Network Working Group   P. Pillay-Esnault, Ed.
Internet-Draft   Huawei
Intended status: Informational   M. Boucadair
Expires: January 4, 2018   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

Copyright Notice

Table of Contents

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 alphanumerical 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 Casssandra 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