Problem Statement for IDentity EnAbled networkS

draft-padma-ideas-problem-statement-03

P. Pillay-Esnault padma@huawei.com
M. Boucadair mohamed.boucadair@orange.com
C. Jacquenet christian.jacquenet@orange.com
G. Fioccola giuseppe.fioccola@telecomitalia.it
A. Nennker axel.nennker@telekom.de
& all contributors

Motivation

What we have:

- Successful network evolving
- Increasing access diversity
- Increasing device diversity
- Ubiquitous mobility is a given
- Identifier/Locator split protocols

What Users want:

- Privacy
- Access Control
- Personalized context-aware features

Motivation

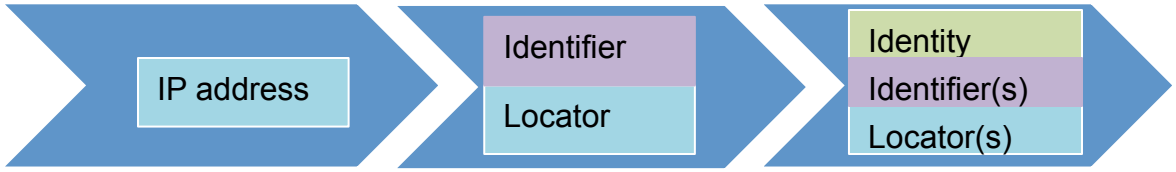
What operators want:

- Operational and deployment simplicity

What we propose:

- IDEAS goal is to facilitate delivering some of these asks
- Deliver a flexible framework
- Introduce Identity-Identifier Split

Identity-Identifier Split

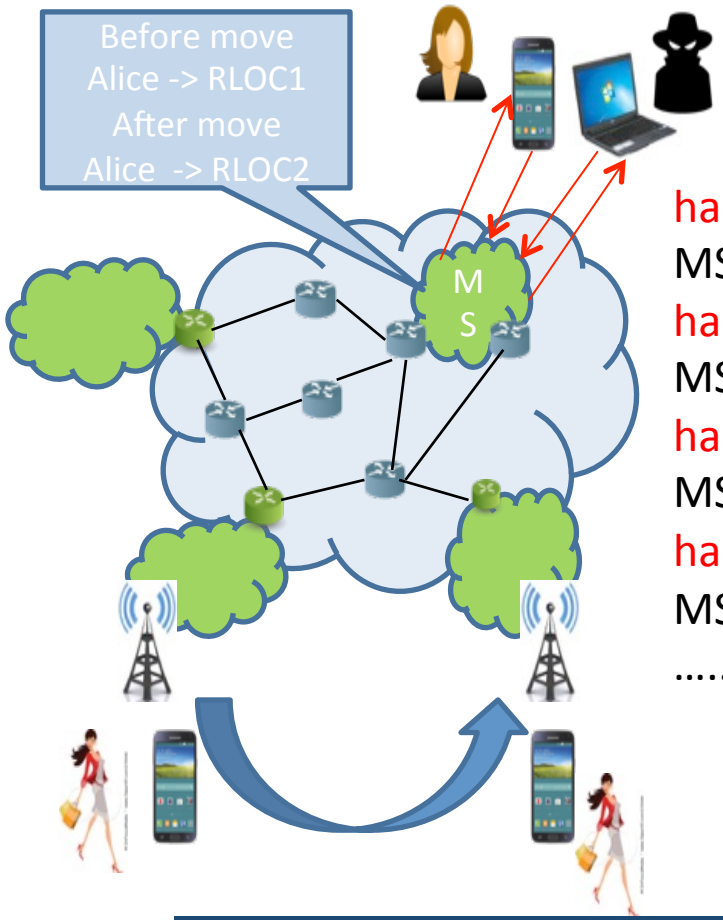


	Identity	Identifier
	Unique per entity	Multiple per entity associated with the identity
On the wire	Never revealed	May be in clear

Identity is an enabler:

- Implementing the lookup access control without being easily defeated
- Protecting privacy of flows to eavesdroppers
- Immutable but erasable external representation (identifier)
- Simple policies based on Identity
- Features based on Identity

Privacy: Who is looking for me?



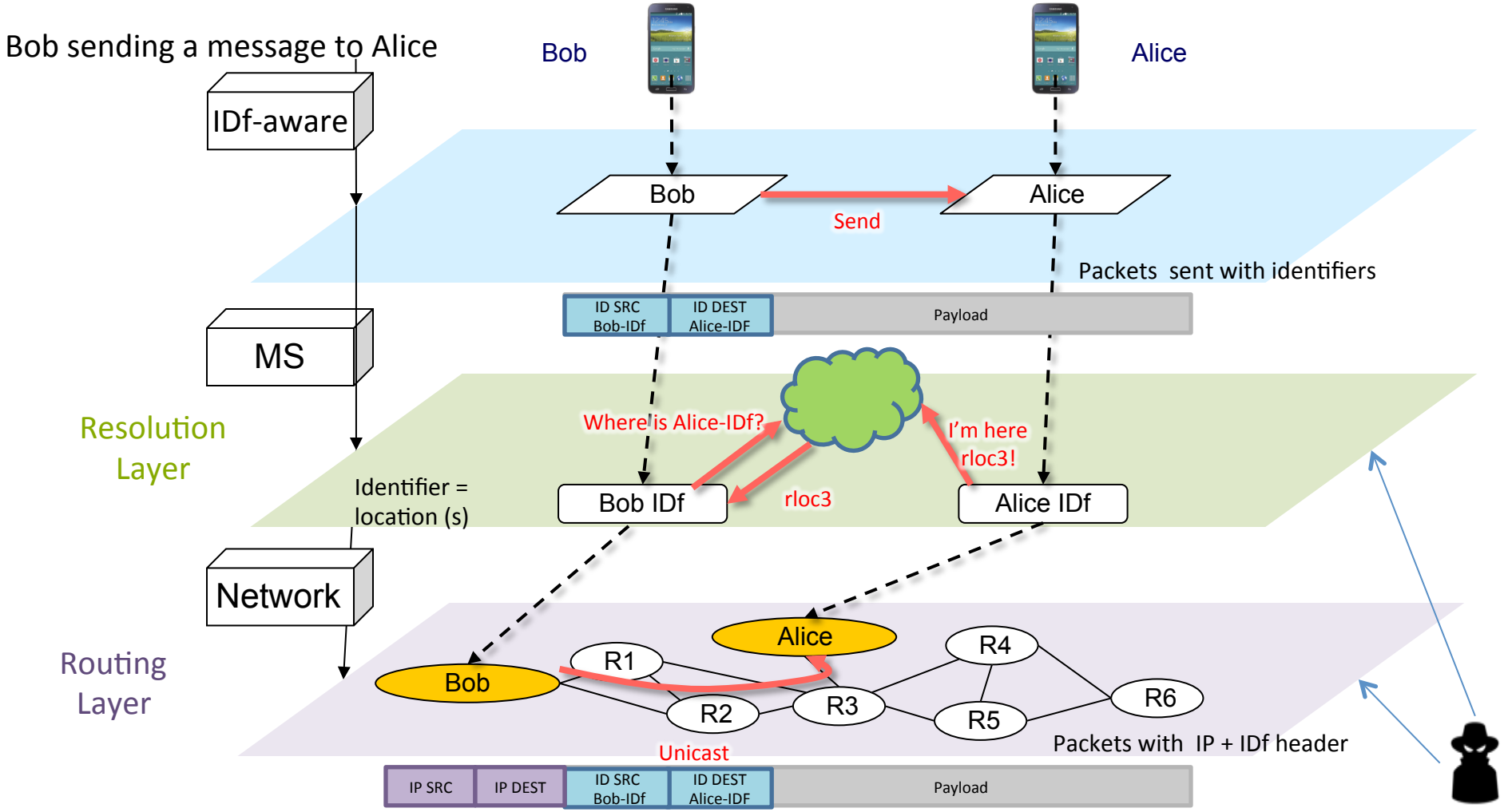
hacker->Where is Alice?
MS-> rloc1
hacker->Where is Alice?
MS-> rloc1
hacker-> Where is Alice?
MS-> rloc2
hacker-> Where is Alice?
MS-> rloc2
…..

Mapping Systems
Great!
One single IDf everywhere
My friends can find me!

Oh but is that really so great??
My IDf means me it is public
Anyone can look me up
Anyone can track me
No privacy!
Easy to defeat control by changing identifier

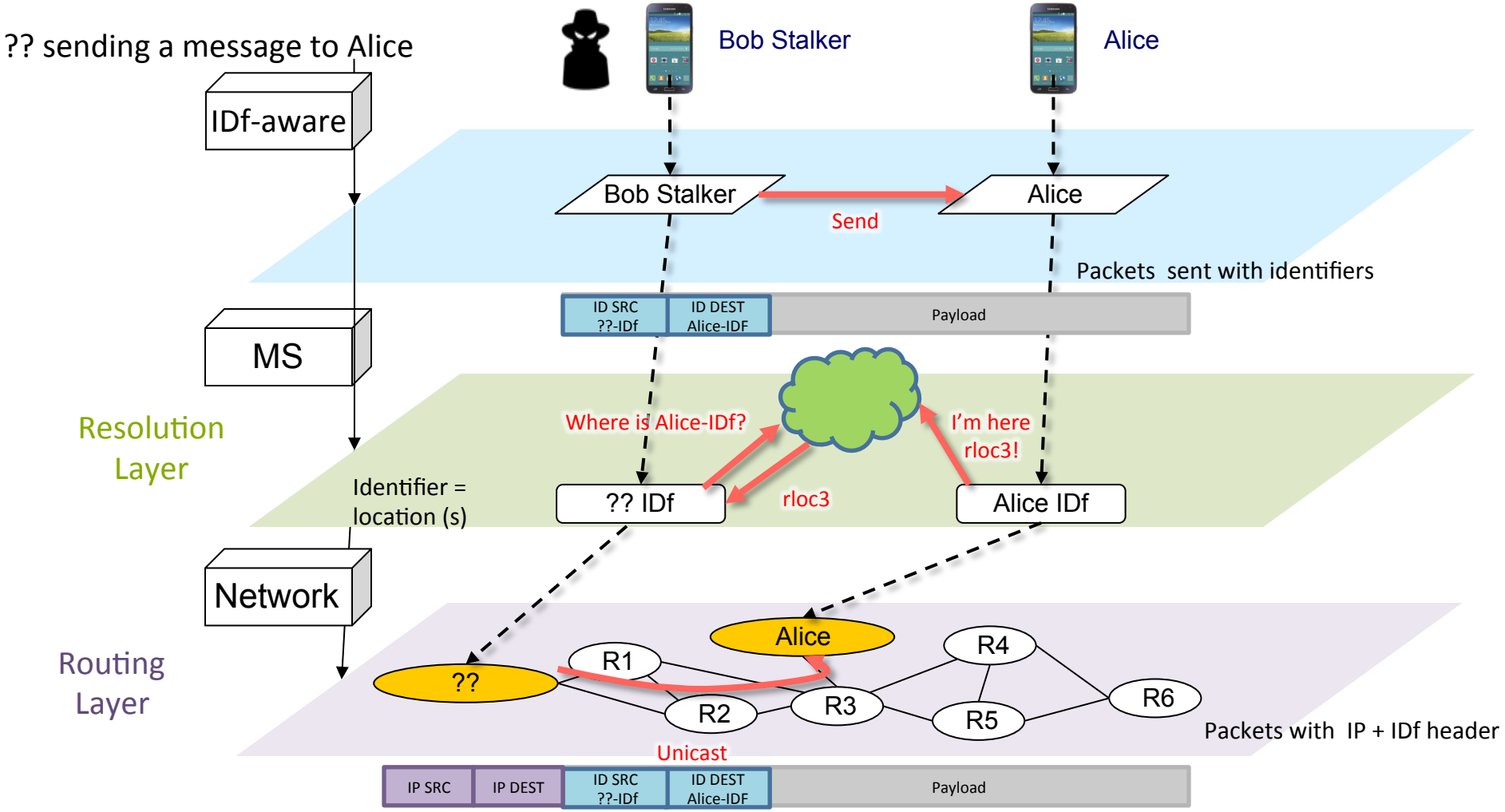
Access control need to be tied to identity
Identifiers are associated with Identity
Balance between long lived identifier for discovery vs privacy

Privacy: Protection against Eavesdroppers



Meaningless clear identifiers to Eavesdroppers
Access Control look up
Tradeoff between encryption and new features based on ID context-awareness

Privacy: Long Lived Identifier – Delete?



Identifiers can be abused by legitimate previous peers
Need erasable external representations of Identity
Finding a balance between identity lifecycle and external view

Lack of Common Infrastructure and Primitives

Diversity of devices

- One solution may not fit all
- Multiple systems?

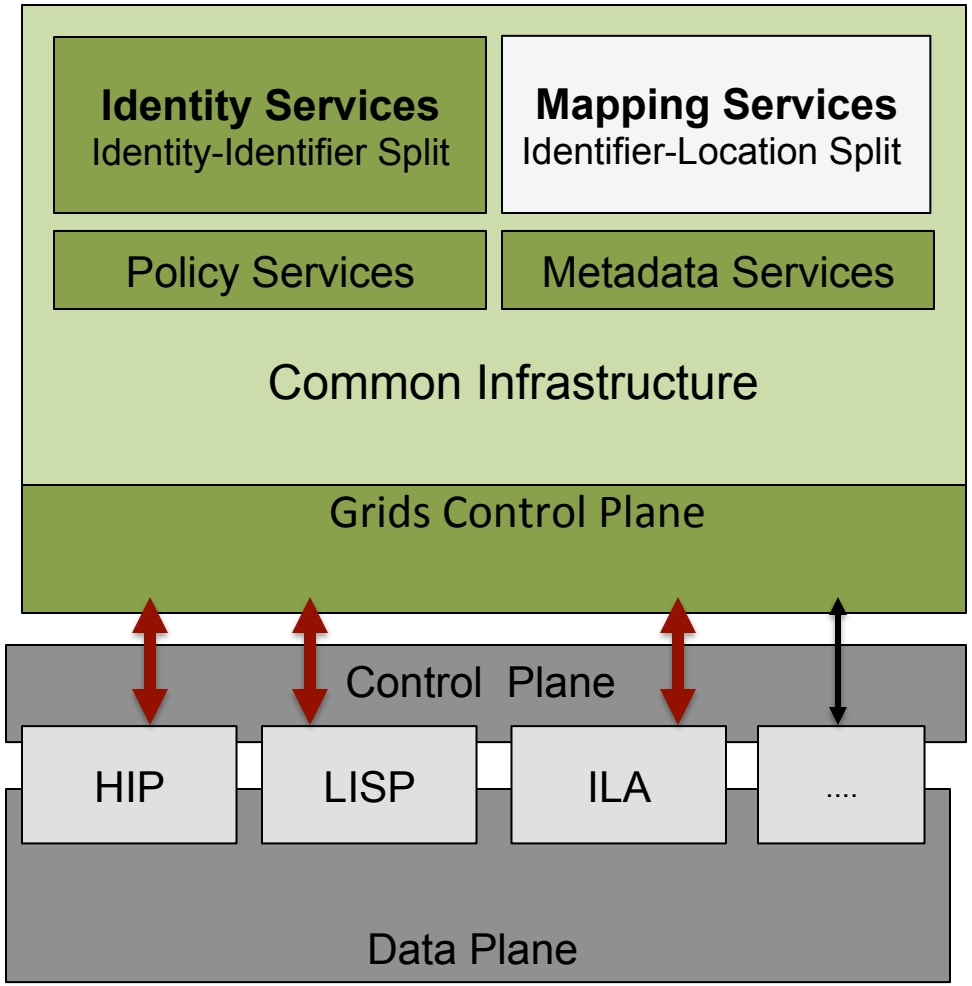
Forseen difficulties of deploying diverse solutions

- Impediment for the deployment of ID-enabled solutions.
- Difficulty to have an overall view of the network.
- Barriers to application of common consistent policies.
- Complex Management due to disjoint information spread over several mapping systems.

Common Infrastructure and Primitives
Need to facilitate deployment and consistency for policies
Need a common infrastructure benefiting all Idf-loc split protocols

Common Infrastructure and Primitives

Generic Identity Services (GRIDS)



Encrypted Control Plane New parameters …

In GREEN: New items in IDEAS

In Grey: Existing

In Red: New items in exisiting protocols WG

Scope of work

- In Scope
  - Network Identifiers (layer 3)
  - Locators are assumed to be ipv4/ipv6
  - Metadata: low frequency or no changes only (e.g type)
  - Identity services in the framework
  - Simple access control mechanism
  - Both Local scope and global scope
- Future work
  - Inter Grids communication

Scope of work

- Out of Scope
  - Resolution or mapping of domain names, application level names or directories
  - Metadata information high frequency changes or in the dataplane
  - Complex policy framework

Relationship with other WG

- HIP WG & LISP WG

Enable the identifier/location protocols to use identity.

Extend the control plane to interact with the framework

- NV03 WG
  - About mapping of VN names to VN Identifiers in the network virtualization space
  - May benefit from an open control plane

Questions?

Use Case drafts

- Identity and its Use Cases in IDEAS

draft-ccm-ideas-identity-use-cases-01

- Use Cases for IDEAS

draft-padma-ideas-use-cases-01

Summary of Issues (1)

- Discovery/Look up related problem
  - Need long lived identifiers for discovery
  - No access control for lookups and data is “public”
  - Anonymous identifiers cannot be used for discovery
  - **Need to give user Identity access control on discovery**
- Observation long-lived Identifiers problem
  - The identifiers are observable and trackable
  - Flows between peers observable
  - Obfuscation then lose ID context-awareness .
  - **Need clear identifiers meaningless to eavesdroppers**

Summary of Issues (2)

- Abuse of known Identifiers problem
  - Can be abused by legitimate previous peers
  - Deletion possible but data associated is lost
  - **Need immutable entry in system but external representation deleted**
- Lack of Common Infrastructure problem
  - Diversity of solutions in future
  - **Need to facilitate deployment and consistency for policies**
  - **Need a common infrastructure benefiting all Idf-loc split protocols**