LISP Working Group
Internet-Draft
Intended status: Informational
Expires: March 28,2023

S. Barkai
Nexar
F. Maino
A. Rodriguez-Natal
Cisco Systems
A. Cabellos-Aparicio
J. Paillisse Vilanova
Technical University of Catalonia
D. Farinacci
lispers.net

December 5, 2022

Portable Edge Multipoint Sockets
draft-barkai-lisp-pems-06

Abstract

This document describes the use of the location/identity separation protocol (LISP) for performing on-path scaling and service-selection in environments where off-path cloud based web measures do not perform well. Scaling and service-selection is achieved by abstracting multipoint queue/channel socket communication objects, addressed by well known or algorithmic endpoint identifiers (EID).
Multipoint sockets are decoupled from specific user-space processes, are portable between hosts and network locations. Portability applied by system management according to global considerations, relies on the LISP network for on-path steering between roaming clients and elastic functional processing. Interoperable on-path scaling is achieved by application specific socket addressing scheme.

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 February 28,2023.

Table of Contents

1. Introduction

Next generation Internet of Things (IoT), Augmented/Virtual Reality (AR/VR) applications involve sensors and clients moving across access anchors back-ended by processing functions elastically allocated per activity across low-latency, high north-south capacity edge locations. Traditional off-path Domain Name Service (DNS)resolutions and Hypertext Transfer Protocol (HTTP) redirects, used for services-selection and scaling do not function well in these environments. Behavior in edge environments differs from that of centralized clouds which contain changes preventing mass cached resolutions invalidation. Redirects which are not co-located within clouds tend to oscillate hot spots across locations and recover slowly from location disconnects.

This document describes the use of the location/identity separation protocol (LISP) for performing on-path scaling and service-selection in environments where off-path cloud based web measures do not perform well. Scaling and service-selection is achieved by abstracting multipoint queue/channel socket communication objects, addressed by well known or algorithmic endpoint identifiers (EID).
Multipoint sockets are decoupled from specific user-space processes, are portable between hosts and network locations. Portability applied by system management according to global considerations, relies on the LISP network for on-path steering between roaming clients and elastic functional processing. Interoperable on-path scaling is achieved by application specific socket addressing scheme

Portable multipoint queues and channels abstraction:

Queue sockets assemble application frames from packets uploaded by multiple EID sources using the LISP stack through re-tunneling router (RTR) configured upon instantiation or delegation. Assembled frames are made available from socket to user space functional processing.

Channel sockets receive application frames and theme EIDs. Frames are segmented into packets and transmitted using the LISP stack via a configured RTR for delivery by signal-free (s,g) multicast [RFC8378].

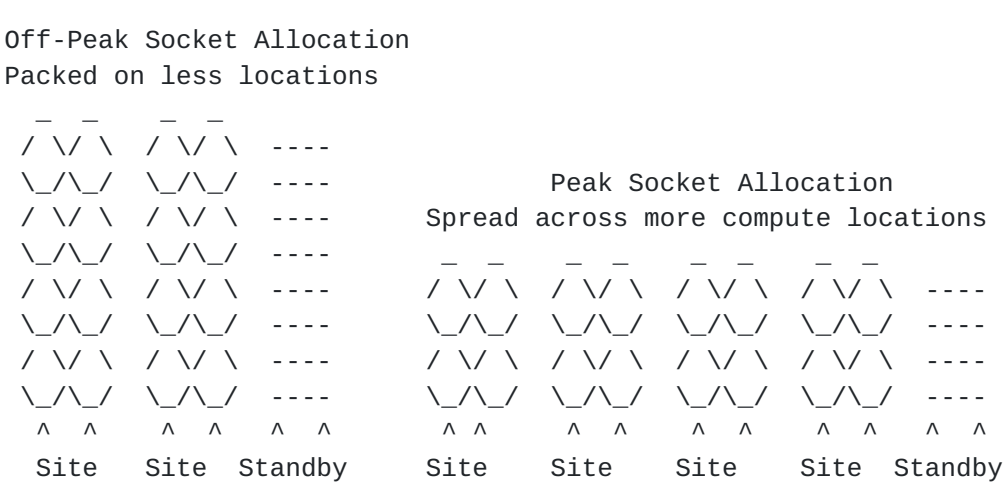

Figure 1: Dynamic allocation of sockets across locations per activity

2. Definition of Terms

Based on [RFC9300][RFC9301]

Edge Computing: a distributed computing paradigm that brings computation closer to the sources of data. This is expected to improve response times and save bandwidth. Programability of edge computing can be associated with Internet of Things (IOT) applications.

Edge Traffic Steering: Traffic steering defines the different paths that application traffic can take to traverse the network. Destination zone is also determined by these paths. In edge computing traffic steering can be used for network-based service selection.

Socket: is a software structure within a network node of a computer network that serves as an endpoint for sending and receiving data across the network. Typical Unix sockets are coupled with specific processes, however this document does not assume this model. A functional and more portable programming model may be used to access sockets structure.

EndpointIdentifier (EID): is a source and destination address of hosts in a typical LISP network. In this document EIDs are used to distinguish between socket objects regardless of the host they are instantiated in right now.

PortableQueueEID: an EID-addressable socket interface assembling point to point and multipoint to point application frames to user space from the LISP packet interface.

PortableChannelEID: an EID-addressable socket interface segmenting point to multipoint and multipoint to multipoint application frames from user space to the LISP interface.

SensorEID: the EID of a connected sensor which uploads data and media frames for curation and processing.

ClientEID: the EID of a client subscribed to a published service (EID Source, EID theme).

3. Deployment Assumptions

(1) An application defines an EID addressing scheme to facilitate the communication between Sensor and Client EIDs, and PortableQueue PortableChannel EIDs.

(2) EIDs and RTRs are assigned to SensorEIDs and ClientEIDs

(3) EIDs and RTRs are assigned to instantiated PortableQueueEIDs and PortableChannelEIDs.

(4) PortableQueueEIDs, PortableChannelEIDs are deployed across a LISP overlay network.

(5) Routing Locations (RLOC) of sensors and clients are determined by their current access anchor.

(6) Socket RLOCS are determined by the edge compute instantiation and delegation procedures

(7) Traffic is steered by LISP: from SensorEIDs to PortableQueueEIDs, and from PortableChannelEIDs to subscribed ClientEIDs.

4. Security Considerations

The LISP overlay network is inherently secure and private.
All information is conveyed using provisioned sockets.
Provisioned sockets EIDs and RLOCs configured in RTRs.
All traffic may be carried over encrypted encapsulation.

5. Privacy Considerations

Privacy and anti-tracking of clients and sensors by use of ephemeral EIDs which are configured in RTRs.

6. Acknowledgments

7. IANA Considerations

No IANA considerations.

8. 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, October 2022, <https://www.rfc-editor.org/info/rfc9301>.

[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>.

Authors' Addresses

Sharon Barkai
Nexar
CA
USA

Email: sbarkai@gmail.com

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
Technical University of Catalonia
Barcelona
Spain

Email: acabello@ac.upc.edu

Jordi Paillisse-Vilanova
Technical University of Catalonia
Barcelona
Spain

Email: jordip@ac.upc.edu

Dino Farinacci
lispers.net
San Jose, CA
USA

Email: farinacci@gmail.com