

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 and evolving Network
- Increasing access diversity
- Increasing device diversity
- Ubiquitous mobility
- Identifier/Locator split protocols

What Users want:

- Privacy
- Access Control
- Personalized context-aware features

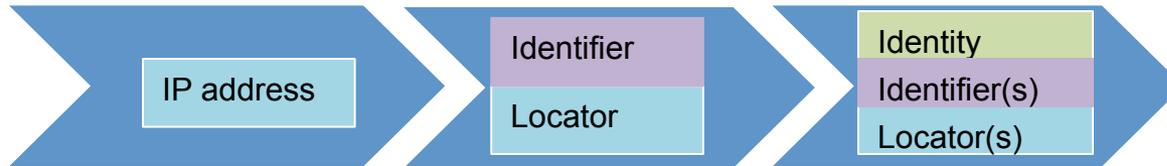
What operators want:

- Operational and deployment simplicity

What we propose:

- IDEAS goal is to facilitate delivery of the tasks above
- Introduce Identity-Identifier Split

Identity-Identifier Split



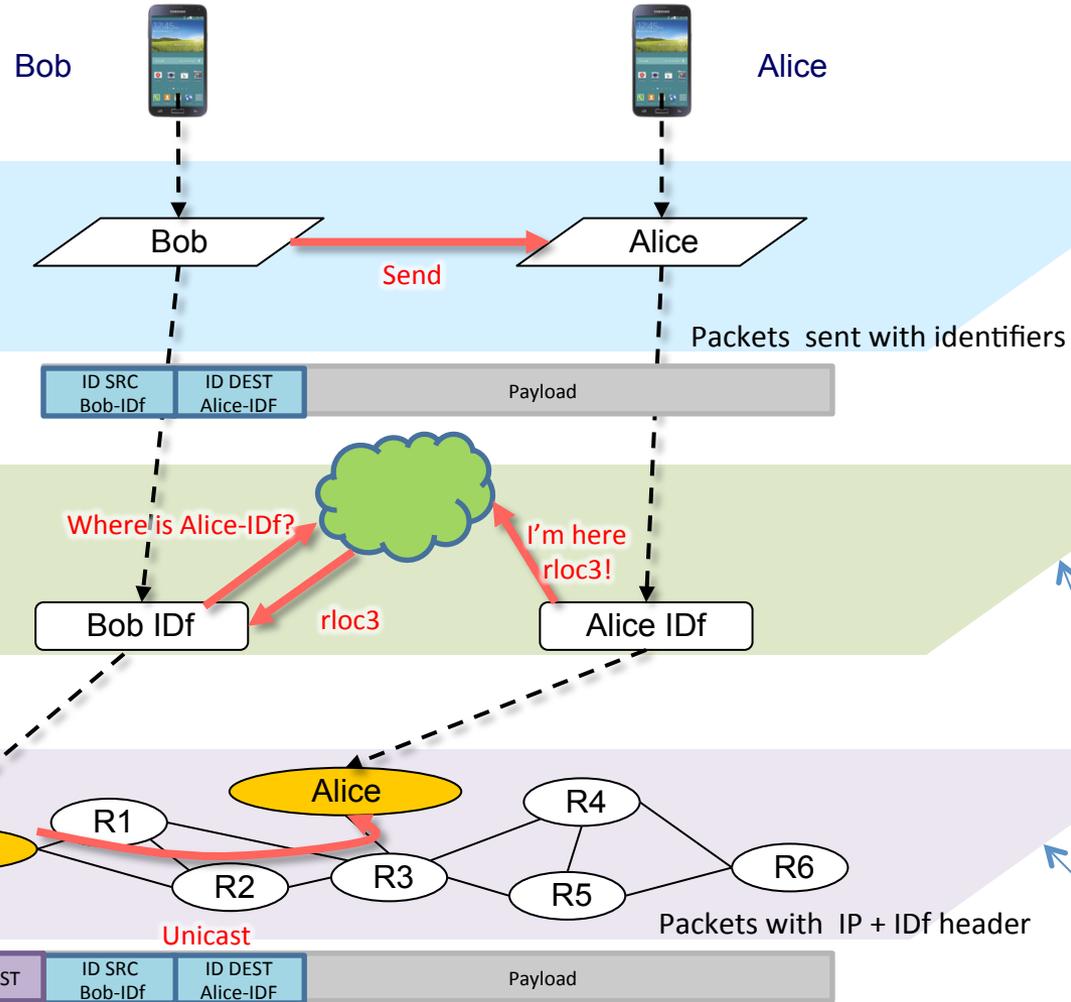
	Identity	Identifier
	Unique per entity	Multiple per entity associated with the identity
On the wire	Never revealed	May be in clear

Identity is an enabler:

- Lookup access control without being easily defeated
- Privacy of flows to eavesdroppers
- Immutable but erasable external representation (identifier)
- Simple policies based on Identity
- Features based on Identity

Privacy: Protection against Eavesdroppers

Bob sending a message to Alice



Meaningless clear identifiers to Eavesdroppers
Tradeoff between encryption and new features based on Identity

Privacy: Long Lived Identifier – Delete?

?? sending a message to Alice



Bob Stalker



Alice

IDf-aware

MS

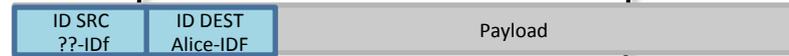
Resolution Layer

Network

Routing Layer



Packets sent with identifiers



Identifier = location (s)

Where is Alice-IDf?

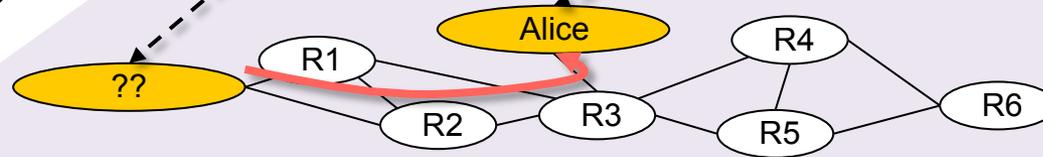


I'm here rloc3!

?? IDf

Alice IDf

Alice



Packets with IP + IDf header



Identifiers can be abused by legitimate previous peers
Need erasable external representations of Identity

Lack of Common Infrastructure and Primitives

Diversity of devices

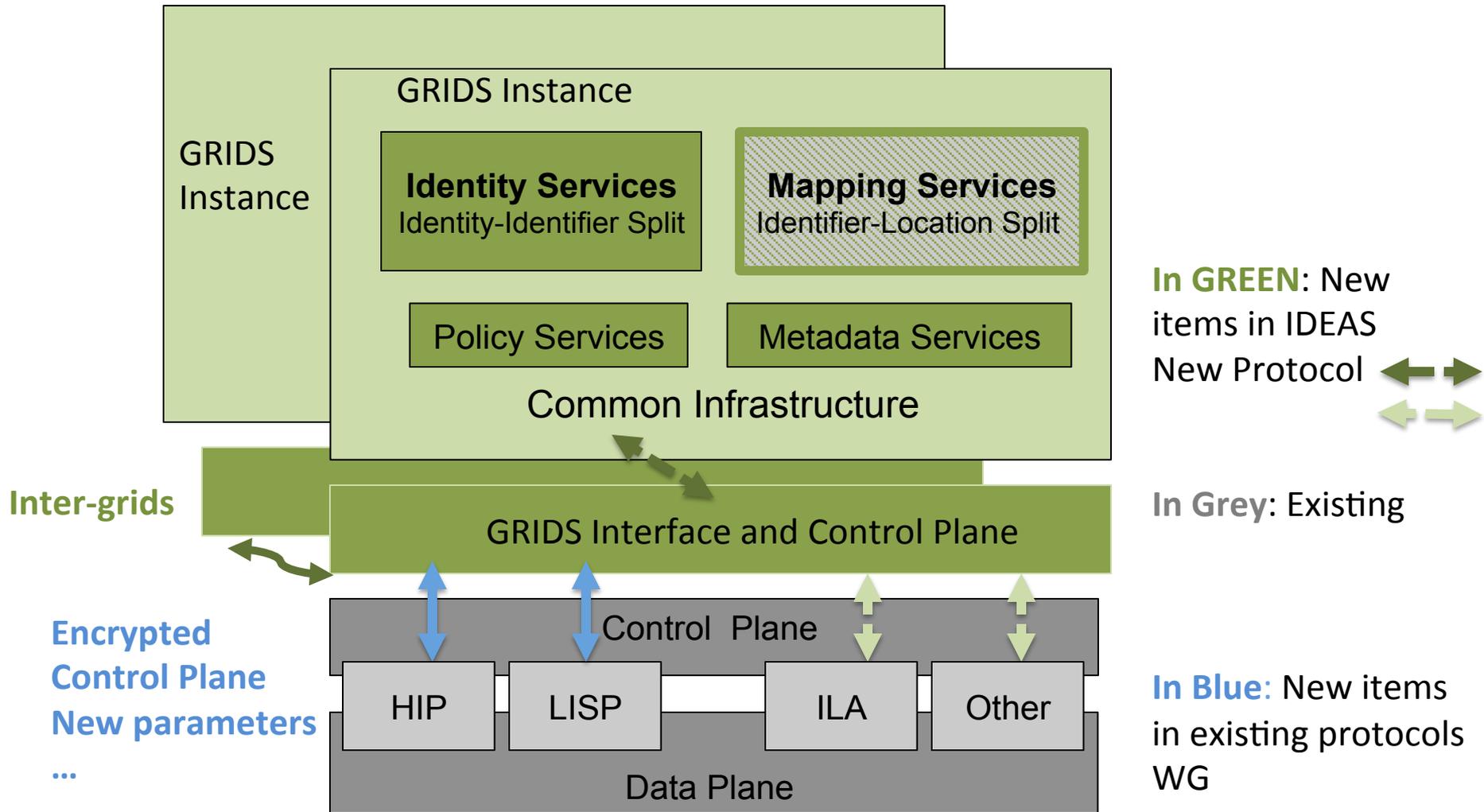
- One solution may not fit all
- Multiple systems?

Forseen difficulties of deploying diverse solutions

- Impediment for the deployment of IDf/Loc 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.

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

GeneRic IDentity Services (GRIDS)



Detailed Grids Requirements: draft-ideas-grids-req-01

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
 - 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 identity-identifier split
 - Collaborate to extend the control plane to interact with the framework
- NV03 WG
 - Mapping of VN names to VN Identifiers in the network virtualization space
 - May benefit from an open control plane

Thank you!

IDEAS Design Team (Co-authors/Proponents)

Albert Cabellos
Technical University of Catalonia
Spain
acabello@ac.upc.edu

Alexander Clemm
Huawei Technologies
USA
ludwig@clemm.org

Axel Nennker
Deutsche Telekom
Germany
axel.nennker@telekom.de

Andreas Stockmayer
University of Tuebingen
Germany
andreas.stockmayer@uni-tuebingen.de

Bingyang Liu
Huawei
China
iubingyang@huawei.com

Christian Jacquenet
Orange
France
christian.jacquenet@orange.com

Bin Da
Huawei
China
dabin@huawei.com

Dave Meyer
USA
dmm@1-4-5.net

David Lake
Dell EMC
UK
d.lake@surrey.ac.uk

Dino Farinacci
Lisper.net
USA
farinacci@gmail.com

Dipenkar (Ray) Raychaudhuri
Rutgers University
USA
ray@winlab.rutgers.edu

Georgios Karagiannis
Huawei Technologies
Germany
Georgios.Karagiannis@huawei.com

Giuseppe Fioccola
Telecom Italia
Italy
giuseppe.fioccola@telecomitalia.it

Jim Guichard
Huawei Technologies
USA
james.n.guichard@huawei.com

Michael Menth
University of Tuebingen
Germany
menth@uni-tuebingen.de

Mohamed Boucadair
Orange
France
mohamed.boucadair@orange.com

Robert Moskowitz
HTT Consulting
USA
rgm@labs.htt-consult.com

Parishad Karimi
Rutgers University
USA
parishad@winlab.rutgers.edu

Sam Sun
CNRI
USA
sam.sun.xun@gmail.com

Shreyasee Mukherjee
Rutgers University
USA
shreya@winlab.rutgers.edu

Tom Herbert
Quantonium
USA
tom@herbertland.com

Uma Chunduri
Huawei Technologies
USA
uma.chunduri@huawei.com

Victor Moreno
Cisco Systems
USA
vimoreno@cisco.com

Yingzhen Qu
Huawei Technologies
USA
yingzhen.qu@huawei.com

Companion Documents

Identity and It's Use Cases
[draft-ccm-ideas-identity-use-cases-01](#)
IDEAS/GRIDS Use cases
[draft-padma-ideas-use-cases-01](#)

Q/A?

Back up

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**