLOC
    Inner Header (S,G): H3ServerEID, EID chosen for theme

3. EdgeRTR resolves subscribed remote EdgeRTRs, replicates

    Outer Header src/dest: EdgeRTR RLOC, remote EdgeRTR RLOC
    Inner Header (S,G): H3ServerEID, EID chosen for theme

4. EdgeRTRs lookups ClientEIDs ClientXTRs RLOCs, replicates

    Outer Header src/dest: EdgeRTR RLOC, ClientXTR RLOC
    Inner Header (S,G): H3ServerEID, EID chosen for theme

5. ClientXTR delivers multicast channel update message to clientEID

Multicast update packets are of the following structure:

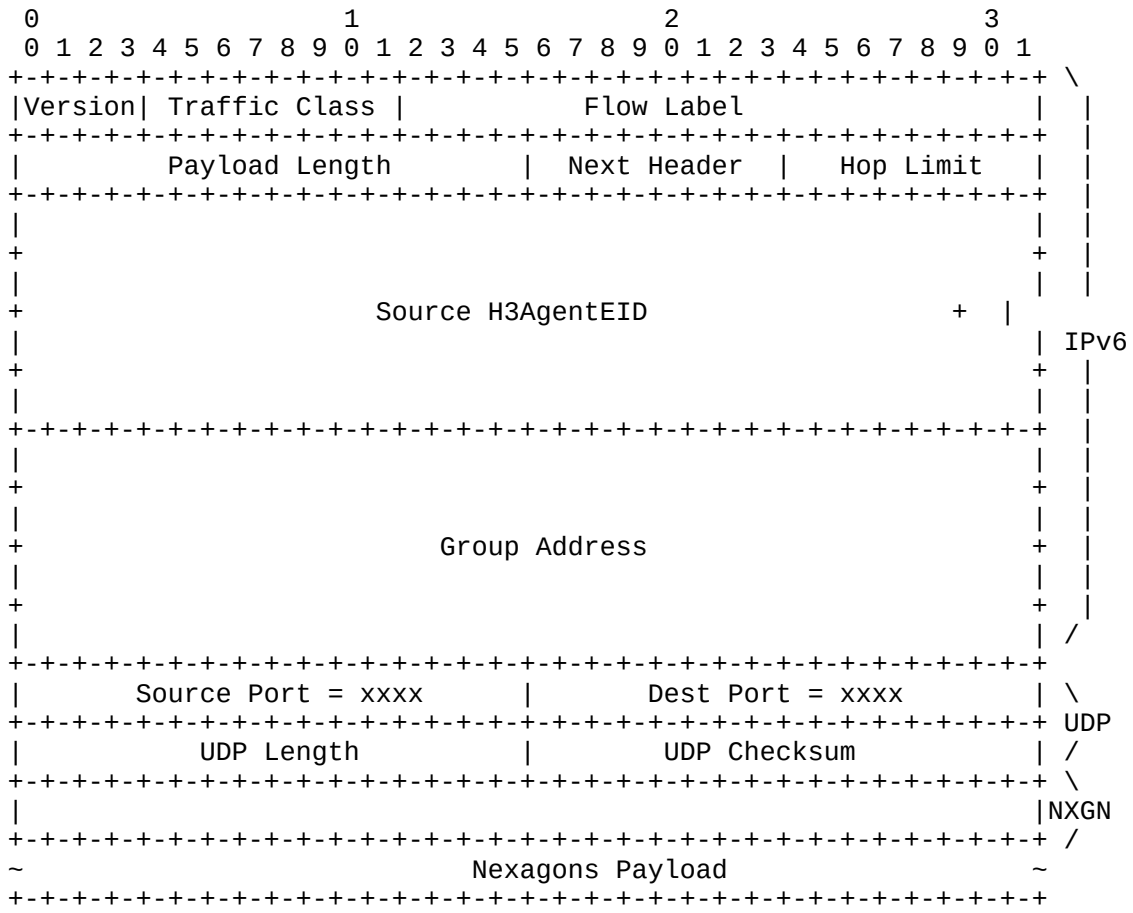

Figure 10: multicast update packet header

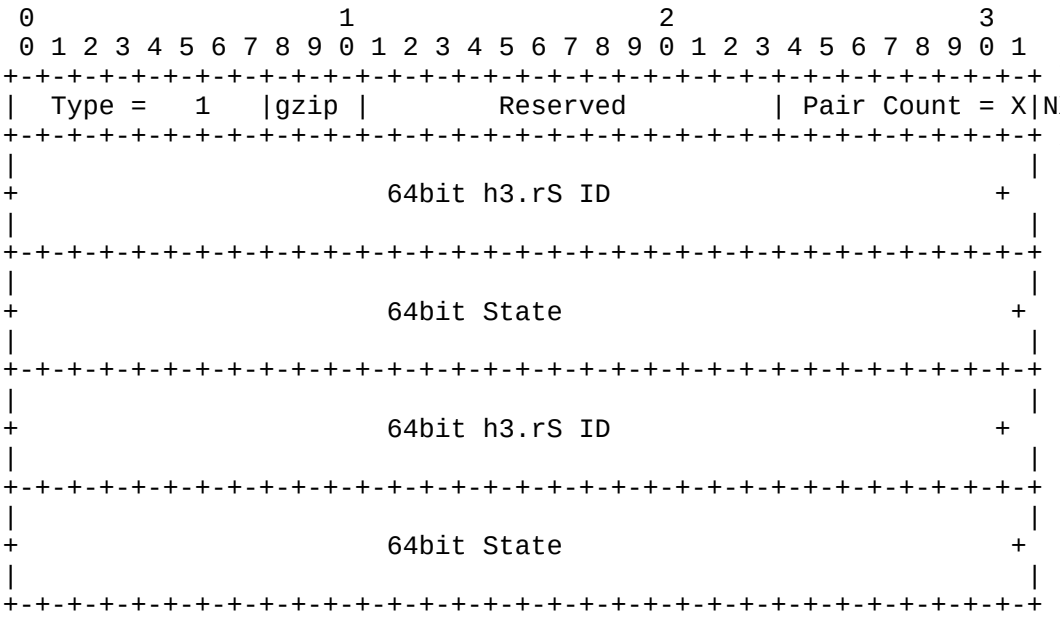

Figure 11: multicast update payload, key-value, key-value..

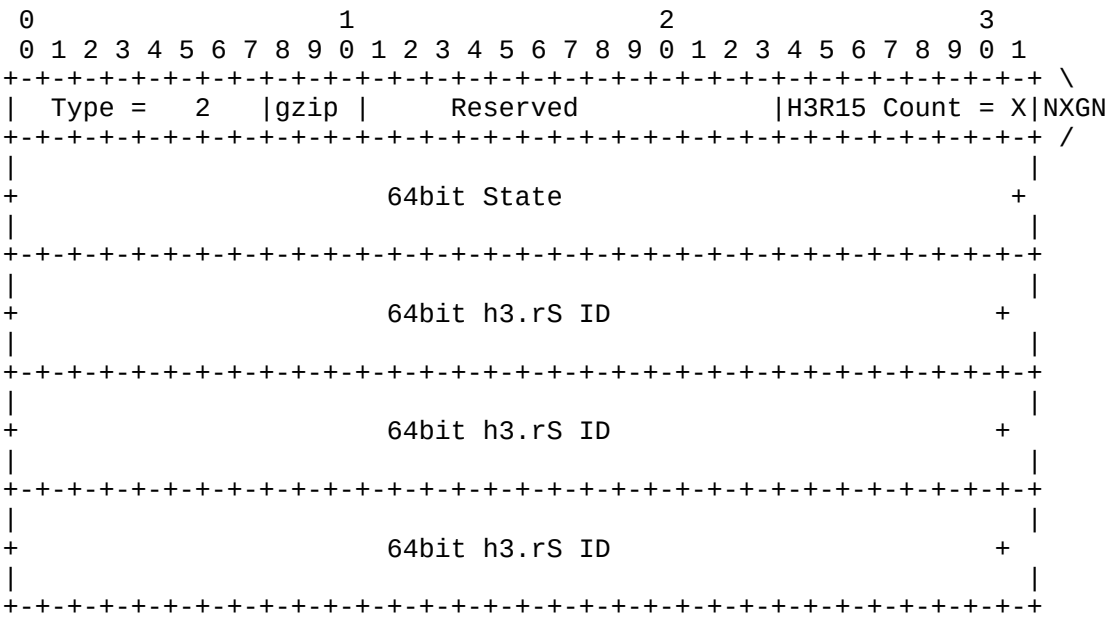

Figure 12: multicast update payload, value, key, key..

6. Security Considerations

The LISP mobility-network is inherently secure and private. All information is conveyed to clients using provisioned Geolocation agents. MobilityClients receive information only via geospatial channels originating at provisioned agents, replicated by EdgeRTRs. All traffic is carried over encrypted encapsulation.

7. Privacy Considerations

In the mobility network, MobilityClients obtain temporary clientEIDs and RLOCs of EdgeRTRs through an AAA process in order to access the network for a certain period. The interface between MobilityClients and EdgeRTRs is the most sensitive from a privacy perspective, as the EdgeRTR can determine the client RLOC and the h3.rB area that the client is engaged with based on header information, even though the traffic on this interface is tunneled and the detection content is encrypted between ClientXTR and EdgeRTR. Enterprises such as vehicle OEMs or carriers can use their own EdgeRTRs (BYO_RTRs), which are pre-provisioned to use the mapping system and are approved by other EdgeRTRs. Beyond the client to EdgeRTR hop, the mapping system does not hold MobilityClientEID information and remote EdgeRTRs are only aware of clients' temporary EIDs. H3AgentEIDs decrypt and parse actual h3.rS detections, taking into account MobilityClientEID credentials encoded in the client EID and assigned by AAA to avoid poorly made or localized detections.

In summary the privacy risk mitigations are:

(1) tapping: all communications are through tunnels therefore may be encrypted using IP-Sec or other supported point to point underlay standards.

(2) spoofing: it is very hard to guess a MobilityClientEID valid for a short period of time. Clients and H3Agents EIDs are provisioned in EdgeRTRs, Clients using the AAA procedure, H3Agents via dev-ops.

(3) credibility: the interface crowd-sources and does not assume to trust single detections. Credit history track MobilityClient aggregate scores from all agents are delivered to AAA subsystem

(4) geo-privacy: Only EdgeRTRs are aware of both clients' RLOC and geo-location, only AAA is aware of client IDs credentials and credit but not geo-location. Ongoing client credit adjustments span all H3Agents administratively to AAA without specific geo-source.

8. Acknowledgments

We would like to kindly thank Joel Halperin for helping structure the AAA section and Geo-Privacy provisions, Luigi Lannone for promoting such LISP based Compute Aware Networking use-cases, helping structure the IANA section, and shepherding this draft to completion. We would like to thank George Ericson from Dell, Lei Zhong from Toyota, Mikael Klein from Ericsson,Leifeng Ruan from Intel, Ririn Andarini from NTT, for helping with Geolocation and Dataflow Virtualization terminology and key-issues during joint work at the AECC. We would like to thank Professor Trevor Darrel and Professor Fisher Yu of BDD for reviewing IANA enumerations for detections-consolidations feasible by visionAI and Edge Computing. We would like to thank Isaac Brodsky, Nick Rabinowitz, David Ellis, and AJ Friend of the H3 steering committee for reviewing the use of the H3 grid in the lisp-nexagon network.

9. IANA Considerations

In accordance with BCP 26 [RFC8126].IANA is asked to create a registry named NEXAGON with the following sub registries.

Spec	IANA Name	Bit	Description
Type	nexagon-type	0-7	Type of key-value encoding
gzip	nexagon-gzip	8-10	gzip major version used
PairCount	nexagon-paircount	24-31	key-value pair count

10. Normative References

[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, mOctober 2022, <https://www.rfc-editor.org/info/rfc9301>.

[RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, DOI 10.17487/RFC4604, December 2006, <https://www.rfc-editor.org/info/rfc4604>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <http://www.rfc-editor.org/info/rfc6733>.

[RFC8126] Cotton, M., Leiba, B., Narten, T., "Guidelines for Writing an IANA Considerations Section in RFCs", RFC8126, DOI 10.17487/RFC8126, Novembere 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8378] Farinacci, D., Moreno, V., "Signal-Free Locator/ID Separation Protocol (LISP) Multicast", RFC8378, DOI 10.17487/RFC8378, May 2018, <https://www.rfc-editor.org/info/rfc8378>.

[H3] Uber Technologies Inc. [n.d.]. H3: Ubers Hexagonal Hierarchical Spatial Index, May 2021, <https://eng.uber.com/h3>.

Authors' Addresses

Sharon Barkai
Oterra
CA
USA

Email: sbarkai@gmail.com

Bruno Fernandez-Ruiz
Nexar
London
UK

Email: b@getnexar.com

Rotem Tamir
Ariga
Israel

Email: r@ariga.io

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

Email: natal@cisco.com

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

Email: fmaino@cisco.com

Albert Cabellos-Aparicio
Universitat Politecnica de Catalunya
Barcelona
Spain

Email: acabello@ac.upc.edu

Jordi Paillisse-Vilanova
Universitat Politecnica de Catalunya
Barcelona
Spain

Email: jordip@ac.upc.edu

Dino Farinacci
lispers.net
San Jose, CA
USA

Email: farinacci@gmail.com