

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 4, 2018

P. Pillay-Esnault, Ed.  
Huawei  
M. Boucadair  
Orange  
G. Fioccola  
Telecom Italia  
C. Jacquenet  
Orange  
A. Nennker  
Deutsche Telekom  
July 3, 2017

Problem Statement for Identity Enabled Networks  
draft-padma-ideas-problem-statement-03

Abstract

This problem statement examines how existing protocols that separate identifiers from their location may benefit from the concept of identity. The proposal laid out herein advocates for a standardized identity/identifier network infrastructure that provides a framework to support identity services in addition to enhancing existing identifier/location mapping and resolution services.

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 <http://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 January 4, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Definition of Terms . . . . .	4
3. Key Problems . . . . .	5
3.1. Privacy . . . . .	5
3.1.1. Tracking Prevention . . . . .	5
3.1.2. Privacy against Eavesdroppers . . . . .	5
3.1.3. Identifier Right to be Forgotten . . . . .	6
3.2. Common Infrastructure and Primitives . . . . .	6
3.3. Allocation Schemes Guidance . . . . .	7
4. Scopes . . . . .	7
4.1. In Scope . . . . .	7
4.2. Out of Scope . . . . .	8
4.3. Future Studies . . . . .	8
5. Relationship between IDEAS and other IETF Working Groups . .	8
5.1. LISP WG . . . . .	9
5.2. HIP WG . . . . .	9
5.3. NVO3 WG . . . . .	9
6. Companion Documents . . . . .	9
7. Security Considerations . . . . .	9
8. IANA Considerations . . . . .	9
9. Contributors . . . . .	10
10. Acknowledgments . . . . .	10
11. Informative References . . . . .	10
Authors' Addresses . . . . .	11

## 1. Introduction

While the separation of identifier from the location is not a new concept, existing solutions such as Host Identity Protocol (HIP) [RFC7401], Location/Separation Protocol (LISP) [RFC6830] and Identifier-Locator Addressing (ILA) [ILA] for IPv6, may benefit from a higher layer abstraction that separates the identity of an entity from its associated identifier(s).

In identifier and Location split protocols, identifiers (IDf) are used for decoupling the identifier and the location information at

the network layer. Typically, a IDf represents an end-point communication tied to an entity. Usually, IDfs are long-lived and may or may not be routable. However, locators (LOC) may be transient and associated with the location of the entity. The LOCs are routable network addresses (e.g. IPv4, IPv6 addresses). The IDfs are mapped to LOCs for forwarding purposes. Modification of LOC information is handled by an a mapping system that updates the IDf/LOC mappings.

In order to communicate with a device, the initiator relies on a mapping system that is designed to process lookup requests on a network IDf and return the LOC(s). While the mapping system fulfills its functionality, this mode of operation has some drawbacks.

The entities update the system with their (IDf,LOC) bindings. In some cases, it may register the LOC of a forwarding element such as a proxy or HIP Rendezvous Server. Regardless, it is assumed that once the entities have registered their (IDf,LOC(s)) tuple to the system, this information is available to all with access to the mapping system. Any request for this information would then be readily available without any discrimination. For example, a public entity needs to have its IDf public to be discovered by clients. However, it might not be always desirable that some devices (e.g. home cameras) are visible to all without any control.

Privacy and security requirements of entities suggest the use of some mechanism to authenticate entities that can dynamically discover them and prevent unwanted communication. In existing architectures it is possible to authenticate IDf, however they are not permanently attached to the entity. This is crucial in a multi-provider and/or multi-domain scenario, related for example to a complex end-to-end service.

Therefore the concept of an identity(IDy) tied to an entity and to its lifecycle should be considered. The IDy is intended to be used for identifying and authenticating an entity. Likewise, the IDy information should not be carried in clear in packet headers. The Section 3 of this document will describe how this IDy may be used.

Furthermore, it would be beneficial to generalize this Identity concept across protocols that may benefit from it. Therefore there is a need for a system which shares some common control plane for services commonly used such as look-ups or updates.

This document examines the possible changes and improvements needed to address these challenges in Identity Enabled networks (IDEAS). It describes the problem statement and advocates for a standardized extensible common control plane for IDf/LOC protocols that supports:

Identity services (including registration and authentication)

Management of access credentials based on IDy

Look-ups with restrictions

Mapping, and resolution services on IDfs

## 2. Definition of Terms

**Entity:** An entity is a communication endpoint. It can be a device, a node, or a (software) process, that needs to be identified and locatable/reachable. Such entity will have one or more communication interfaces. An entity may have multiple IDfs simultaneously that are NOT associated with any particular interface(s). It is reached by the resolution of one or more of its IDfs to one or more LOCs.

**Identity (IDy):** The essence of "being" of a specific entity. An IDy is not to be confused with an IDf: while an IDf may be used to refer to an entity, an IDf's lifecycle is not necessarily tied to the lifecycle of the IDy it is referencing. On the other hand, the IDy's lifecycle is inherently tied to the lifecycle of the entity itself.

**Identifier (IDf):** An IDf denotes information to unambiguously identify an entity or an entity group within a given scope. An IDf is the equivalent of an End point identifier (EID) in LISP or Host Identity Tag (HIT) in HIP. It may be visible in communications.

**Locator (LOC):** A locator is a routable network address. It may be associated with an IDf and used for communication on the network layer according to LOC/IDf split principle. A LOC is the equivalent of a Routing Locator (RLOC) in LISP or an IP address in HIP.

**Metadata (META):** Data associated with an IDy and its IDfs in the framework. The metadata is to be used for storing long-lived slow changing information such as the nature of the entity (e.g. camera or phone).

**IDy/IDf mapping:** One IDy may be associated to multiple IDfs. The IDfs are mapped to one IDy.

**Identifier-based:** When an entity is only reachable through one or more communication access then a protocol or a solution is said to

be identifier-based if it uses an ID-LOC decoupling and a mapping system (MS) as base components of the architecture.

Generic Identity Services (GRIDS): GRIDS is a set of services to manage the lifecycle of ID[y|f]s, to map and resolve IDfs and LOCs, and to associate META with entities. It is a distributed system that stores the IDy, IDf, the associated LOC(s), and META in the form of tuples (ID, LOC, and META). Meta queries are supported and queries are restricted to authenticated and authorized IDys.

Identity Enabled Networks (IDEAS): IDEAS are networks that support the IDf/IDy decoupling as well as IDf /LOC decoupling using GRIDS. Reaching an entity is achieved by the resolution of IDf(s) to LOC(s).

Scope: Domain of applicability or usability of an IDfs and IDys. The scope may be global or limited, e.g., considered local with geographic proximity or private within an administrative domain.

### 3. Key Problems

#### 3.1. Privacy

##### 3.1.1. Tracking Prevention

Access to a mapping system may reveal the location and other sensitive information about an entity to the requestor of a look-up on an IDf. Repeated look-ups on the mapping system may be misused for tracking IDfs of an entity or mount an attack.

To preserve its privacy, the entity or infrastructure may restrict access for look-ups for certain IDfs or IDys or entity with specific meta. (E.g. nature of an entity stored in meta as a camera).

Currently, even if look-ups on the mapping systems were modified not to return a result if the requestor is barred, it would be easily defeated if the requestor changes its IDf. However, if all IDfs of an entity are associated with the IDy, then the requestor entity cannot easily defeat the aforementioned filtering rule by just changing its IDf.

##### 3.1.2. Privacy against Eavesdroppers

Eavesdroppers may observe the traffic and deduce the flows between two IDfs or entities. To protect its privacy, an entity may choose additional temporary IDfs for communications.

However, this mechanism makes discovery difficult and the entity must at least have a long-lived IDf for this purpose.

The use of obfuscation is another solution to protect the source and destination IDf however this implies extra processing or DPI for functionalities such as late binding.

The use of IDy as an indirection to the actual IDfs used on the wire present the advantage of having the source and destination ephemeral IDfs in clear but authorized use may still maps these to the IDy. The IDy of an entity must not be revealed in packets. Therefore, encrypting the control plane mechanisms (requests and replies) is required to avoid eavesdroppers to deduce who are the peers of communication flows.

### 3.1.3. Identifier Right to be Forgotten

The control of the IDy/IDf mappings can restrict access to selected requesting IDys/IDfs and also limit that access over time to implement an "identifier right to be forgotten".

The advantage of this method is that entities may use IDfs for communication to better protect their IDy. Only authorized communication partners can find out the corresponding IDys. The concept of IDy proposed by IDEAS helps to provide privacy in communication in a similar way as IPv6 privacy extension minimizes the risk of being tracked by a stable MAC address. To that end, access restriction is needed for mapping system requests that also need to be encrypted to avoid eavesdropping.

### 3.2. Common Infrastructure and Primitives

Currently, each of the IDf-based protocols uses its own specific mapping databases. While IDf-based data plane mechanisms may serve fundamentally different objectives and may not need to interoperate, there is a potential benefit in providing them with a common interface for common services such as IDy/IDf registration, discovery, update, resolution and access control policy. Furthermore, the lack of a common infrastructure with standardized invocation interfaces has the following downsides:

- a. An impediment for the deployment of IDf-based. Indeed, it would be inefficient to deploy several specialized mapping/ resolution network databases within the same administrative domain. Furthermore, there will be additional expense and overhead to administer multiple proprietary mapping systems.

- b. Difficulty to have an overall view of the network. If multiple IDf-based solutions with distinct mapping systems are deployed, troubleshooting may be difficult as the information may be located in different places.
- c. Complex Management due to disjoint information spread over several mapping systems. Operations such as merging networks are error prone and more challenging to detect and fix. Additionally, there will be considerable management overhead whenever devices migrate.
- d. Barriers to the enforcement of common and consistent policies. For example, in cross-platform IoT networking, brokering services may be needed to enforce routing/security/QoS/TE policies on behalf of partnering structures - service provider, energy provider, content provider, etc.

The common infrastructure may be supported within limited or private scopes. In addition support of private instances provides the necessary separation for specific users or applications.

### 3.3. Allocation Schemes Guidance

Currently, there is no consistent guidance or allocation scheme for non-IP address format public IDfs across all protocols. Each protocol has historically assigned their IDfs independently, be it structured or not. An agreed scheme or a collision detection mechanism within a scope may facilitate cross-domain communication in the future. This would simplify the implementation of some use cases to facilitate cross-silo communications or to better address the merging of networks.

The support of several allocation schemes by carving specific ranges within a name space and recycling should be explored for the future mapping systems. The operations and ease of deployment should also be considered as they may influence policy enforcement schemes related to the allocation of IDfs of the use of relevant META.

## 4. Scopes

### 4.1. In Scope

The scope of this work is on the network layer (layer 3). The network identities that may be alphanumeric are assumed to map to numerical IDfs as in LISP, HIP or ILA. The LOCs are assumed to be IPv4 or IPv6 addresses.

The META is assumed to be tied to the IDy or IDf and slow changing.

While the issues described in the document may be generalized to a broader scope, IDEAS is focused on delivering functionalities at the network layer only.

#### 4.2. Out of Scope

The following are out of scope for this effort:

- o The resolution or mapping of domain names or any application level naming or directories (like URIs ...).
- o META information with rapid changes

#### 4.3. Future Studies

Other network addressing schemes may be considered for future studies.

### 5. Relationship between IDEAS and other IETF Working Groups

This document is meant to encourage the IETF community to investigate the opportunity of a new specification effort to address some specific problems from an IDy Enabled Networks standpoint in general. The focus is to find a common solution and infrastructure that can be shared by current protocols and facilitate the introduction of new IDy-based services while avoiding rehashing the same problems again each time a new service pops up.

We propose to address these problems with a GeneRic IDentity Services (GRIDS) infrastructure which includes standardized access and multiple services. The services include secured registration, discovery, updates with data integrity, mapping and resolution capabilities, define relationships between identities or group of identities, access control policy and security.

Some other working groups are already working to address some specific limitations or enhancement of identifier-based protocols but do not take IDy requirements as highlighted in this document into consideration. These working groups include LISP, HIP and NVO3.

Protocols and architectures defined by these WGs may assume a mapping system or other resolution techniques, but they are not currently covering the other services mentioned in this document.



### 5.1. LISP WG

The LISP WG has been working on multiple mapping systems (ALT, DDT) for the LISP control plane and the primary function of this mapping system is to map and resolve the IDf to IP addresses (EID/RLOC mapping). LISP WG is also looking at Cassandra and blockchain. Though some requirements are common, GRIDS has new specific requirements described in [IDEAS-REQ].

### 5.2. HIP WG

The HIP WG has based its IDy to IDf resolution service on DNS. Operational IDf to Loc for fast mobility with low latency is handled by HIP-RVS [RFC8005] and specific HIP Mobility Notification messaging [RFC8046].

### 5.3. NVO3 WG

The NV03 WG has been working on a mapping of VN names to VN IDs in the network virtualization space and their requirements differ from the wireless broadband requirements and cross-silo communications that have been mentioned in this document.

## 6. Companion Documents

There are three companion documents:

- o Use Cases for Identity Enabled Networks [IDEAS-USE]
- o Requirements for Generic Identity Services in Identity Enabled Networks [IDEAS-REQ]
- o Identity Use Cases in IDEAS [IDEAS-IDY]
- o Gap Analysis for Identity Enabled Networks [IDEAS-GAP]

## 7. Security Considerations

Due to the sensitivity of IDy tied to IDf and LOC, there is a need to pay attention to security ramifications. In particular, the security goals should include confidentiality, possible encryption for integrity of sensitive data and privacy.

## 8. IANA Considerations

This document has no actions for IANA.

## 9. Contributors

The following individuals (by first name alphabetical order) have contributed to this document:

- o Albert Cabellos
- o Alex Clemm
- o Dino Farinacci
- o Georgios Karagiannis
- o Jim Guichard
- o Michael Menth
- o Robert Moskowitz
- o Tom Herbert
- o Uma Chunduri

This present document is based on an extract of the first version of the draft. The authors and their affiliations on the original document are: D. Farinacci (lispers.net), D. Meyer (Brocade), D. Lake (Cisco Systems), T. Herbert (Facebook), M. Menth (University of Tuebingen), Dipenkar Raychaudhuri (Rutgers University) and Julius Mueller (ATT).

## 10. Acknowledgments

The authors would like to thank Stewart Bryant, David Lake, Bingyang Liu, Dave Meyer, Dipenkar Raychaudhuri, Yingzhen Qu, and Onur Ozan Koyluoglu for their review and input on this document. The authors would like to thank Jean-Michel Esnault, Renwei Li, Lin Han, Kiran Makhijani Erik Nordmark, Burjiz Pithawala, and Jeff Tansura who participated in numerous discussions.

This document was produced using Marshall Rose's xml2rfc tool.

## 11. Informative References

[IDEAS-GAP]

Qu, Y., Cabellos, A., Moskowitz, R., Liu, B., and A. Stockmayer, "Identity Use Cases in IDEAS", July 2017, <<https://tools.ietf.org/html/draft-xyz-ideas-gap-analysis-00/>>.

- [IDEAS-IDY] Chunduri, U., Clemm, A., and M. Menth, "Identity Use Cases in IDEAS", June 2017, <<https://tools.ietf.org/html/draft-ccm-ideas-identity-use-cases-00/>>.
- [IDEAS-REQ] Pillay-Esnault, P., Clemm, A., Farinacci, D., and D. Meyer, "Requirements for Generic Resilient Identity Services in Identity Enabled Networks", March 2017, <<https://datatracker.ietf.org/doc/draft-padma-ideas-req-grids/>>.
- [IDEAS-USE] Pillay-Esnault, P., Farinacci, D., Herbert, T., Jacquenet, C., Lake, D., Menth, M., Meyer, D., and D. Raychaudhuri, "Use Cases for Identity Enabled Networks", March 2017, <<https://datatracker.ietf.org/doc/draft-padma-ideas-use-cases-00/>>.
- [ILA] Herbert, T., "Identifier-locator addressing for network virtualization", March 2016, <<https://datatracker.ietf.org/doc/draft-herbert-nvo3-ila/>>.
- [RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <<http://www.rfc-editor.org/info/rfc6830>>.
- [RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <<http://www.rfc-editor.org/info/rfc7401>>.
- [RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <<http://www.rfc-editor.org/info/rfc8005>>.
- [RFC8046] Henderson, T., Ed., Vogt, C., and J. Arkko, "Host Mobility with the Host Identity Protocol", RFC 8046, DOI 10.17487/RFC8046, February 2017, <<http://www.rfc-editor.org/info/rfc8046>>.

Authors' Addresses

Padma Pillay-Esnault (editor)  
Huawei  
2330 Central Expressway  
Santa Clara, CA 95050  
USA

Email: padma.ietf@gmail.com

Mohamed Boucadair  
Orange  
Rennes 35000  
France

Email: mohamed.boucadair@orange.com

Giuseppe Fioccola  
Telecom Italia

Email: giuseppe.fioccola@telecomitalia.it

Christian Jacquenet  
Orange  
Rennes 35000  
France

Email: christian.jacquenet@orange.com

Axel Nennker  
Deutsche Telekom

Email: Axel.Nennker@telekom.de

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 4, 2018

Y. Qu, Ed.  
Huawei  
A. Cabellos  
Technical University of Catalonia  
R. Moskowitz  
HTT Consulting  
B. Liu  
Huawei  
A. Stockmayer  
University of Tuebingen  
July 3, 2017

Gap Analysis for Identity Enabled Networks  
draft-xyz-ideas-gap-analysis-00

Abstract

Currently there are several identifier/locator separation protocols, such as HIP, ILA, ILNA and LISP. This document analyzes the technical gaps between existing solutions and today's privacy requirements.

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 <http://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 January 4, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Specification of Requirements . . . . .	3
3. Definition of Terms . . . . .	3
4. Overview of ID/LOC Protocols . . . . .	4
4.1. LISP . . . . .	4
4.2. HIP . . . . .	5
4.3. ILA . . . . .	6
5. Gap Analysis . . . . .	6
5.1. The Split of Identity and Identifier . . . . .	6
5.2. A Common Identifier-to-Locator Mapping System . . . . .	7
5.3. User-Defined Access Policies in the Mapping System . . . . .	7
6. Analysis of DNS . . . . .	7
7. Security Considerations . . . . .	8
8. IANA Considerations . . . . .	8
9. Contributors . . . . .	8
10. Acknowledgments . . . . .	8
11. References . . . . .	8
11.1. Normative References . . . . .	8
11.2. Informative References . . . . .	10
Authors' Addresses . . . . .	11

## 1. Introduction

The separation of location and identifier has been discussed for many years, as documented in [RFC4984]. IP addresses have been overloaded to serve as both locators and identifiers. Several identifier and locator separation (ID/LOC) protocols have been proposed, such as HIP [RFC7401], [ILA] and LISP [RFC6830]. They create two separate namespaces: identifiers (IDs) and Locators (LOCs). Identifiers uniquely identify network entities no matter where they are located, and locators are assigned based on topology information and are typically routable.

In an ID/LOC protocol, a service is needed to maintain mappings between identifiers and locators and to perform lookups from identifiers to locators (and probably vice-verse). Currently each ID-based protocol uses its own mapping database and mechanism to get this mapping information [RFC6836][RFC8005].

As pointed out by [IDEAS-PS][IDEAS-IDY-USE], the concept of identity (IDy) tied to a network entity can help to solve some of the privacy issues that are associated with today's networks. The goal of this document is to analyze the technical gaps between the existing ID/LOC protocols and today's requirements. The following gaps are summarized: the split of identifier and identity; a common mapping system supporting both IDf/LOC mapping and IDy/IDf mapping; and user-defined access policies.

## 2. Specification of Requirements

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].

## 3. Definition of Terms

This document makes use of the terms that have been already defined in the problem statement draft of IDEAS [IDEAS-PS]. They are included here for reader's convenience. In case of any discrepancies between the two drafts, the problem statement draft overrides.

**Entity:** An entity is a communication endpoint. It can be a device, a node, or a virtual machine (VM), that needs to be identified. An entity may have one or multiple identifiers (long-lived or ephemeral) simultaneously. An entity is reached by the resolution of one or more of its identifiers to one or more locators.

**Identity (IDy):** the essence of "being" of a specific entity. An identity is not to be confused with an identifier: while an identifier may be used to refer to an entity, an identifier's lifecycle is not necessarily tied to the lifecycle of the Identity it is referencing. On the other hand, the identity's lifecycle is inherently tied to the lifecycle of the entity itself.

**Identifier (IDf):** denotes information to unambiguously identify an entity within a given scope (e.g. HIP HIT, LISP EID). There is no constraint on the format, obfuscation or routability of an IDy. The IDy may or may not be present in the packet whose format is defined by ID-based protocols (HIP/LISP).

**Identifier-based (ID-based):** When an entity is only reachable through one or more communication access then a protocol or a solution is said to be ID-based if it uses an ID-LOC decoupling and a mapping system (MS) as base components of the architecture. Examples of ID-based protocols are HIP, LISP and ILA.

Identity Enabled Networks (IDEAS): IDEAS are networks that support the identifier/locator decoupling. Reaching an entity is achieved by the resolution of identifier(s) to locator(s).

Locator (LOC): denotes information that is topology-dependent and which is used to forward packets to a given entity attached to a network (IPv4/IPv6/L2/L2.5 Address). An entity can be reached using one or multiple locators; these locators may have a limited validity lifetime.

ID/LOC: Identifier and Locator Separation.

LISP: Locator/ID Separation Protocol.

HIP: Host Identity Protocol.

ILNP: Identifier-Locator Network Protocol.

ILA: Identifier-Locator Addressing.

DNS: Domain Name System.

#### 4. Overview of ID/LOC Protocols

##### 4.1. LISP

The Locator/ID Separation Protocol (LISP) [RFC6830] is structured around four main components: the data plane, the control plane (both specified in [RFC6830]), the LISP Mapping System Interface [RFC6833] and the Mapping System (e.g., LISP-DDT [RFC8111] and LISP+ALT [RFC6836]).

The LISP architecture decouples identifier and locator by means of the mapping system interface. This well-defined interface separates data/control from the mapping system architecture. As a result, LISP does not assume any mapping system architecture. The LISP WG has, at the time of this writing, specified two mapping systems: LISP-DDT [RFC8111] and LISP-ALT [RFC6836].

Both mapping system assume hierarchical identifiers, but the WG has explored other architectures such as DHT for flat identifiers, or monolithic mapping systems.

One of the main design principles behind LISP is to decouple the identifier (EIDs) from the locators (RLOCs). By means of the LISP Canonical Address Format (LCAF) [RFC8060] LISP provides a flexible syntax to encode both EIDs and RLOCs.



In terms of security, LISP supports authorization for mapping updates and the authentication of the clients updating such information. This is achieved by means of the authentication data field in the Map-Register message. In addition, LISP clients can verify the security of data origin, authentication and delegation. This is specified in [LISP-SEC] and the security mechanisms incorporated in LISP-DDT [RFC8111].

#### 4.2. HIP

The Host Identity Protocol (HIP) [RFC7401] is a SIGMA-security compliant exchange of current entity location for a pair of cryptographically ownership provable Identifiers (HITs). HIP is, at its inception, focused on the management of the Identifier/Location mapping. HITs are valid, non-routable IPv6 addresses that carry the cryptographic protocol suite and a hash of the HI (Host Identity public key).

One method of discovery of a peer's HIT and initial location is either via DNS RR 55 [RFC8005] with A|AAAA RR to the peer or A|AAAA RR pointing to the peer's Rendezvous Service (RVS) server [RFC8004]. The Initiating peer cannot detect from DNS the difference in destination. The RVS server "slingshots" the I1 packet to the recipient. The recipient decides, based on local policy, to respond with the next exchange packet, R1. Thus using an RVS server not only supports client mobility, it also hides a peer's location unless it wants to be 'found'.

HIP provides Identity/Location separation through changes in the peer IP stack behavior with only needing RVS added to the infrastructure. HIP aware systems register to their RVS server(s) via a HIP exchange, augmented with an RVS registration parameter [RFC8003]. All location changes are made securely over HIP [RFC8046]. Location changes are sent directly to peers and to the RVS server(s). HIP fully supports double jumps (both peers move) and state lose recovery (full protocol state machine).

HIP supports multihomed systems [RFC8047], fully decoupling Identifier (HITs) from all interfaces. Multiple data-paths are enabled with HIP. ESP via BEET mode [rfc7402] is most commonly used. L2VPNs support is defined in [HIP-VPLS] and provided in commercial products targeting SCADA environments. A non-cryptographic envelope is proposed [HIP-IP].

HIP works equally well over IPv4 or IPv6 networks. The HIP data-path can be either IPv4 (via the HIP 32-bit Local Scope Identifier) or IPv6 using the HIT. IPv4 applications can run transparently over IPv6 and IPv6 over IPv4.

HIP well supports Identifiers to location, and weakly Identity to Identifiers. Besides DNS support, identities may be supported in HIP with X.509 certificates [rfc8002] to provide 3rd party assertions of HITs and HIs. Identifiers to Identity reversal is poorly handled, though potentially needed for support of FTP PASV and other protocols with embedded addresses. DHT has been demonstrated [RFC6537], but not fielded. The new work on Hierarchical HITs [HHIT] proposes new methods to couple DNS and a registry for the reverse lookup.

#### 4.3. ILA

In [ILA], an IPv6 address is divided into two parts: a locator and an identifier. As other ID/LOC protocol, the locator indicates the topological location of a network entity, and the identifier identifies the entity in communications. ILA can be used to implement overlay networks for network virtualization, and also addresses use cases in mobility.

However, the mapping service in ILA is still TBD [ILA-MS-TBD].

### 5. Gap Analysis

#### 5.1. The Split of Identity and Identifier

In existing ID/LOC Protocols, the IDf/LOC mappings stored in the mapping system are assumed to be public. A legitimate requestor can lookup any record, and escape access control policy, if there is any, by changing to a different identifier. Also a network entity may want to hide its true identity for privacy protection by using ephemeral identifiers [LISP-ANNOY].

To address these issues, [IDEAS-PS] introduces the concept of identity (IDy). An IDy uniquely identifies "who" is a communication entity. Identifier and locator together identifies "where" is the entity. With this 2-tier identification, multiple identifiers can be bound to the same entity (IDy) and exchanged in clear on the wire, without having to worry about the identity being compromised by outside observers.

Since the lifecycle of an identity is the same as the entity, the lifecycles of identity and its associated identifiers are decoupled. It is possible for identifiers to be added or removed without affecting the identity. This further abstraction can bring additional benefits. [IDEAS-IDY-USE] describes the identity use cases.

In summary:

- o The notion of identity is not adequately supported.
- o Two tiers of identification are needed, with identifiers anchored at the identity.

## 5.2. A Common Identifier-to-Locator Mapping System

IDf/LOC mapping service is essential for ID/LOC protocols [RFC6833], however now each protocol is using its own mapping database even within the same administrative domain. This potentially adds additional operational cost and management complexity.

A common mapping system supporting both IDf/LOC mapping and IDy/IDf mapping can work with existing ID/LOC protocols, as well as add extra identity based services. It can provide consistent access control, common interface for services such as registration, discovery and resolution. A unified database can help to ease network management [IDEAS-PS].

## 5.3. User-Defined Access Policies in the Mapping System

Different from DNS, which generally maintains public name-to-IP mapping information, an IDf/LOC mapping system maintains more private information. However existing mapping systems assume the information stored is public, and this may cause privacy violation. A network entity may want to set a customized access policy to control who can get its identifier and location information. This policy should be tied to identity, so it is not affected by identifier changes of the requestor.

General system-wide access control (e.g., an operator can set a system-wide access control list for a DNS server, only permitting the customer network prefixes to access it) can provide some privacy, but it is not sufficient. What is needed are: fine-grained level of access control at the level of data records associated with each individual entity; and reinforcement of the access policies.

## 6. Analysis of DNS

Since the 1980s, DNS has been pivotal to translate human readable names that are easy to remember into hard-to-remember IP addresses. It provides a global distributed directory service and is a very powerful and useful technology to translate the domain name hierarchy to IP address space.

Even though the DNS was designed to be resilient, it is prone to DDOS attacks as discussed extensively in the Technical Plenary of IETF97. Furthermore, some studies have also described challenges in the

response time and caching techniques and latency in the Internet [DNS1] [DNS2] [DNS3] [GNRS].

[DNS-DUP] proposed a mobility solution using DNS dynamic updating protocol. However for a communication session when both hosts are moving, the session fails and the hosts SHOULD query DNS and get the new address and then restart the communications.

The use of a mapping system rather than using DNS system has been discussed extensively in [IVIP], [RFC6115], on the lisp-wg mailing list [LISP-DIS], and initial HIP design team (circa 1999-2003).

## 7. Security Considerations

IDEAS control plane may be used to maintain and transmit confidential data, such as identity, access policy and metadata. Access to the data needs to be authorized/authenticated. Control plane messages containing such data need to be encrypted. The exact details of encryption/authentication are topics for future research.

## 8. IANA Considerations

This document has no actions for IANA.

## 9. Contributors

TBD.

## 10. Acknowledgments

The authors would like to thank Dino Farinacci, Michael Menth, Padma Pillay-Esnault, Alex Clemm, Uma Chunduri for their review and input on this document.

This document was produced using Marshall Rose's xml2rfc tool.

## 11. References

### 11.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC6115] Li, T., Ed., "Recommendation for a Routing Architecture", RFC 6115, DOI 10.17487/RFC6115, February 2011, <<http://www.rfc-editor.org/info/rfc6115>>.

- [RFC6537] Ahrenholz, J., "Host Identity Protocol Distributed Hash Table Interface", RFC 6537, DOI 10.17487/RFC6537, February 2012, <<http://www.rfc-editor.org/info/rfc6537>>.
- [RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <<http://www.rfc-editor.org/info/rfc6830>>.
- [RFC6833] Fuller, V. and D. Farinacci, "Locator/ID Separation Protocol (LISP) Map-Server Interface", RFC 6833, DOI 10.17487/RFC6833, January 2013, <<http://www.rfc-editor.org/info/rfc6833>>.
- [RFC6836] Fuller, V., Farinacci, D., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT)", RFC 6836, DOI 10.17487/RFC6836, January 2013, <<http://www.rfc-editor.org/info/rfc6836>>.
- [RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <<http://www.rfc-editor.org/info/rfc7401>>.
- [RFC7402] Jokela, P., Moskowitz, R., and J. Melen, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)", RFC 7402, DOI 10.17487/RFC7402, April 2015, <<http://www.rfc-editor.org/info/rfc7402>>.
- [RFC8003] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Registration Extension", RFC 8003, DOI 10.17487/RFC8003, October 2016, <<http://www.rfc-editor.org/info/rfc8003>>.
- [RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004, October 2016, <<http://www.rfc-editor.org/info/rfc8004>>.
- [RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <<http://www.rfc-editor.org/info/rfc8005>>.
- [RFC8046] Henderson, T., Ed., Vogt, C., and J. Arkko, "Host Mobility with the Host Identity Protocol", RFC 8046, DOI 10.17487/RFC8046, February 2017, <<http://www.rfc-editor.org/info/rfc8046>>.

- [RFC8047] Henderson, T., Ed., Vogt, C., and J. Arkko, "Host Multihoming with the Host Identity Protocol", RFC 8047, DOI 10.17487/RFC8047, February 2017, <<http://www.rfc-editor.org/info/rfc8047>>.
- [RFC8060] Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", RFC 8060, DOI 10.17487/RFC8060, February 2017, <<http://www.rfc-editor.org/info/rfc8060>>.
- [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, <<http://www.rfc-editor.org/info/rfc8111>>.

## 11.2. Informative References

- [DNS-DUP] Yahya, B. and J. Ben-Othman, "Achieving host mobility using DNS dynamic updating protocol", October 2008, <<http://ieeexplore.ieee.org/document/4664258/>>.
- [DNS1] Jung, J., Sit, E., Balakrishnan, H., and R. Morris, "DNS Performance and the Effectiveness of Caching", 2002, <<http://nms.lcs.mit.edu/papers/dns-ton2002.ps>>.
- [DNS2] Liston, R., Srinivasan, S., and E. Zegura, "DNS Performance and the Effectiveness of Caching", 2002, <<http://www.cc.gatech.edu/fac/Ellen.Zegura/papers/dnsdiversity.pdf>>.
- [DNS3] Briscoe, B., Anna Brunstrom, A., Andreas Petlund, A., David Hayes, D., David Ros, D., Ing-Jyh Tsang, I., Stein Gjessing, S., Gorry Fairhurst, G., Carsten Griwodz, C., and M. Michael Welzl, "Reducing Internet Latency: A Survey of Techniques and their Merits", November 2014, <<http://ieeexplore.ieee.org/document/6967689/>>.
- [GNRS] Karimi, P. and S. Mukherjee, "Global Name Resolution Service", March 2017, <<https://datatracker.ietf.org/doc/draft-karimi-ideas-gnrs/>>.
- [HHIT] Moskowitz, R., Xu, X., and B. Liu, "Hierarchical HITs for HIPv2", June 2017, <<https://datatracker.ietf.org/doc/draft-moskowitz-hierarchical-hip/>>.
- [HIP-IP] Moskowitz, R., Xu, X., and B. Liu, "Encapsulation of IP within IP managed by HIP", June 2017, <<https://datatracker.ietf.org/doc/draft-moskowitz-hip-IPnHIP/>>.

- [HIP-VPLS] "HIP-based Virtual Private LAN Service (HIPLS)", February 2017, <<https://datatracker.ietf.org/doc/draft-henderson-hip-vpls/>>.
- [IDEAS-IDY-USE] "Identity Use Cases in IDEAS", June 2017, <<https://datatracker.ietf.org/doc/draft-ccm-ideas-identity-use-cases/>>.
- [IDEAS-PS] "Problem Statement for Identity Enabled Networks", March 2017, <<https://datatracker.ietf.org/doc/draft-padma-ideas-problem/>>.
- [ILA] Herbert, T., "Identifier-Locator Addressing for Network Virtualization", March 2016, <<https://datatracker.ietf.org/doc/draft-herbert-nvo3-ila/>>.
- [ILA-MS-TBD] Herbert, T., "Re: [Ideas] A comment on the use case draft", March 2017, <<https://www.ietf.org/mail-archive/web/ideas/current/msg00081.html>>.
- [IVIP] Whittle, R., "Ivip (Internet Vastly Improved Plumbing) Architecture", September 2010, <<https://tools.ietf.org/html/draft-whittle-ivip-arch-04>>.
- [LISP-ANNOY] "LISP EID Anonymity", April 2017, <<https://datatracker.ietf.org/doc/draft-farinacci-lisp-eid-anonymity/>>.
- [LISP-DIS] "LISP Discussion", <<https://www.ietf.org/mail-archive/web/lisp/current/msg03733.html>>.
- [LISP-SEC] Maino, F., Ermagan, V., Cabellos, A., Saucez, D., and O. Bonaventure, "LISP-Security (LISP-SEC)", Work in Progress, October 2012.

## Authors' Addresses

Yingzhen Qu (editor)  
Huawei  
2330 Central Expressway  
Santa Clara, CA 95050  
USA

Email: yingzhen.qu@huawei.com

Albert Cabellos  
Technical University of Catalonia  
C/ Jordi Girona s/n  
Barcelona 08034  
Spain

Email: acabello@ac.upc.edu

Robert Moskowitz  
HTT Consulting  
Oak Park, MI 48237  
USA

Email: rgm@labs.htt-consult.com

Bingyang Liu  
Huawei  
156 Beiqing Rd  
Beijing 100095  
China

Email: liubingyang@huawei.com

Andreas Stockmayer  
University of Tuebingen  
room B305, Institute of Computer Science  
Tuebingen 72076  
Germany

Email: andreas.stockmayer@uni-tuebingen.de