



HAL
open science

Design of a user-level naming solution for the future Internet

Nahla Abid

► **To cite this version:**

Nahla Abid. Design of a user-level naming solution for the future Internet. Networking and Internet Architecture [cs.NI]. Télécom Bretagne; Université de Rennes 1, 2015. English. NNT: . tel-01277483

HAL Id: tel-01277483

<https://hal.science/tel-01277483>

Submitted on 22 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



THÈSE / Télécom Bretagne

sous le sceau de l'Université européenne de Bretagne

pour obtenir le grade de Docteur de Télécom Bretagne

En accréditation conjointe avec l'Université de Rennes 1 École doctorale Matisse

Mention : Informatique

présentée par

Nahla Abid

préparée dans le département Réseaux, Sécurité et Multimédia
Laboratoire Irisa & Orange Labs

Design of user-level naming solution for the future Internet

Thèse soutenue le 30 janvier 2015

Devant le jury composé de :

César Viho

Professeur, Université de Rennes 1 / président

Hakima Chaouchi

Professeur, Telecom SudParis / rapporteur

Lila Boukhatem

Maître de conférences (HDR), Université Paris-Sud / rapporteur

Yacine Ghamri-Doudane

Professeur, Université de la Rochelle / examinateur

Philippe Bertin

Ingénieur de Recherche Senior, Orange Labs – Cesson Sévigné / Examineur

Jean-Marie Bonnin

Professeur, Télécom Bretagne / Directeur de thèse

Sous le sceau de l'Université européenne de Bretagne

Télécom Bretagne

En habilitation conjointe avec l'Université de Rennes 1

Ecole Doctorale – MATISSE

DESIGN OF A USER-LEVEL NAMING SOLUTION FOR THE FUTURE INTERNET

Thèse de Doctorat

Mention : Informatique

Présentée par **Nahla Abid**

Département : Réseaux, Sécurité et Multimédia (RSM)

Laboratoire : Orange Labs / Irisa

Directeur de thèse : Jean-Marie Bonnin

Encadrant : Philippe Bertin

Jury :

M. César Viho, Professeur, Université de Rennes 1 (Président)

Mme Hakima Chaouchi, Professeur, Telecom Sud Paris (Rapporteur)

Mme Lila Boukhatem, Maître de conférences, Université Paris Sud (Rapporteur)

M. Yacine Ghamri-Doudane, Professeur, Université de la Rochelle (Examinateur)

M. Jean-Marie Bonnin, Professeur, Telecom Bretagne (Directeur de thèse)

M. Philippe Bertin, Ingénieur de Recherche Senior, Orange Labs (Encadrant)

Acknowledgments

This thesis owes its accomplishment to the help, support and assistance of several people. First, and foremost, I would like to express my sincere gratitude and appreciation to my supervisors, Prof. Jean-marie Bonnin and Dr. Philippe Bertin, for their guidance during my research. Their support and gentle encouragements have been precious for the development and the accomplishment of this thesis content. I am very grateful to both of them.

Furthermore, I would also like to thank the reviewers for accepting to review my work.

I am deeply obliged to my friends and colleagues in Orange Labs and Telecom Bretagne for their support and help during my PhD program. I have learnt a great deal from them all. I would like to thank my friend Siwar for her special friendship. I would never forget her help during the stressful and difficult moments of this thesis. She had the kindness to listen to me, and to encourage me to go ahead and finalize this research work.

My deepest gratitude goes to my parents for their unflagging love, faith and unconditional support throughout my life and my studies. I owe them everything. I would also like to thank my sister Nouha and my brother Houssein for their love and care since we were kids. A special thought goes to my aunt and my friend Malika. Thank you all with all my heart! You are an endless source of love!

Last but not least, I am very much indebted to my husband and my soulmate Mourad for his love, patience and support. His trust and sacrifice motivated me to focus on the accomplishment of this thesis. I am grateful for everything!

Abstract

Naming is a fundamental element to evolve the current Internet into the next stage. The new host-level and user-level scenarios of the future networks introduce great pressure towards the initial two-level naming system of the Internet, which is requested to evolve in order to answer these new requirements. More specifically, special attention should be paid to person-to-person communications and multi-device support in future naming schemes' design.

This thesis concentrates on the study of the naming research trends considering to improve future Internet's support to both host-level and user-level requirements. The Identifier/Locator split concept has been widely approved as a crucial solution for current Internet's naming problems. This is why, we first concentrate our work on studying several Identifier/Locator split solutions. We provide a qualitative overview and a quantitative cost analysis of the proposed approaches. Based on the results that we have obtained, we emphasize the host-centric character of these solutions and we show that they have shortages regarding additional user-level requirements.

In order to complement previous research work in the naming area, we present in this thesis a new naming proposal that we call Service-Aware Naming Architecture (SANA). Our solution is built around three key points. First, we challenge the traditional Identifier/Locator split paradigm by getting rid of terminals' identifiers and promoting users and services identification. Second, we provide a transparent multi-device support to the network. And finally, we make user's session switching between different terminals agnostic to applications and networks. SANA cost analysis results show that our solution has comparative performance with traditional Identifier/Locator solutions. It also outperforms other user-level naming solutions in terms of signaling cost and size of resolution systems.

By covering these aspects intrinsically, we believe that SANA can be consid-

ered a significant candidate for future naming systems with respect to user-level requirements.

Key words: Naming, Addressing, Mobility, Identifier/Locator split, Future Internet

Résumé

Le nommage est un élément fondamental à l'évolution de l'Internet. Les nouveaux scénarios de niveau hôte et utilisateur contraignent le système de nommage initial et à deux niveaux de l'Internet. Celui-ci est alors appelé à évoluer pour répondre à ces nouvelles exigences. Plus spécifiquement, une attention particulière devrait être accordée à la communication entre les utilisateurs et au support des multi-terminaux dans la conception des futurs systèmes de nommage.

Cette thèse s'intéresse à l'étude du problème de nommage dans l'Internet du futur en tenant en compte les contraintes à la fois de niveau hôte et de niveau utilisateur. Le concept de séparation Identifiant / Localisateur a été largement approuvé comme une solution pour les problèmes actuels de nommage. Pour cette raison, nous nous concentrons d'abord sur l'étude de plusieurs solutions implémentant cette approche. Nous fournissons une vue d'ensemble qualitative et une analyse quantitative des coûts des approches proposées.

En se basant sur les résultats obtenus, nous soulignons que ces solutions sont centrées sur les hôtes et nous montrons qu'elles sont inadéquates avec les exigences supplémentaires de niveau utilisateur.

Afin de compléter les travaux de recherche déjà existants, nous présentons dans cette thèse une nouvelle architecture appelée SANA (Service-Aware Naming Architecture). Notre solution est basée sur trois points clés. Tout d'abord, nous remettons en question le concept de séparation Identifiant/Localisateur en promouvant l'identification des utilisateurs et des services. Ensuite, nous fournissons un support multi-terminaux transparent pour le réseau. Et enfin, nous assurons un transfert de session transparent au réseau et aux applications entre des terminaux du même utilisateur.

Les évaluations de SANA montrent que notre solution offre des performances comparables aux celles des approches de séparation Identifi-

ant/Localisateur. SANA dépasse aussi d'autres solutions de nommage de niveau utilisateur en termes de coût de message de signalisation et de la taille des systèmes de résolution.

En couvrant ces aspects, SANA peut être considérée comme un candidat potentiel pour les futurs systèmes de nommage en prenant en compte le niveau utilisateur.

Mots clés: Nommage, Adressage, Mobilité, Séparation Identifiant/Localisateur, Internet du futur

Contents

Acknowledgments	i
Abstract	iii
Résumé	v
Contents	vii
List of Figures	xiii
List of Tables	xvii
1 Introduction	1
1.1 Context and Problem Statement	2
1.2 Contributions	4
1.3 Organization of the Dissertation	5
2 State of the Art: Naming and Addressing in IP Networks	9
2.1 Introduction	9
2.2 Terminology	12
2.3 The Future Internet: Problems and Research Directions	13
2.4 Internet Namespaces	16
2.4.1 IP Addresses: A Dual Role	16
2.4.2 Shortcomings of Internet Namespaces	17
2.5 Identifier/Locator (Id/Loc) Separation Concept	18
2.5.1 Origins	19
2.5.2 Main Idea	19
2.5.3 Requirements and Design Goals of Identifier/Locator Split Architectures	21

2.5.3.1	ITU-T Requirements on Identifiers and locators	21
2.5.3.2	ITU-T Requirements on Mapping Storage Function	22
2.5.3.3	ITU-T Requirements on Mapping Function	23
2.5.3.4	Other Requirements	23
2.5.4	RRG Architectural Requirements	23
2.6	A Survey of Identifier/Locator Separation Solutions	25
2.6.1	Classification Approaches	25
2.6.2	Host-based Schemes	27
2.6.2.1	Namespaces	28
2.6.2.2	Resolution mechanism	29
2.6.2.3	Answers to functional ITU Requirements	31
2.6.2.4	Answers to RRG Design Goals	31
2.6.3	Map-and-Encap Schemes	33
2.6.3.1	Namespaces	33
2.6.3.2	Resolution Mechanism	34
2.6.3.3	Answers to Functional requirements	35
2.6.3.4	LISP Answers to RRG Design Goals	35
2.7	Comparison and Analysis	37
2.8	Discussion	39
2.9	Chapter Conclusion	40
3	Cost Analysis of Identifier/Locator Split Solutions	43
3.1	Introduction	43
3.2	Definition of Costs	44
3.3	Preliminaries	45
3.3.1	System Modeling	45
3.3.2	Assumptions	46
3.4	Connection Establishment Signaling Cost (CEC)	48
3.4.1	HIP Connection Establishment Cost CEC (HIP)	49
3.4.2	LISP Connection Establishment Cost CEC (LISP)	49
3.4.3	ILNP Connection Establishment Cost	50
3.5	Data Packet Delivery Cost (DPC)	50
3.5.1	HIP Data Packet delivery Cost	50
3.5.2	LISP Data Packet delivery Cost DPC(LISP)	51
3.5.3	ILNP Data Packet delivery Cost	51
3.6	Mobility Signaling Cost (MSC)	51

3.6.1	Mobility Signaling Cost of HIP MSC (HIP)	51
3.6.2	Mobility Signaling Cost of LISP	52
3.6.3	Mobilty Signaling Cost of ILNP	53
3.7	Numerical Results	53
3.7.1	Impact of N_{CH}	54
3.7.2	Impact of Network Scale	56
3.7.3	Impact of Velocity	57
3.7.4	Impact of Cell's Radius	58
3.8	Chapter Conclusion	58
4	Towards User-level Naming Architectures	61
4.1	Introduction	61
4.2	New Use Cases and User-level Requirements	62
4.2.1	The user as Endpoint of Communications	62
4.2.2	User Multi-homing	63
4.2.3	Handover between Devices/ User-level Mobility	64
4.2.4	Selection of a Proper Device / a Proper Network	64
4.3	Do Host-based and Network-based Id/Loc Split Solutions meet User-level Requirements?	65
4.4	Evolution of Naming Models	67
4.5	Users and Services identification in Recent Naming Proposals	69
4.5.1	Layered Naming Architecture (LNA)	69
4.5.1.1	Namespaces	69
4.5.1.2	Resolution Mechanisms	70
4.5.1.3	Answers to User-level requirements	70
4.5.2	User Id Routing Architecture (UIR)	72
4.5.2.1	Namespaces	72
4.5.2.2	Resolution Mechanisms	73
4.5.2.3	Answers to User-level requirements	74
4.5.3	Policy Oriented Naming Architecture (PONA)	74
4.6	Discussions	75
4.7	Conclusion	77
5	SANA: A Service-Aware Naming Architecture for Future Internet	79
5.1	Introduction	79
5.2	Design Principles Behind SANA	80

5.3	General Design of SANA (Service-Aware Naming Architecture)	82
5.3.1	Terminology	82
5.3.2	User-centric vs Host-centric Naming Architecture	83
5.3.3	General Architecture of SANA	84
5.3.4	Namespaces	86
5.3.5	Resolution System	87
5.4	Data and Control Planes	88
5.4.1	Data Transport Plane	88
5.4.2	Control Plane	90
5.5	Communication Scenarios	93
5.5.1	Scenario 1: Registering a new user SId	93
5.5.2	Scenario 2: Communication Process	95
5.5.3	Scenario 3: Host Mobility	97
5.5.4	Scenario 4: Host Multi-homing	99
5.5.5	Scenario 5: User Multi-homing vs. Device Multi-homing	100
5.5.6	Scenario 6: User-Session Transfer	101
5.6	Chapter Conclusion	101
6	Design Enhancements and Evaluation of SANA Architecture	103
6.1	Introduction	103
6.2	Architectural Discussions and Design Enhancements	104
6.3	Integration of SANA domains and Legacy Domains	105
6.4	Answers to Functional ITU Requirements	107
6.5	Answers to RRG Design Goals	107
6.6	Answers to user-level Requirements	109
6.7	Security	110
6.8	Optimization of Resolution Performances	111
6.9	Summary	112
6.10	Analytical Evaluations	117
6.10.1	Assumptions and Network Model	117
6.10.2	SANA Connection Establishment Cost CEC(SANA)	118
6.10.3	SANA Data Packet Processing Cost DPC(SANA)	119
6.10.4	LNA Connection Establishment Cost CEC(LNA)	120
6.10.5	UIR Connection Establishment Cost CEC(UIR)	120
6.11	Numerical Results	121
6.11.1	Impact of Correspondent Nodes	121
6.11.2	Impact of Network Scale	123

6.12 Resolution System Performance: SANA vs Id/Loc split architectures	124
6.13 Chapter Conclusion	129
7 Conclusion & Perspectives	131
A Résumé de la Thèse	135
B List of Publications	141
Bibliography	143

List of Figures

1.1	Number of Global Connected Devices [cis]	2
1.2	Global Mobile Devices and Connections Growth [cis]	3
2.1	The Double Role of IP Addresses	17
2.2	The Identifier/Locator Split	20
2.3	ITU functional model for Id/Loc Split [ITU]	21
2.4	Growth of the BGP Table	24
2.5	Raj Jain Naming Reference Model [PPJ]	26
2.6	Classification of Naming Approaches	27
2.7	HIP Host Protocol Stack	29
2.8	ILNP Host Protocol Stack	29
2.9	HIP Registration and Base Exchange Mechanisms	30
2.10	LISP Node Protocol Stack	33
2.11	LISP Architecture	35
3.1	Network Configuration Model	46
3.2	HIP Network Configuration Model	47
3.3	LISP Network Configuration Model	48
3.4	ILNP Network Configuration Model	48
3.5	Impact of N_{CN} on Connection Establishment Cost	54
3.6	Impact of N_{CH} on Data Packet Processing Cost	55
3.7	Impact of Network Scale on Connection Establishment Cost	56
3.8	Impact of network scale on Connection Establishment Cost	57
3.9	Impact of velocity on Mobility Signaling Cost	58
3.10	Impact of Cell radius on Mobility Signaling Cost	59
4.1	User Session Handover between two devices	64
4.2	Selection of a Proper Device in User Multi-homing Case	65
4.3	User Multi-homing Case in a HIP Environment	67

4.4	The Different Naming Models	68
4.5	LNA Namespaces	70
4.6	LNA Connection Establishment Flow	71
4.7	Email Example in an LNA-based Network	72
4.8	UIR Architecture	73
4.9	PONA Architecture	75
5.1	Services among the devices	82
5.2	A Possible Structure of an MId	82
5.3	A Possible Structure of an SId	83
5.4	Dependency Diagram	84
5.5	User-centric Network Architecture	84
5.6	Host-centric Network Architecture	85
5.7	SANA General Architecture	85
5.8	SANA Protocol Stack	86
5.9	Resolution Steps in SANA	88
5.10	SANA Resolution Model vs other Naming Models	89
5.11	Data and Control Planes in SANA	90
5.12	User Data Plane in SANA	90
5.13	Data Packet Format in SANA	91
5.14	SBP Packet Format in SANA	91
5.15	MSIB Map_Request Packet Format	93
5.16	MSIB Map_Answer Packet Format	93
5.17	MUP Packet Format	94
5.18	Announcing a new SId	94
5.19	Announcing a new SId	95
5.20	Connection Establishment in SANA	96
5.21	Intra-AR Host Mobility in SANA	98
5.22	Inter-domain Host Mobility in SANA	98
5.23	User and Device Multi-homing in SANA	100
5.24	Session Transfer in SANA	101
6.1	Communication between two SANA hosts	106
6.2	SANA Network Configuration	117
6.3	LNA Network Configuration	118
6.4	UIR Network Configuration	119
6.5	Connection Establishment Cost/Correspondent Nodes	122
6.6	Connection Establishment Cost/Correspondent Nodes	123

6.7 Data Packet Delivery Cost/Correspondent Nodes 124

6.8 Connection Establishment Cost/Network Scale 125

6.9 Connection Establishment Cost/Network Scale 126

6.10 Total Size of Resolution Structure in SANA and Identifier/Locator Split Approach 127

6.11 Number of Signaling Messages According to the Number of Terminals 128

List of Tables

2.1	Main Research Projects on the Future Internet	15
2.2	HIP and ILNP Answers to functional ITU Requirements	31
2.3	HIP and ILNP Answers RRG Requirements	33
2.4	LISP Answers to functional ITU Requirements	36
2.5	Comparative Analysis of Naming Schemes	38
3.1	List of Parameters used in the Analytical Model	47
3.2	Numerical Values of Messages Size	53
4.1	Answers to User-level Requirements	76
5.1	SBP Packets Types	92
5.2	MSIB Packets Types	92
5.3	Types of MUP Packets	94
6.1	SANA Answers to Functional ITU-T Requirements	108
6.2	Summary of all the Naming Schemes (1/4)	113
6.3	Summary of all the Naming Schemes (2/4)	114
6.4	Summary of all the Naming Schemes (3/4)	115
6.5	Summary of all the Naming Schemes (4/4)	116
6.6	Numerical Values of Messages Size in SANA	121

Chapter 1

Introduction

Naming and addressing are fundamental elements to evolve the current Internet into the next stage. The new requirements of the future networks shape the naming concepts considerably. Many new challenges are arising such as the increasingly diverse and dynamic environment expected for users and the enormous proliferation of connected devices. Consequently, special attention should be paid to person-to-person communications and multi-device support in future naming schemes' design.

Due to the importance of the naming problem in both industry and academia, this PhD thesis has been proposed by Orange Labs in collaboration with Telecom Bretagne. The research work conducted in the context of this PhD brings a critical point of view towards the current trends in the naming area. This PhD work has been involved in an Orange internal research project (LETSMOVE) and in other european projects (4WARD¹ and SAIL²). In addition, it has resulted in the publication of several international papers [ABB11][ABB12][ABB14] and an international patent [AB14].

Section 1.1 presents in more details the context and the problem statement of our research work. Our contributions are presented in Section 1.2. Finally Section 1.3 describes the organization of this dissertation.

¹<http://www.4ward-project.eu/>

²<http://www.sail-project.eu/>

1.1 Context and Problem Statement

It seems that the exceptional success and growth of Internet technologies is a never-ending process which still faces new challenges even after around 40 years of its creation. Today, Internet is evolving into a seamlessly connected network that aims at simplifying the communication experience of its users by making its service offering a single any time any where and any device process. Barriers between fixed and mobile devices are disappearing. Moreover the two industries are converging and constellating based on their service offering capabilities.

Based on the Cisco networking forecast report [cis] and as depicted in Figure 1.1, it is estimated that by 2018, there will be 177 million connected devices globally, growing eight-fold from 22 million in 2013.

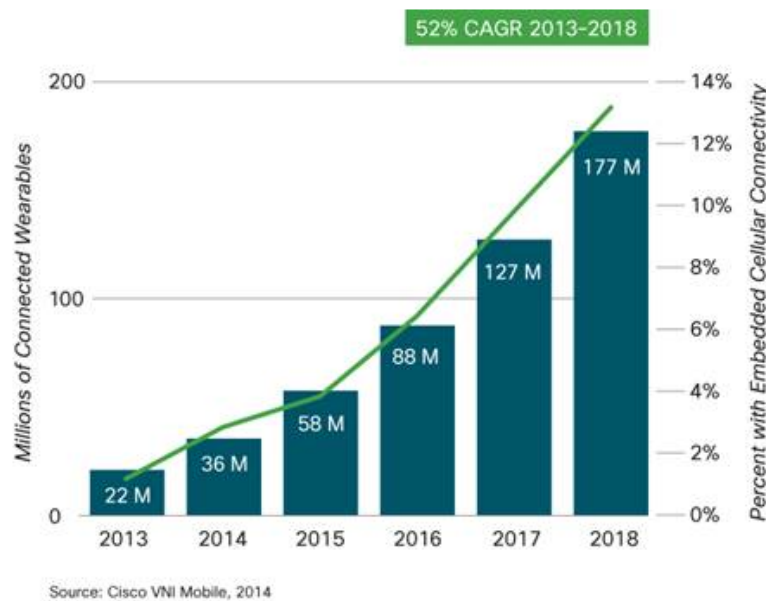


Figure 1.1: Number of Global Connected Devices [cis]

By the end of 2014, the number of connected devices will exceed the number of people on earth. Moreover, by 2020 it is expected that more than five billion consumers worldwide will be connected to the Internet via 20 billion wired and wireless devices [Aaa].

It means that for the future Internet, real-world user multi-device scenarios will be largely widespread. As devices are expected to converge in their functionalities and capabilities as show in Figure 1.2, a single user will then

be presented with a vast array of communication options and alternatives. Reachability will be at the center, which intuitively means that a given user should be served regardless of access networks and owned devices.

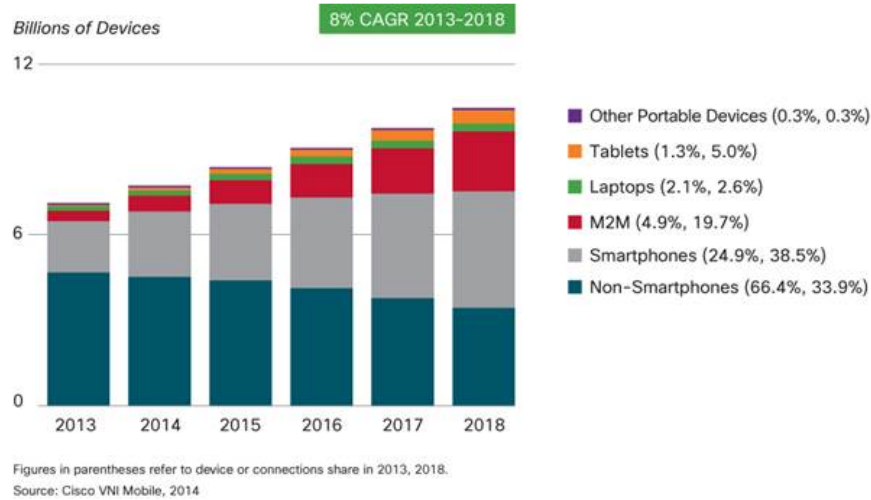


Figure 1.2: Global Mobile Devices and Connections Growth [cis]

Realizing these upcoming scenarios introduces obviously new technical challenges in the area of naming. The way with which users, terminals and services are named plays a crucial role in how the future Internet can handle the above described communication trends.

In 1970's, when Internet appeared, naming and addressing had never been a major concern to consider. The reason was that at that time, networks were small-sized and sufficiently simple, and hosts were static. Consequently, the main goals of a naming and addressing scheme were limited to connectivity, accessibility and reachability.

However and as stated above, within the last forty years, trends in IP networks kept growing in users, number of connected devices, and variety of services and usages leveraging new architectural needs. Today, Internet architecture is challenged by several new problems, such as smooth mobility and multi-homing support, security and traffic engineering.

All these facts drive obviously new constraints on the naming and addressing architecture of the Internet. As a consequence, a clear need to rethink the basic naming system has appeared.

Over the past decade, naming topic has gained too much importance in the discussions around the future Internet design. Initially, the naming system

of the Internet is composed of two global namespaces, namely IP addresses [Int81][DH95] and DNS names [Moc87a].

Although being behind the exceptional success of the Internet, there is now an agreement in the research community that this system presents many shortcomings and fails as such to meet the new challenges of the future. Research work in this area addresses the semantic overloading of IP addresses [MZF07]. It is an architectural ill that is responsible for endhost problems like mobility, multi-homing and security and for more general architectural issues like routing scalability and traffic-engineering.

Research directions in this area consider the Identifier/Locator split [MZF07] mechanism as an interesting solution. However, because of their host-level character, schemes based on this approach present many limitations when applied to solve user-level problems.

To summarize, existing Id/Loc separation proposals, although numerous in the literature, inherit from the host-centric character of the Internet early design. However, new user and data-centric communication models impose new requirements for naming systems. The balance between what Identifier/Locator split offers and what is needed in a future naming system is the central point of this thesis.

1.2 Contributions

The work done in this thesis contributes to the naming research activities in the future Internet. Many works have been done around this topic. However, almost these solutions resolve the problem from a host-level point of view. The critical need to study user-level requirements and propose a complementary architecture is the main initiator of this thesis.

As consequence, in this work, we have developed the following contributions.

- **Evaluating main naming proposals towards ITU-T and RRG requirements:**

First of all, after locating the existing naming system weaknesses, we review carefully the different proposed schemes of Id/Loc split concept. We qualitatively evaluate them toward ITU-T and RRG design goals. Hence, we extract a list of conclusions.

- **Classification and cost analysis of existing Id/Loc split schemes:**

We develop analytical model for protocols modeling and analysis. We also define various analysis criteria in both control plane and data plane. Related work in the literature have given much importance to define and discuss theoretical features of these schemes. However, analytical evaluations and comparison lack in the literature. Our contribution consists in analytically evaluating these main proposals and comparing them.

The main interesting points of these two analyses are the conclusions and perspectives that we draw out after each analysis. Through these conclusions, we pave the way towards proposing enhancements or even a novel scheme. For instance, we demonstrate the benefits and drawbacks of host-level and network-level schemes.

- **Proposal of a new user-level naming scheme called SANA:**

After investigating the different Id/Loc schemes, we conclude their shortcomings and we emphasize their host-centric character and their shortcomings in supporting user requirements. We propose a novel naming architecture called SANA that takes into account user-level scenarios besides host-centric requirements.

- **Evaluation of SANA and comparison with other Id/Loc split proposals:**

After proposing a new scheme, it is essential to analyze and evaluate it in comparison with other protocols and proposals. It is also essential to study its impacts on other networking aspects. Therefore, we have compared SANA with both host-level solutions and user-level solutions. Results show that SANA succeeds to provide an additional naming level while keeping a good performance.

1.3 Organization of the Dissertation

The structure of this dissertation is organized as follows.

Chapter 2: This chapter presents a survey of naming mechanisms and related problems in IP networks. The chapter has two main parts. The first part presents a comprehensive state of the art in the domain of naming in

IP networks. It gives an overview of the deployed naming architecture in the Internet and highlights the different problems of its two-level naming system. The second main part of Chapter 2 introduces the Identifier/Locator split concept and how it can answer to the problems cited in the former part. Moreover, a classification of proposed Id/Loc split approaches is proposed. In order to qualitatively study the efficiency of the introduced schemes, we list ITU-T and RRG design requirements and we carefully study the answers brought by each of these categories to these different requirements.

Chapter 3: To investigate in more details the strong and weak points of each scheme, we dedicate Chapter 3 to define a cost analysis model. We believe that this is an important step in our work, because it allows to quantify the different properties described in Chapter 2. Thus, in Chapter 3, we develop an analytical model to evaluate the different Id/Loc split proposals. In addition, we define a variety of analysis criteria that can examine thoroughly the main properties of each scheme. This part is partially published in [\[ABB14\]](#).

Chapter 4: In this chapter, we draw in more details the evolution of naming models. We highlight through some communication scenarios the importance of users in future Internet scenarios.

Based on these scenarios, we define a list of user-level requirements. We first show why host-level naming approaches described in Chapter 3 do not suit this type of user-level scenarios. Moreover, we study few recently proposed user-level naming solutions. A comparison between these solutions and the requirements that we have proposed shows that some features are not still addressed in the literature.

After investigating the proposed Id/Loc split schemes, we conclude their shortages, the missing points and we propose a novel user-level naming architecture.

Chapter 5: We detail here our proposal. We first provide the design principles that motivate SANA. Then we present an overview of the naming and resolution procedures in SANA. Finally, the different communication flows of SANA are detailed.

Chapter 6: This chapter describes, in two main sections, the answers

of SANA to host-level and user-level requirements. First, it provides an analytical evaluation of our proposal and compares it with previous analytical results. Then, it provides analytical evaluation results of SANA using the same framework presented in Chapter 3. A comparison between SANA performances and previously obtained Id/Loc split schemes performances is provided.

Chapter 7: It closes the thesis by giving concluding remarks and different perspectives for future investigation.

Chapter 2

State of the Art: Naming and Addressing in IP Networks

2.1 Introduction

Naming and addressing are fundamental components of Internet architecture. Names and addresses are used at different levels of the TCP/IP [Pos80] stack for various purposes. For instance, from an application layer view, hosts need names to identify and discover each other. In the networking layer, routing protocols use addresses to route packets.

The basic original Internet naming and addressing architecture was based on a single namespace of IP addresses [Int81][DH95]. Since its deployment in the Internet, an IP address has served two main functions: *identifier* for hosts and *locator* for routing. In the literature, these functions are referred to as '*the Dual Role of an IP Address*' [MZF07].

In 1983, a second namespace of Fully Qualified Domain Names (FQDNs)¹ was added, and a Domain Name System (DNS) [Moc87a] was introduced to map between the two namespaces, i.e. FQDNs and IP addresses. DNS is standardized by the Internet Engineering Task Force (IETF) as RFC 882 [Moc87a][Moc87b] and RFC 883 [Moc83]. The idea behind introducing domain names is to replace the use of numerical IP addresses by human-friendly and simple names. The use of such names can be considered as one of the Internet's greatest successes because it gives the internet a human character.

¹http://en.wikipedia.org/wiki/Fully_qualified_domain_name

Additionally, over time, a number of additional namespaces have emerged (URL [BLMM94], URI [BLFM05], etc.), many of which include some components of domain names and are also served by DNS. These namespaces are all located at the application-layer level.

These namespaces were sufficient to satisfy the two main primary goals of Internet, i.e. connectivity and reachability.

But although being behind the exceptional success of the Internet, there is now an agreement in the research community that this system presents many shortcomings [Nik07][Jai06b] and fails as such to meet the new challenges of the future. Hereafter, we cite the most known Internet problems related to its naming and addressing system.

- Address space exhaustion [GA92]: The dramatic development of the Internet industry in the last ten years has led to the depletion of the remaining IPv4 address space available to the Regional Internet Registries (RIRs)². IPv4 address space exhaustion will create a great restriction on the Internet, and will inevitably raise serious problems as time progresses.
- Multihoming is not natively supported [Ste07]: The use of host and/or site multihoming is not as straightforward as it seems to be at first look. Technical issues related to multihoming span several levels of the TCP/IP model. Address selection (both for source and destination addresses) is one of the major problems with multihoming. This selection process is affected by at least the following aspects: administrative policies, characteristics (QoS, bandwidth, delay, etc) on different interfaces, the cost of using a certain interface and the requirements of applications, user, or operator.
- Mobility is cumbersome and complex [Per02]: In future networks, users will be using devices with a variety of networking technologies and will be highly mobile. Some of the applications may need high throughput and strict delay constraints, e.g., video streaming, online gaming, and medical applications. Therefore, these networks should support key features, such as full support for user mobility, host mobility. However, in the existing architecture, if hosts, or users change their networks and/or locations, then their IP addresses may also change. Consequently, their

²http://en.wikipedia.org/wiki/Regional_Internet_registry

transmission control protocol (TCP) connections at the transport layer are broken. Recently, variants of Mobile IP protocols [CGK⁺02] have been developed to resolve the mobility limitations of Internet architecture. However, these protocols cause signaling overhead, create a single point of failure, and lack smooth handover capabilities and interoperability between IPv4 and IPv6.

- Router table size is exploding [Hus01]: Because of multihoming and traffic engineering, the Forwarding Information Base (FIB)³ of the Default Free Zone (DFZ) is growing greater than linear rate. Today, the DFZ routing tables have already reached 280,000 entries, which bring great challenges to the memory sizes and processing capabilities of the core routers.
- Network Address Translator (NAT) traversal [Hai00][HS01]: The use of NATs break the flexible end-to-end model of the Internet.

Research efforts conducted on this field concluded that it is necessary to rethink the original naming system of Internet. Research work in this area addresses the semantic overloading of IP addresses [MZF07]. The concept of 'Identifier/Locator Split' [MZF07] has been identified as a key solution for this architectural problem.

In this chapter, we are interested in introducing the state of the art research in the naming and addressing fields.

Section 2.2 is a brief explanation of some of the terminologies related to naming and addressing and that we use in this dissertation. Section 2.3 presents an overview of the research projects on Future Internet. The chapter introduces in Section 2.4 fundamental naming concepts and challenges of the existing Internet naming architecture. In Section 2.5, we introduce the 'Identifier/Locator Split' concept and its different architectural implications. In the final part of this chapter, we provide a comprehensive survey and analysis of a representative sample of Identifier/Locator proposals. The chapter is concluded with an analysis and a comparison of the different approaches.

³http://en.wikipedia.org/wiki/Forwarding_information_base

2.2 Terminology

During our research work, we have noticed that a commonly approved terminology is lacking in the fields of naming and addressing. In order to make the understanding of this dissertation easier, we define hereafter the terminology that we use.

Name This term is used in a very general sense, to refer to any label that is attached to a network entity (host, user, service, application, etc.).

Address The ITU-T Recommendation Y.2091 [20911] defines an address as : *'An address is the identifier for a specific termination point and is used for routing to this termination point.'* In this report, the terms Locator (Loc) and Address are used for the same purposes.

Identifier (Id) The ITU-T Recommendation Y.2091 [20911] defines an identifier as : *'An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g. physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).'*

It is worth noticing that the objective of an identifier is not only to uniquely identify an entity or a group of entities (in multicast case for example) in the network. Thus, it may include several properties as described in Section 2.5.3.1.

Namespace It is a set N of names from which all names for a given collection of objects are taken. A name from a given namespace may be bound to one and only one object at a time [Day08]. Examples of objects are: users, hosts, services, etc.

2.3 The Future Internet: Problems and Research Directions

The *Future Internet*⁴ and the *Next-generation Internet*⁵ are summarizing terms used to refer to all research activities that strive for developing the original Internet and designing new communication architectures. At present, it is widely known that current Internet is facing serious problems at different design levels [Jai06b].

Several projects and initiatives have been started over the past decade to develop a more efficient and a more secure next generation Internet that remedies the current architectural issues [ZPT+11] and responds to the future requirements [Jai06a]. Future Internet research encompasses many design fields such as routing functions, content delivery mechanisms, security and others .

These research efforts can be divided into two classes :

Clean Slate Design This approach consists in defining the ideal Internet architecture while ignoring all the existing stuff. In this respect, the process of design has been called 'clean slate', meaning that the research community is encouraged not to be constrained by features of the existing network.

The most famous example of this category is Interprocess Communication (IPC) model [DMM08a] which is proposed by John DAY.

John DAY is one of the Internet pioneers and has written an interesting book untitled '*Patterns in Networks Architectures : A return to Fundamentals*' [Day08]. In this book, the author presents a historic and comprehensive survey of the Internet architecture. He presents the rationals behind the first architectural choices of Internet. The author criticizes the layered model on which the Internet has been built. Besides, John DAY proposes an alternative approach to networking called, 'IPC Model' [DMM08b][Day08]. The main problem of this approach is its compatibility with the legacy networks. It is why it had very little chance of ever being realized in real-world scenarios.

Evolutionary Design It supports incremental ameliorations to the Internet. Examples of evolutionary approaches include : IPv6 addresses

⁴[http://en.wikipedia.org/wiki/Future Internet](http://en.wikipedia.org/wiki/Future_Internet)

⁵[http://en.wikipedia.org/wiki/Next Generation Internet](http://en.wikipedia.org/wiki/Next_Generation_Internet)

[DH98], Network Address Translators (NATs) [SE01], security mechanisms [Atk95][FKK96],etc.

In [PPJ11a][PPJ11b] the authors present a survey of the different research projects conducted all over the world and which address the future Internet design. In Table 2.1, we summarize the most significant projects in this field.

Project Name	Country	Type of approach	Main Contributions and Components
GENI (Global Environment for Network Innovations) [EF09]	USA	Evolutionary	Federation and security Providing a global large-scale experimental testbed for future Internet test and validation
FIND (Future Internet Design) ⁶	USA	Clean slate	Named Data Networking ⁷ Mobility first ⁸ NEBULA ⁹ eXpressive Internet Architecture (XIA) ¹⁰
FIA (Future Internet Assembly) ¹¹	Europe	Evolutionary	4Ward ¹² FIRE ¹³
AKARI (Architecture Design Project for New Generation Network) ¹⁴	Japan	Clean slate	Optical Access Network Architecture Network Virtualization

Table 2.1: Main Research Projects on the Future Internet

In the context of future Internet design, naming and addressing appear to be a hot subject of discussion in the research community. Indeed, it is because these two fields are fundamental in network architectures. All the research projects cited above address the shortcomings of the existing Internet naming system. They also emphasize the importance of proposing a new naming architecture for the Future Internet.

In the following, we introduce the existing naming system of Internet and we present its architectural shortcomings.

2.4 Internet Namespaces

The conventional Internet architecture is historically based on end-to-end addressing and on two host-based namespaces which are globally deployed.

On the one hand, there are Domain Names [Moc87a] which provide hierarchical human readable host names. They can be resolved to IP addresses [RMKdG94] by the mean of Domain Name System. In the current Internet, the DNS offers a resolution service. It is responsible for mapping DNS names into IP addresses. The DNS protocol was specified in the early 1980s by the IETF. It is a large-scale, hierarchical, distributed database that converts user-level domain names into IP addresses. This database comprises records that are dispersed in various geographical locations all over the world. In fact, the process of resolving a DNS name into an IP address can require several steps, that is, following a sequence of DNS internal mappings until finally arriving at the required IP address.

On the other hand, IP addresses [RMKdG94] play a more complicated role in the Internet. In the following, we detail the current usages of IP addresses in existing architectures.

2.4.1 IP Addresses: A Dual Role

In the current Internet architecture, IP addresses play a dual role of locators (Loc) and endpoint identifiers (Id) as shown in Figure 2.1.

In fact, from the network layer point of view, these addresses are used as routing information serving to denote the topological location of the hosts in the network. Thus, if a host moves, its location changes and consequently its IP address has to change too. This role is called the *locator* role of an IP address.

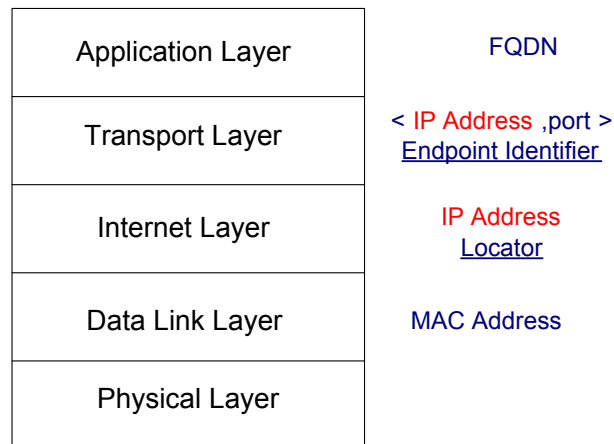


Figure 2.1: The Double Role of IP Addresses

However, from upper layers point of view, IP addresses play a second role which is identifying the host itself during communications and connections. This role is referred to as the *identifier* role of an IP address. At that level, IP addresses are not supposed to change during a communication even if the host changes its location.

To summarize, it means that in the existing Internet, an IP address is supposed to answer to the following three questions :

- Who the host is ?
- Where the host is ?
- How to reach the host ?

2.4.2 Shortcomings of Internet Namespaces

As the Internet evolved from its initial purposes to a more complicated structure, new requirements appeared such as the increasing need of having mobile and multihomed hosts everywhere and a more secure Internet. Unfortunately, Internet architecture, as it was conceived forty years ago, is no longer able to meet those new needs for many reasons. Although being behind the exceptional success of the Internet, there is now an agreement in the research community that the naming and addressing system of Internet is, to a large extent, the reason of Internet's limitations [MZF07].

Today, the Internet is unable to naturally support mobility, security and multi-homing. In the following, we cite some of the Internet's architectural problems related to naming.

- **DNS Latency:** Updating the current IP address in DNS can be too slow to support mobility. DNS provides fast queries but it is not designed for fast updates and quick retrieval of dynamic information. Caching mechanisms were proposed to help DNS support mobility. However, very frequent DNS updates causes inconsistency of caching information [JSBM02][RS04][WTL07]. Furthermore, most hosts do not even have modification access to the DNS servers they are using.
- **The semantic overloading of IP addresses:** The IP address of an endpoint changes whenever the endpoint moves in order to reflect the change in the topological position, thus making the identifier of the endpoint not persistent. For example, a TCP connection uses a quintuplet that includes two IP addresses, each representing an endpoint. If the IP address of one endpoint changes, i.e., when there is mobility involved, the TCP connection fails. Clearly, to handle mobility the transport protocol should be able to refer to the endpoints independent of their network location.

If we add to that the case of multi-homed hosts, the dual role of IP addresses makes the management of multiple and dynamic addresses at the same time harder than necessary.

- **Mechanisms of authentication are not naturally supported:** Attacks like IP address spoofing are very common nowadays.

[MZF07], [Jai06a] in the line of many other papers draw up in detail the different aforementioned problems that encounter the initial naming design of Internet.

2.5 Identifier/Locator (Id/Loc) Separation Concept

The International Telecommunication Union (ITU)¹⁵ has published a series of recommendations that aim at standardizing functions and architectures related to the next generation Internet design.

¹⁵<http://www.itu.int/en/Pages/default.aspx>

The Id/Loc separation has been defined by the ITU-T Recommendation Y.2015 [ITU] as '*decoupling the semantic of IP address into the semantics of node IDs and LOCs. Distinct namespaces are used for node IDs and LOCs so that they can evolve independently. LOCs are associated with the IP layer whereas node IDs are associated with upper layers in such a way that ongoing communication sessions or services shall not be broken by changing LOCs due to mobility and multihoming*'.

Academia and industry have first countenanced the Identifier/Locator separation paradigm [MZF07] as a solution to provide solid basis for mobility and multihoming of terminals and routing scalability [Hus01].

The main idea is to add a new host-level namespace to identify end hosts while continuing to use IP addresses for location purposes only. The deployment of such solutions requires the introduction of an additional resolution system to resolve hosts identifiers to their corresponding locators.

2.5.1 Origins

Identifier/Locator split dates back to Saltzer's paper [Sal93] in which there was pointed out that network nodes and attachment points should be identified separately. The idea was not considered at that time and it is only in the late 1990s that it appeared again.

The Internet Architecture Board (IAB) workshop [MZF07] about naming and addressing held in 2006 focused on routing scalability problems and current Internet addressing architecture limitations. It led up to many interesting observations almost converging to consider the Identifier/Locator split approach as a key solution for the traditional problems of mobility, multihoming, scalable routing and traffic engineering issues. This encouraged the investigation of many architectural proposals. This concept also has been recently introduced in the standardization activities of the ITU Telecommunication Standardization Sector (ITU-T). It studies possible deployment of this concept in the future architectures.

2.5.2 Main Idea

The Identifier/Locator split approach proposes to replace the IP namespace with two separate namespaces : a locator namespace and an identity namespace. The locator namespace is composed of locators that denote the location

of hosts. On the other hand, the identity namespace is composed of identifiers that persistently identify hosts.

From a protocol stack point of view, locators would be used in network layer for routing and location purposes and identifiers would be used in transport and application layers to identify sessions. The separation between locator and identifier roles results in a better support of mobility and multi-homing since locators can change anytime without disrupting ongoing sessions. Figure 2.2 illustrates this new architectural concept.

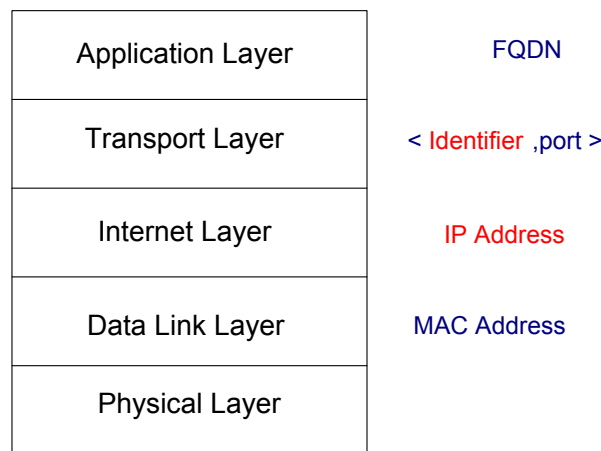


Figure 2.2: The Identifier/Locator Split

The Identifier/Locator split takes an interesting step towards solving the Internet architectural problems. However, it brings significant changes to the existing architecture of Internet and it requires additional costs.

Technically speaking, in order to deploy a new solution based on this concept, the following functional architectural elements are required :

- The introduction of new namespaces of identifiers
- The choice of the convenient types of identifiers and the mechanisms to generate and manage them
- The conception of additional mapping systems to bind new identifiers to corresponding locators

These different technical implications of Id/Loc split concept have been studied in the ITU-T and have been subject to the requirements presented in Section 2.5.3.

2.5.3 Requirements and Design Goals of Identifier/Locator Split Architectures

The goal of this section is to enumerate requirements and design goals to be taken into account when conceiving an Id/Loc-based Future Internet architecture. We later will use these properties to evaluate proposed Id/Loc solutions.

In ITU-T Y2015, authors propose a functional and generic model of Id/Loc split architectures.

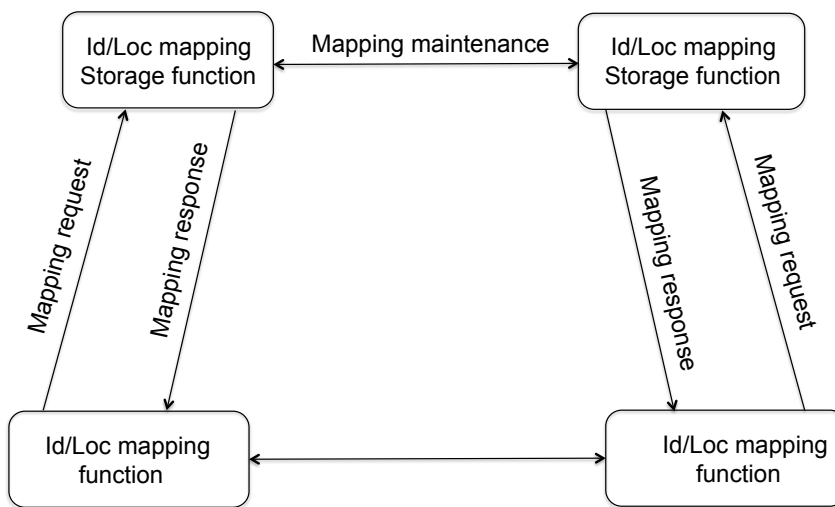


Figure 2.3: ITU functional model for Id/Loc Split [ITU]

The two main functions are the following:

- Mapping Storage Function (MSF) : maintain ID/LOC mapping data.
- Mapping Function (MF) : communicate with each other to distribute, update and retrieve mapping information.

2.5.3.1 ITU-T Requirements on Identifiers and locators

When introducing a Future Internet Architecture based on locator/ID separation, the identifier namespace has to fulfill some mandatory requisites. In the following, we sum up general requirements for identifiers as proposed in ITU-T 2015:

- *Req.id 1*: The identifier decouples the network layer and the upper layers.

- *Req_id 2*: The identifier must be unique within its scope (local or global).
- *Req_id 3*: The identifier must be persistent and location-independent. The relation between the identifier namespace and the locator namespace is of type 1 - n.
- *Req_id 4*: Sessions are tied to identifiers, and not locators.

In addition to these properties we add further requirements and optional properties:

- *Req_id 5*: An identifier is required to be able to identify any type of entities, not only hosts (e.g. users, services, etc.).

This requirement is important because the future Internet will be a network that connects diverse types of entities.

- *Req_id 6*: An identifier can be retrieved by resolving a friendly-user name. This requirement improves the user experience.

- *Prop_id 7*: An identifier can be either permanent or temporary.

For security reasons, temporary identifiers can be used in order to avoid identity spoof attacks.

- *Prop_id 8*: An identifier namespace can be either hierarchical or flat. Hierarchical and flat identifiers can be used depending on the context.

- *Prop_id 9*: The registration process of an identifier should be easy.

The registration process should not cause additional delays in the naming architecture.

2.5.3.2 ITU-T Requirements on Mapping Storage Function

Here are the requirements on Mapping Storage Functions (MSF) as announced by ITU-T.

- *Req-MSF 1*: MSFs must be distributed to avoid single point of failure in the naming system.
- *Req-MSF 2*: Signaling overhead required to maintain the MSF up to date must be low.

- *Req-MSF 3*: Mapping update must be fast.
- *Req-MSF 4*: The mapping information retrieval time shall be lower than the connection setup time.
- *Req-MSF 5*: Security mechanisms are required to avoid eavesdropping entity attacks.

2.5.3.3 ITU-T Requirements on Mapping Function

- *Req-MF 1*: Security mechanisms are required between MSFs and MFs.
- *Req-MF 2*: Compatibility with other classical nodes.

2.5.3.4 Other Requirements

We add the two following requirements:

- Location privacy: In terms of privacy, Identifier/Locator split concept may introduce new tracking possibilities. By knowing an entity's identifier, anyone is able to initiate a lookup in the mapping system to find the whereabouts of that entity.
- Fault tolerance: Identifier/Locator split may allow to send all the locators early in the communication in order to improve fault tolerance.

2.5.4 RRG Architectural Requirements

The IRTF Routing Research Group (RRG) provides several design goals [LE11], among them the decoupling of identifiers and locators.

- **Improved Routing Scalability:** In the last years, Internet has witnessed an explosion of its routing table size [BGT02] as depicted in Figure 2.4.

This routing scalability problem is mainly due to increasing users' demands on Provider Independent (PI) addresses¹⁶. PI addresses directly come from the Regional Internet Registries. So that, they provide flexibility in changing providers. Routing scaling problem necessitates architectural changes and should be taken into consideration as an important requirement of a future Internet architecture.

¹⁶http://en.wikipedia.org/wiki/Provider-independent_address_space

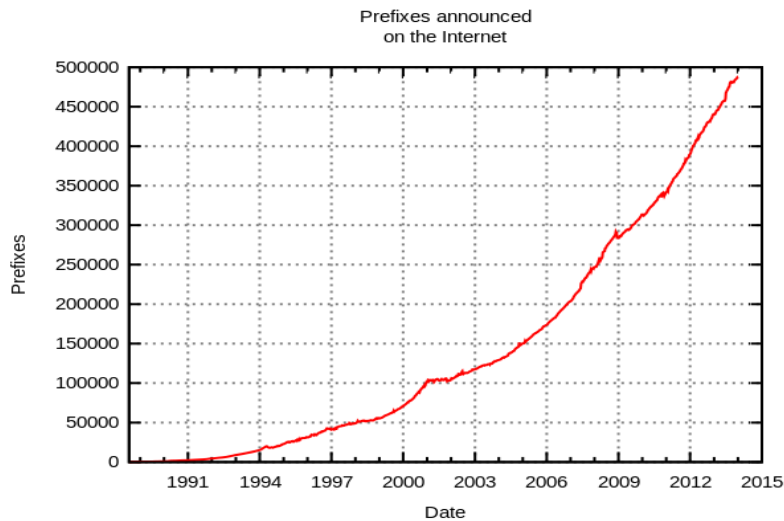


Figure 2.4: Growth of the BGP Table

- **Scalable Support for Mobility** : Internet lacks today fundamental solutions to the mobility problem. In fact, almost the proposed mobility architectures are based today on Mobile IP [Per02] [JPA04] concept. The host in Mobile IP is identified with its IP address. Whenever it changes its network of attachment, the host registers its new address, i.e. care of address (CoA) in Mobile IP terminology, into its Home Agent (HA). HA is the entity which is responsible for mapping home addresses into CoAs and for forwarding packets to the current location of the host.

Such solutions present several limitations, among them the security issues, triangulation problems and reliability and latency issues [SS04]. A naming and addressing architecture proposal should present more efficient solutions to the mobility problem.

- **Scalable Support for Multi-Homing** : Multi-homing is the major reason behind the explosion of routing tables as more than one prefix should be announced in the routing entries. An efficient naming and addressing architecture should provide multi-homing without impacting the size of routing tables.
- **Scalable Support for Traffic Engineering** : Inter-domain traffic engineering today is frequently accomplished by injecting more-specific prefixes into the global routing table, which results in a negative impact

on routing scalability. The idea is to be able in the future to provide traffic engineering while keeping the size of routing tables reasonable.

- **Simplified Renumbering** : Renumbering is not easily supported today in Internet [CAF10]. It also has negative impacts on the routing scaling problem. It is required to make renumbering easier and less costly in future addressing schemes.
- **Deployability** : In order to be deployable, a naming and addressing solution should support already existing functions of the Internet and provide a transition mechanism.

2.6 A Survey of Identifier/Locator Separation Solutions

This section surveys recent proposals that can be potentially applied to define the future Internet architecture based on the Identifier/Locator separation concept.

There is a wide variety of proposed solutions in the literature: Host Identity Protocol (HIP) [MNJH08], Internet Indirection Infrastructure (I3) [SAZ⁺04], HI3 [NAO04], Forwarding directive, Association, and Rendezvous Architecture (FARA) [CBFP03], Locator/Identifier Separation Protocol (LISP) [FFML10], Identifier/Locator Separation Protocol (ILNP) [RA12], Site Multihoming by IPv6 Intermediation (SHIM6) [NB09], and the list is long. In this section, we intend to examine classification approaches of these proposals.

2.6.1 Classification Approaches

In the literature, Identifier/Locator separation proposals have been categorized in several ways. In [PPJ], the authors propose a three-dimensional classification model of naming systems. The model consists of three orthogonal planes, as depicted in Figure 2.6:

- *The management plane* : This plane gathers all the functions related to name formats (hierarchical/flat) and name assignment mechanisms (centralized/distributed authority)

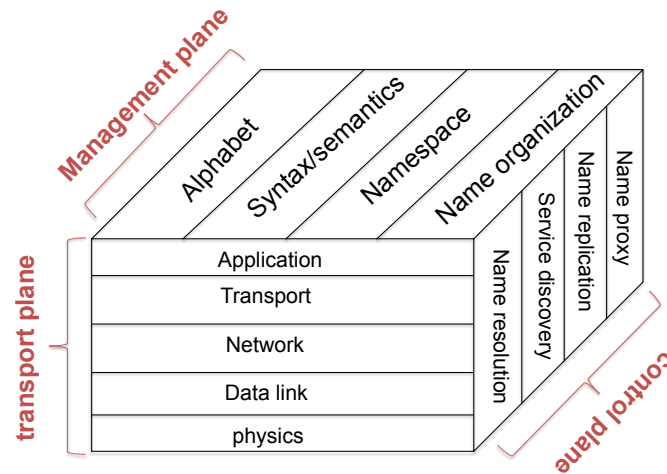


Figure 2.5: Raj Jain Naming Reference Model [PPJ]

- *The transport plane* : This plane deals with the resolution mechanism used in the naming system.
- *The control plane* : This plane is concerned with the reliability and the security aspects of the naming system.

Although being a novel way to classify naming schemes, the model proposed above is very high-level. Functions supported by the management plane and the control plane are included in functional ITU-T requirements on identifier, MSFs and MFs. However this model does not enable to classify solutions of the transport plane which include the Id/Loc split proposals.

In order to be able to provide a refined and sharpened analysis of proposed Id/Loc solutions, we classify proposals with respect to the following categories as depicted in Figure 2.6.

The classification method is based on the used routing mechanism. Therefore, we distinguish two categories:

Routing on flat identifiers: This class of approaches proposes to get rid of classical hierarchical routing and to use new routing mechanisms based on flat identifiers [CCK+06][SGF+10][Cae07]. Examples of this approach are: ROFL (Routing on Flat labels) [CCK+06] and Identity Based Routing (IBR) [SGF+10].

Routing on hierarchical IP addresses: This category is divided into two sub-categories.

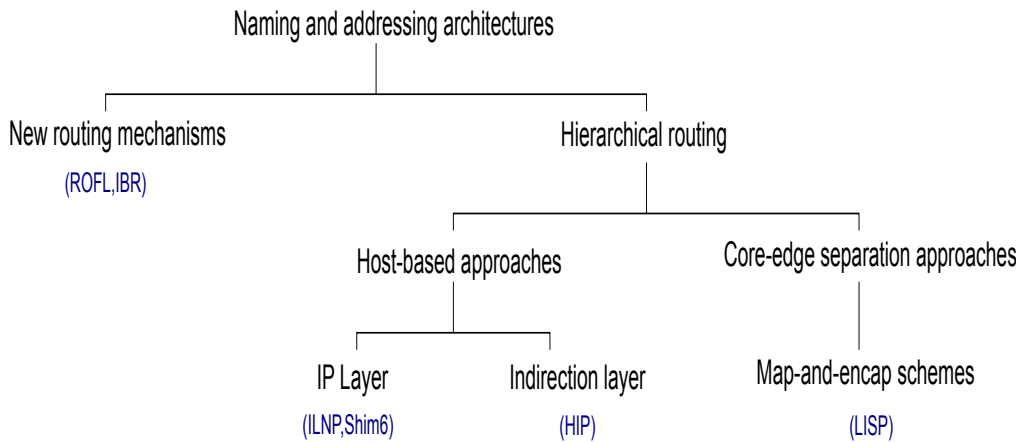


Figure 2.6: Classification of Naming Approaches

- **Core-edge separation approaches:** the split is placed in the network. The basic idea is that there is no change to the end host. The routers take care of the split. At the edge of the network, the identities are resolved into the locators needed for communication. This category splits the existing IP address space into two parts : a topological part that acts as location information and an identification part that identifies the host.
- **Host-based approaches:** the split is placed in the end-host. This approach requires the insertion of a new ID sub-layer usually between the transport and the network layers. Thus, the upper layers are bound to an identity instead of a locator.

In the following we go into details of each scheme and we analyze its benefits and drawbacks. We choose to study proposals that have been standardized by the IETF.

2.6.2 Host-based Schemes

This class of approaches decouples identifiers from locators by two ways:

- *Adding extra naming layer between the network layer and the transport layer:* HIP [MN06] is a typical example of this approach. HIP provides a host-based way of implementing the Identifier/Locator split approach. The original ideas of HIP were presented by Bob Moskowitz in IETF meetings in 1998 and 1999. Thereafter, HIP has gained more popularity

and has been developed by a group of people from Ericsson, Boeing, HIIT, and other companies and academic institutions, first as an informal activity close to the IETF and later within the IETF HIP working group (WG) and the HIP research group (RG) of the Internet Research Task Force (IRTF).

- *Dividing the IP namespace into identifiers and locators:* ILNP [ABH09] is an example of this approach. It is derived from the previous concept of GSE/8+8 [O'D96]. ILNP is currently standardized and recommended by the IRTF Routing Research Group (RRG) in RFC 6115.

This class of solution solves parts of the Internet's problems other than routing scalability.

In the following, we analyze HIP and ILNP solutions following the namespace criteria, the resolution mechanism criteria and the mobility management criteria.

2.6.2.1 Namespaces

In HIP, IP addresses continue to act as pure locators, while HIP introduces a novel, globally unique namespace (the Host Identity namespace).

The elements of the Host Identity namespace are called HITs (Host Identity Tags). They are 128-bit public self-certifying cryptographic keys. They are used to identify hosts in upper layers. The cryptographic nature of HITs allows to integrate strong security features such as authentication, confidentiality, integrity, and protection against certain kind of Denial-of-Service (DoS) and Man-in-the-Middle (MitM) attacks. The protocol stack of a HIP node is depicted in the following figure 2.7.

The way with which ILNP splits the roles of identification and location is different. ILNP [RA12] does not introduce an additional namespace. It rather divides the existing address space into Endpoint Identifiers and Routing Locators.

In fact, the 128-bit IPv6 addresses in the packet headers are split into 64 bits for the Routing Locator and 64 bits for the Endpoint Identifier. The Locator has significance only in the network layer, and the Identifier has significance only in the transport layer. In addition to that, whereas the use of IP addresses at the application layer is quite common, ILNP is strict about only using fully qualified domain names (FQDN) at the application layer, as illustrated in Figure 2.8.

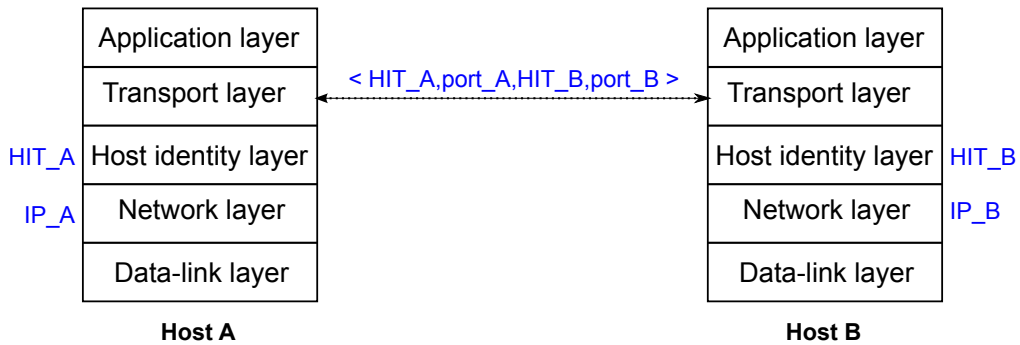


Figure 2.7: HIP Host Protocol Stack

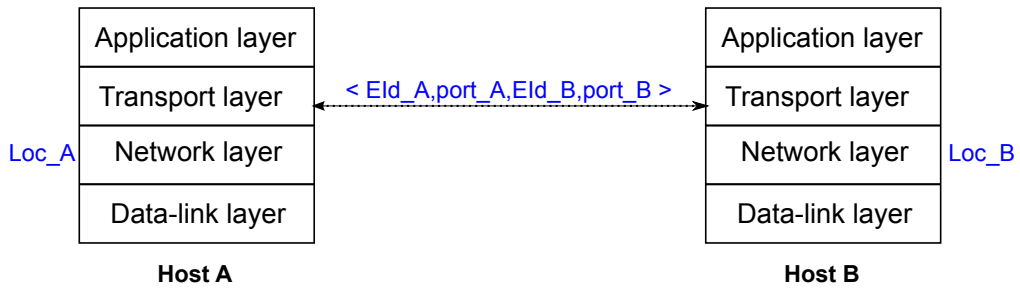


Figure 2.8: ILNP Host Protocol Stack

2.6.2.2 Resolution mechanism

HIP introduces a new mechanism, called the Rendezvous Server (RVS) [LE08], responsible for making the mapping between IP address(es), HIs and HITs. RVS is the equivalent of MSF in the ITU-T terminology.

The main advantage of a RVS comparing to a classical DNS-based location service is its ability to update its records, and thus the network information, within a short time. This makes its use suitable with the increasing need of mobility. Each host in the network has to register to one or more RVS referring to the mechanism described in [LKE08][LE08]. And each time the host changes one of its IP address (es), it has to inform it(s) RVS to keep it (them) updated with the new changes.

The connection establishment between two HIP hosts, initiator and responder, is performed as described in Figure 2.9. This process is called the Base Exchange (BE).

The initiator looks up the responder's FQDN in DNS. As a result, it gets the Host Identifier (HI), HIT(s) and corresponding RVS IP address. The HI is a public key and directly represents the Identity of the host. A HIT is a hash

of the HI. The first message in the four way handshake (I1) passes through the RVS, and is no longer sent directly to the IP address of the responder. However, the rest of the HIP messages (R1, I2 and R2) are communicated directly between the two hosts.

When receiving an I1 packet, a RVS checks that the HIT contained in the receiver's HIT field of the packet header matches one of the HITs of its nodes. If so, it replaces the destination IP address of the packet by one of the responder's IP addresses, it recomputes the IP checksum. In addition, the source IP address of the packet is changed from the initiator IP address to the RVS IP address.

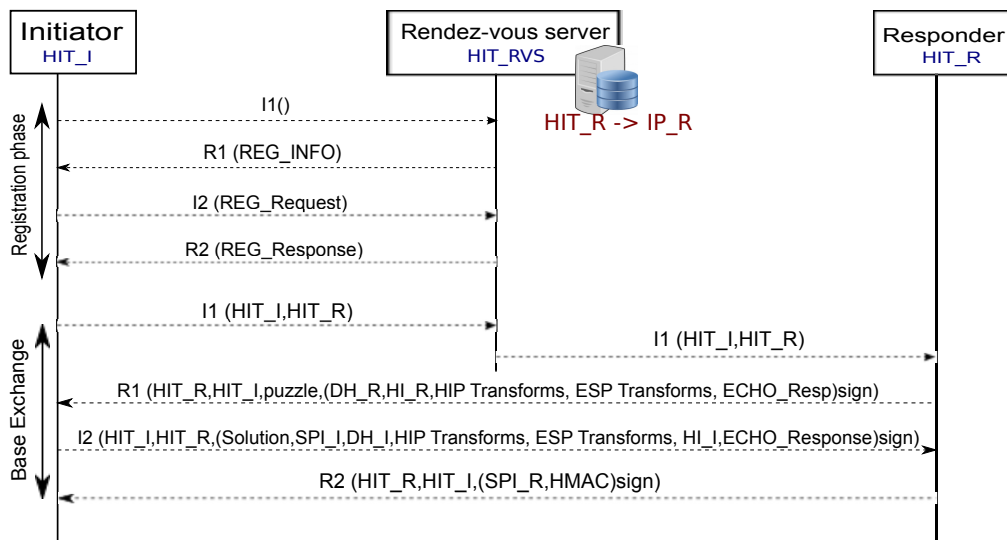


Figure 2.9: HIP Registration and Base Exchange Mechanisms

The resolution mechanism of ILNP is based on DNS system. It uses it as a location service manager to provide mappings between FQDNs, locators and identifiers.

A single query to the DNS by the initiator using the FQDN of the Correspondent Node (CN) would yield the Identifier and the Locator(s) of the CN. The MN uses the Secure Dynamic DNS Update to update the DNS about its current location every time it changes a Locator. The initiator then sends an initial packet (e.g. TCP SYN, UDP) to the responder at one of the Locators provided by the DNS.

2.6.2.3 Answers to functional ITU Requirements

In Table 2.2, we summarize the answers of both HIP and ILNP to the ITU-T functional requirements.

Functional ITU requirements	HIP	ILNP
Req_id 1	Yes	Yes
Req_id 2	Yes	Yes
Req_id 3	Yes	Yes
Req_id 4	Yes	Yes
Req_id 5	hosts only	hosts only
Req_id 6	Yes	Yes
Prop_id 7	permanent only	permanent and temporary
Prop_id 8	flat (work in progress on hierarchical HITs)	hierarchical
Prop_id 9	requires security mechanisms	easy
Req_MSF 1	Centralized	Centralized
Req_MSF 2	No	Yes
Req_MSF 3	to be further evaluated	to be further evaluated
Req_MSF 4	to be further evaluated	to be further evaluated
Req_MSF 5	No	No
Req_MF 1	Yes (registration mechanism)	No
Req_MF 2	No	Yes
location privacy	to be further evaluated	to be further evaluated
fault tolerance	No	No

Table 2.2: HIP and ILNP Answers to functional ITU Requirements

2.6.2.4 Answers to RRG Design Goals

- **Routing Scalability:**

HIP allows the use of Provider Aggregatable (PA) addresses. So, address aggregation is possible without any change in routing system which makes HIP a scalable solution.

In ILNP, hosts can be multi-homed and by using PA addresses, address aggregation is completely possible. So, ILNP is considered as a scalable solution.

- **Mobility:** The HIP mobility architecture extension is described in [NHVA08]. HIP defines a new *locator* parameter that contains the current IP address(es) of the sending entity. For example, when the mobile host changes its location and therefore IP address, it generates a HIP control packet with one or more Locator parameters, protects the packets integrity, and sends the packet to its currently active peer hosts. Note that the IP version of the locators may vary; it is even possible to use both IPv4 and IPv6 addresses simultaneously, and make a decision of the IP version used on outgoing IP packets depending on a local policy. The mobile node also has to update its current location within its RVS. To summarize, we can say that HIP relies on a host-based mobility approach. The mobility procedure in ILNP is processed as follows. When a mobile node changes its location, it first updates its DNS entry. Then, it sends an ICMP Locator Update message to each of its current correspondents. The ICMP Locator Update message contains all currently valid Locators for the originating node.
- **Multi-homing:** HIP multi-homing extension is defined in [NHVA08]. Multi-homing in HIP is provided in the same way as mobility. Multi-homed hosts announce their IP addresses using the locator parameter described above. Multi-homing in ILNP is also performed with the same way as mobility. The host uses an ICMP Locator Update message to declare all its new locators to its correspondent nodes. It also update the DNS.
- **Traffic engineering:** In both HIP and ILNP, traffic engineering (TE) is facilitated. Policies can use node identity regardless of location, making it easier to configure and maintain TE policy.
- **Renumbering:** Renumbering is no longer costly in HIP and ILNP. When users change their service providers and get different locator prefixes, their identifiers remain unchanged

HIP and ILNP answers to RRG design goals are summarized in the following Table.

	HIP	ILNP
Routing Scalability	Yes	Yes
Mobility	Yes	Yes
Multi-homing	Yes	Yes
Traffic Engineering	Yes	Yes
Renumbering	Yes	Yes

Table 2.3: HIP and ILNP Answers RRG Requirements

2.6.3 Map-and-Encap Schemes

LISP is standardized in RFC 6830. It has been chartered as Working Group [17](#) in the IETF and has been already deployed in an international test-bed [[KIF11](#)].

2.6.3.1 Namespaces

LISP can be seen as adding an extra communication layer below the existing one, as illustrated in Figure 2.10.

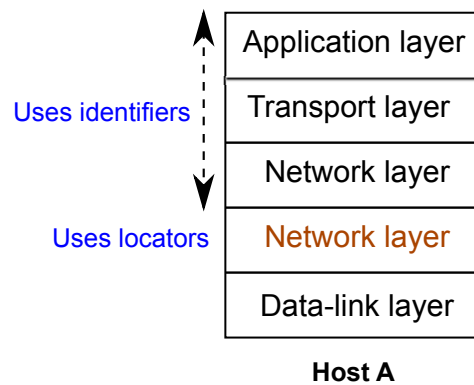


Figure 2.10: LISP Node Protocol Stack

LISP splits the semantic of IP addresses into two functions: The Endpoint Identifiers (EIDs) and the Routing Locators (RLOCs).

LISP implements a Map-and-Encap scheme [[SIBF12](#)]. Packets are encapsulated at the border router of the sender domain (called the Ingress Tunnel Router (ITR)) and decapsulated at the border router of the receiving domain

¹⁷<https://datatracker.ietf.org/wg/lisp/charter/>

(the Egress Tunnel Router (ETR)). This makes it possible for the core routing (the routing between the domains) to be independent of the encapsulated Endpoint Identifiers and thus be optimized for the topological characteristics of the core network.

2.6.3.2 Resolution Mechanism

If a host in one LISP-capable domain wants to send a packet to a host in another LISP-enabled domain, the following happens as depicted in Figure 2.11.

- The host looks up the name of the correspondent host in DNS, which gives an Endpoint Identifier.
- The host puts its Endpoint Identifier as the source and the correspondent host's Endpoint Identifier as the destination.
- The packet traverses to the ITR. The ITR encapsulates the packet in a new packet with the Routing Locator of the ITR as the source and the Routing Locator of an ETR for the domain as the target (this mapping is either previously cached or is determined by the mapping mechanism).

For the mapping infrastructure, a number of approaches have been proposed; among them are LISP-CONS (Content distribution Overlay Network Service for LISP) [BCF⁺08], LISP-NERD (a Not-so-novel EID-to-RLOC Database) [FFM⁺13], LISP+ALT (LISP Alternative Logical Topology) [FFML11] and LISP-TREE [JCAC⁺10].

LISP-CONS is a control-plane protocol for distributing identifier-to-locator mappings for LISP. LISP-CONS operates on a distributed Endpoint Identifier-to-Routing Locator (EID-to-RLOC) database. This database is distributed among the authoritative Answering Content Access Resources (Answering-CAR). An Answering-CAR (aCAR) advertises 'reachability' for its EID-to-RLOC mappings through a hierarchical network of Content Distribution Resources (CDRs), and responds to mapping requests from the system. LISP-NERD uses a signed database of EID to RLOC mappings. A Content Delivery Network (CDN) [xin09] is used to distribute signed databases and updates. Successive incremental updates are used to keep databases up to date without having to retrieve entire copies. In LISP-NERD, ITRs contain entire mapping database.

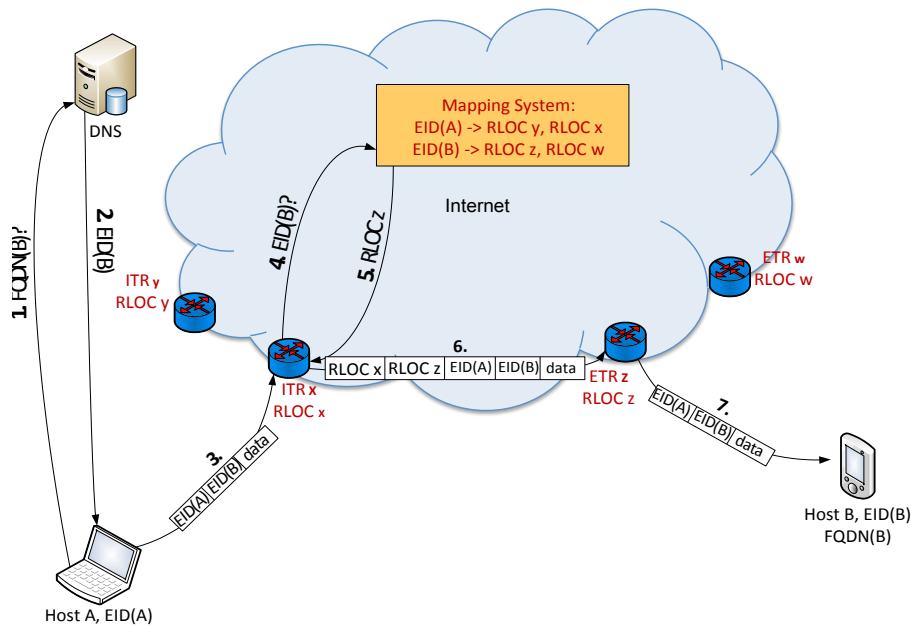


Figure 2.11: LISP Architecture

LISP-TREE is based on DNS and has a similar hierarchical topology: blocks of EIDs are assigned to the levels of the hierarchy by following the current IP address allocation policy. It can work with the existing DNS implementations, providing the benefit of 20 years of operational experience.

The most widely used approach is LISP-ALT. LISP-ALT uses the Border Gateway Protocol (BGP) [RL94] and generic routing encapsulation (GRE) [HLFT94] to construct an overlay network for advertising Endpoint Identifier prefixes. Because the mapping mechanism is decoupled from the forwarding mechanism, however, any mapping mechanism can be used.

2.6.3.3 Answers to Functional requirements

In Table 2.4, we present LISP answers to functional requirements of the ITU-T.

2.6.3.4 LISP Answers to RRG Design Goals

- **Routing Scalability:** LISP offers a solution to reduce the BGP routing table size. In fact, RLOCs in LISP are Provider Aggregatable (PA) addresses.
- **Mobility:** LISP-MN [NJPC⁺13] is a LISP version that supports host

Functional ITU requirements	LISP
Req_id 1	Yes
Req_id 2	Yes
Req_id 3	No
Req_id 4	Yes
Req_id 5	hosts only
Req_id 6	No
Prop_id 7	permanent
Prop_id 8	hierarchical
Prop_id 9	easy
Req_MSF 1	Distributed
Req_MSF 2	high
Req_MSF 3	to be further evaluated
Req_MSF 4	to be further evaluated
Req_MSF 5	No
Req_MF 1	No
Req_MF 2	Yes
location privacy	to be further evaluated
fault tolerance	No

Table 2.4: LISP Answers to functional ITU Requirements

mobility. In LISP-MN, the device itself implements a lightweight version of LISP. Every mobile node receives an EID address from its home network and keeps this EID independently of its location. Mobile nodes also receive addresses that belong to the foreign network they are visiting. These addresses are used as RLOCs. A new mapping is registered to the Map-Server of its home network by the mobile node each time it moves and changes RLOCs (i.e., visited network). The mappings bind the EID of the mobile device to the RLOCs received from the visited network. The Map-Server does not need to advertise the EID address to the mapping system as it belongs to the less specific prefix it already advertises. The mobility is thus transparent for the mapping system, ensuring scalability.

- **Multi-homing:** LISP provides host and site multi-homing without increasing the BGP routing table size
- **Traffic engineering:** LISP provides ingress and egress traffic engineering [LWW11]. In fact, the separation between EIDs and RLOCs makes possible to deploy a traffic engineering service controlling both incoming and outgoing packet flows. For example, ranking RLOCs in the mapping system can be a way to implement ingress or egress traffic engineering in LISP.
- **Renumbering:** LISP provides simplified renumbering.

2.7 Comparison and Analysis

	HIP	ILNP	LISP
Type of approach	host-based	host-based	network-based
Architecture	indirection	changes in the semantics of an IP address	map-and-encap
New network entities required	Yes (RVS)	No	Yes (LISP Routers)
Changes in DNS	Yes (new RR)	Yes (new RR)	No
IPv4 support	Yes	Possibly	Yes
IPv6 support	Yes	Yes	Yes
Routing table size reduction	Yes	Yes	Yes
Host mobility	Yes	Yes	In progress
Host multi-homing	Yes	Yes	Not currently defined
Traffic engineering	Yes	Yes	Yes
Renumbering	tbd	tbd	tbd
Multicast	Yes	Yes	Not currently defined
NAT traversal	Yes	Yes	In progress
Mobile networks	Yes	Yes	Not currently defined
Security	Yes	No	No

Table 2.5: Comparative Analysis of Naming Schemes

2.8 Discussion

In the comparison presented above, we have analyzed two types of Identifier/Locator approaches, i.e. network-based approach and host-based approach. We have chosen to present LISP as a candidate of network-based approaches because LISP is today the most famous solution in this category. Actually, there is today an international LISP Cisco-operated network deployed over 60 sites covering 10 countries all over the world. This network has been operational since more than three years and is used for demonstration purposes and proof-of-concept. OpenLISP¹⁸ is an open source implementation of LISP.

On the other hand, the rationals between choosing HIP and ILNP as representative solutions of host-based approaches are the following. First, HIP is one of the first protocols that implement the Identifier/Locator separation concept with respect to an indirection scheme. Moreover, HIP presents many interesting security properties. Today, there are three public known implementations of HIP : HIP4BSD¹⁹ , HIPL²⁰ and OpenHIP²¹.

ILNP is a more recent proposal comparing with HIP and LISP. The idea of ILNP has been approved by IETF because the protocol presents a different way of solving the naming problem. To our knowledge, there is no current implementation of ILNP. However, [AB12] enumerates the deployment requirements of ILNP.

Now, let us deep in more details in the technical aspects of these three naming proposals. Although technically different, the three proposals have a main common point. They rely on adding an indirection level between the location space and the naming space. In LISP and ILNP for instance, this indirection is allowed through a semantic separation of the meanings of an IP address. In HIP, the separation is more tough. HIP radically separates locators from identifiers by adding a new namespace to the Internet.

It can be seen from Table 2.5 that LISP main strong points are the following. In the line of other network-based solutions, it requires no changes to the hosts. That is, LISP can be deployed with a minimal configuration changes at the level of core routers only. It is then incrementally deployable

¹⁸<http://www.openlisp.org/>

¹⁹<http://www.hip4inter.net>

²⁰<http://hipl.hiit.fi>

²¹<http://www.openhip.org>

and interoperable with the existing Internet addressing architecture.

For host-based approaches, things are different. HIP requires for instance stack changes in the end hosts. It makes HIP not incrementally deployable. HIP provides a clean separation architecture. For that, it requires the introduction of new core components, mainly the RVS infrastructure. HIP also requires changes in the DNS system by adding new corresponding HIP records. HIP communications are also very secure. However, there is of course a tradeoff between providing clean mobility and security support and real performances. All these facts can make the HIP architecture 'unrealistic' and missing of credibility in a real-world scenario.

ILNP is also a host-based split approach but it achieves the separation in a different way than HIP. It does not add a new namespace. However, similarly to HIP it requires changes to the hosts. The strongest point of ILNP is its interoperability with other IP networks. An ILNP node can communicate normally with a non-ILNP node. However, the reliance on DNS as a location manager in ILNP can cause some doubts regarding the performance of the protocol in high mobile scenarios. It is somehow the same problem of the existing Internet. An additional fundamental problem of ILNP is the lack of location privacy. Any one can look up the FQDN of a host and can get its set of identifiers and locators. Although architecturally not so complicated, several properties of ILNP should be further studied.

Now, let us investigate this important question ' Why Identifier/Locator split solutions have not been yet deployed?'. What are the primary reasons? Are weaknesses in technical design or disadvantages comparing to substitutes behind that?

It seems that although positive feedbacks regarding the architectural concept are here, real world deployability and business reasons make things more complicated. People still consider identifier/locator split as a big change in networks. Different stakeholders including OS vendors, ISPs and academia should push toward adopting this approach and defending its benefits. The first step toward that is to work further on performance evaluations of these approaches.

2.9 Chapter Conclusion

This chapter has presented the naming and addressing concepts that are the basis of our research work. The chapter has presented in three main sections

the following fields: naming and addressing basis of the Internet, Internet's problems related to its two-level naming scheme and the benefits behind deploying Id/Loc split proposals. The first section explains why naming becomes problematic in the existing architecture and why it is important to solve the double role problem, as well as its relationship with other networking features. The Id/Loc split approach has been analyzed from network-based and host-based perspectives.

The state of the art presented in this Chapter allows us to understand the complexity of the naming problem. Thus, the mandatory questions are: 1) What are the performances of these approaches? 2) Can these solutions apply in a user-level environment? The following two chapters address these two questions. Chapter 3 presents performance evaluation results of Id/Loc split concept. Chapter 4 presents an answer to the second question. It studies the possible use of these solutions in a user-level context.

Chapter 3

Cost Analysis of Identifier/Locator Split Solutions

3.1 Introduction

From previous Chapter 2, we have realized that research efforts conducted to overcome the problem of naming have given much attention to the Identifier/Locator split paradigm [MZF07].

Although several technical approaches have been proposed and analyzed, the exact performance of these systems is still unclear. In the literature, we find several work [SJR09][LPJX08][TMS12][YJ12] that focuses on analyzing the advantages and peculiarities of Id/Loc split approaches from a theoretical view. However, despite such an effort, quantitative performance studies of such approaches are missing. There has been no comprehensive cost analysis of Id/Loc separation approaches that takes into account all possible costs.

In this chapter, we develop an analytical cost model for studying the performances of HIP, ILNP and LISP. Our main motivation is to compare the performance of host-based and network-based Id/Loc split approaches through the study of these three protocols. Therefore, we develop corresponding analytical cost models and we study the following performance metrics:

- The connection establishment cost
- The data packet delivery cost

- The mobility signaling cost

We also present numerical results to demonstrate the impact of the above cited metrics on the total cost, and thus on the efficiency of each proposal. We believe that our cost analysis will help network architects and engineers to study the behavior of Id/Loc split architectures and to discuss possible deployments.

3.2 Definition of Costs

Our motivation behind carrying out different analyses is mainly to investigate the strong and weak points of each identifier/locator split scheme. We can hence be able to draw out conclusions and perspectives, paving the way towards proposing enhancements or even a novel scheme. For this rationale, we consider this work as an essential step and one of the corner stones of the thesis.

We consider the cost of data/bytes/packets' transmission through the network. This shows the load on the network and evaluates the impact of each Id/Loc scheme. In IP networks, the transmission cost is proportional to the distance in hops between the source and the destination [XA02]. Thus, we calculate a cost as the product of the transmitted data size and the traversed hop distance.

Hereafter, we present the considered criteria and metrics for protocols analyses. Because Id/Loc concept brings changes to communication establishment and processing, we consider the following three types of costs:

- **The connection establishment cost (CEC):** It is the accumulative resolution messages overhead required to obtain the destination host's IP address. CEC is calculated as the product of the size of the resolution messages and the distance in hops [LC10][PKCP09].
- **The data packet delivery cost (DPC):** It represents the cost of delivering data packets between two hosts in the network. It is calculated as the product of the data packet size and the distance in hops between the two hosts.
- **The mobility signaling cost (MSC):** It is the accumulative mobility signaling messages cost required to keep the mobile host (MH) reachable.

We have chosen to study these three criteria because of the following reasons:

CEC quantifies the impact of adding a new resolution step in the session establishment procedure. It can then decide of the efficiency of the scheme.

DPC quantifies the difference between processing data in an end-to-end approach and a map-and-encap approach.

MSC quantifies the delays required by each scheme to deal with a mobility scenario. As Id/Loc split concept has been basically introduced to solve mobility problems in the existing architecture, MSC is a very important criteria to take into consideration.

3.3 Preliminaries

3.3.1 System Modeling

In this section, we develop analytical models to study several costs of Identifier/locator split architectures. We consider an all-IP architecture based on wireless and wired networks with hexagonal cell structure as depicted in Figure 3.1. We further assume that each cell is served by one access router. The number of rings represents the network size R . Figure 3.1 shows a network with $R = 3$ as it is having 3 rings.

In our model, a Mobile Host (MH) is a host in movement within the network. It can then change its location from one cell to another. An MN can be in communication with one or more Correspondent Hosts (CHs). A CH is also supposed to be within the network. We assume that CHs do not move and have a fixed location in the network.

An IP handover rate is equal to the cell-boundary crossing rate. The residence time of an MH in a given cell is a random variable which follows an exponential distribution with mean value $1/\mu_c$. We consider then the fluid-flow mobility model [KJ05] [AW02] to represent the MH's movement. Under this model, it is assumed that the direction of the movement is uniformly distributed over the range $]0, \pi]$.

The cell boundary crossing rate is expressed as follows :

$$\mu_c = (vP) / (\pi A)$$

where :

- v is the average movement speed of an MH (expressed in m/s)

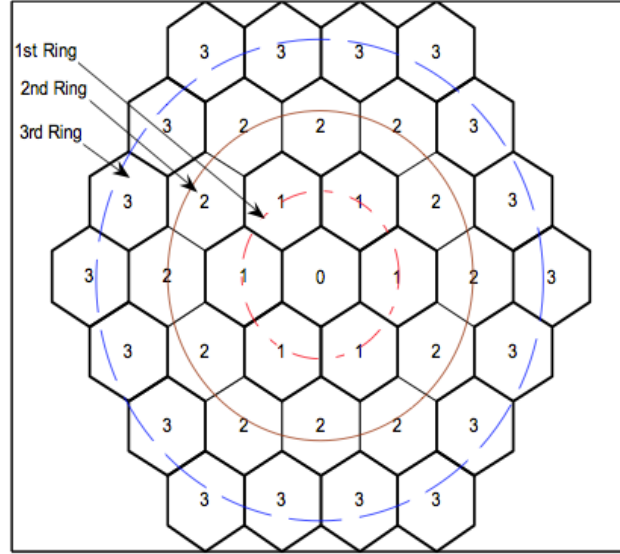


Figure 3.1: Network Configuration Model

- P is the cell perimeter
- A is the cell's area

Considering a hexagonal-shaped cell side length L , we have :

$$P = 6L, A = (3\sqrt{3}/2) L^2$$

and hence

$$\mu_c = (4\sqrt{3}/3\pi) (v/L)$$

Table 3.1 shows the main parameters and their descriptions.

3.3.2 Assumptions

HIP Network : We assume as shown in Figure 3.2 that all the network nodes are served by one RVS. The distances between an MH and RVS and a CH and RVS are denoted $d_{MH,RVS}$ and $d_{CH,RVS}$ respectively. The distances between an MH and DNS and a CH and DNS are $d_{MH,DNS}$ and $d_{CH,DNS}$. In our model, we assume that : $d_{MH,RVS} = d_{CH,RVS}$

Notations	Descriptions
N_{CH}	The average number of CHs which are communicating with MH
$d_{x,y}$	The average hop distance between entity x and entity y
μ_c	The cell boundary crossing/handover mean rate
μ_s	The session duration mean rate
λ_s	The session arrival mean rate to MH
$C_{Protocol}^{Packet}$	The cost of processing packet
$Size_P$	Size of packet P in bytes

Table 3.1: List of Parameters used in the Analytical Model

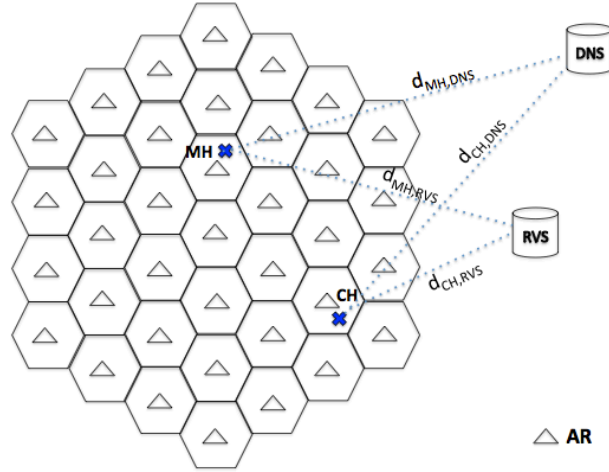


Figure 3.2: HIP Network Configuration Model

LISP Network : The LISP network configuration is shown in Figure 3.3. Each cell contains an AR which can serve as an ITR and an ETR. We also assume that the resolution structure is constructed of only one resolver server.

ILNP Network : The ILNP network configuration is depicted in Figure 3.4. We consider that the network area is served by one DNS server.

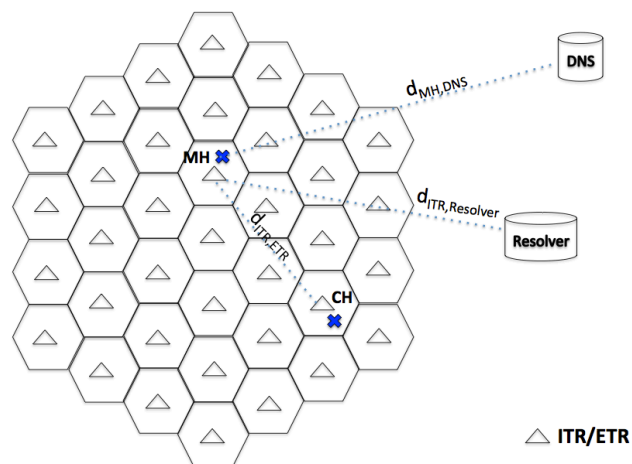


Figure 3.3: LISP Network Configuration Model

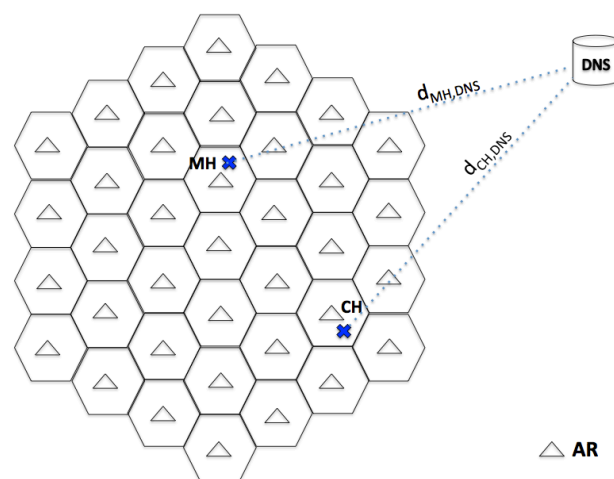


Figure 3.4: ILNP Network Configuration Model

3.4 Connection Establishment Signaling Cost (CEC)

In this section, we calculate the connection establishment cost in a HIP-based network, a LISP-based network and an ILNP-based network.

3.4.1 HIP Connection Establishment Cost CEC (HIP)

The connection establishment flow messages in the HIP case is shown in Figure 2.9. The resolution mechanism in HIP includes two main phases. In the first phase, the initiator interrogates the DNS to obtain the HIT of the responder's RVS. Then in the second phase, it starts the base exchange. Thus, CEC (HIP) is calculated as the sum of the cost of the DNS query and the cost of the base exchange. It is expressed as follows :

$$CEC(HIP) = \lambda_s (2 C_{DNS}^{IPv6} + C_{HIP}^{I1} + C_{HIP}^{R1} + C_{HIP}^{I2} + C_{HIP}^{R2}) \quad (3.1)$$

Where :

$$C_{HIP}^{I1} = d_{MH,RVS} * Size_{I1.to.RVS} + d_{RVS,CH} * Size_{I1.via.RVS}$$

$$C_{HIP}^{R1} = d_{MH,CH} * Size_{R1}$$

$$C_{HIP}^{I2} = d_{MH,CH} * Size_{I2}$$

$$C_{HIP}^{R2} = d_{CH,MH} * Size_{R2}$$

3.4.2 LISP Connection Establishment Cost CEC (LISP)

In a LISP-based network, establishing a connection between two hosts requires the following steps. The initiator first queries the DNS to obtain the responder's EID. It then sends a normal IPv6 packet to its ITR. The ITR interrogates the resolver via a Map Request message to obtain the RLOC of the responder's ETR. The resolver responds to the ITR via a Map Reply message. In our analysis, we assume that the resolver always holds the RLOC of the ETR, and thus, it does not interrogate the resolution infrastructure. This case corresponds to the lowest cost of a connection establishment in LISP. CEC (LISP) is then expressed as follows :

$$CEC(LISP) = \lambda_s (2 C_{DNS}^{IPv6} + C_{MH,ITR}^{IPv6} + C_{ITR,Resolver}^{Map-request} + C_{Resolver,ITR}^{Map-reply}) \quad (3.2)$$

Where :

$$C_{DNS}^{IPv6} = Size_{IPv6} * d_{MH,DNS}$$

$$C_{MH,ITR}^{IPv6} = Size_{IPv6} * d_{MH,ITR}$$

$$C_{ITR,Resolver}^{Map-request} = Size_{Map-request} * d_{ITR,Resolver}$$

$$C_{Resolver,ITR}^{Map-reply} = Size_{Map-reply} * d_{Resolver,ITR}$$

3.4.3 ILNP Connection Establishment Cost

The ILNP-based initiator interrogates the DNS to obtain a vector of responder's identifiers and locators. Thus, CEC (ILNP) is calculated as follows:

$$CEC(ILNP) = \lambda_s (2 C_{DNS}^{IPv6}) \quad (3.3)$$

Where :

$$C_{DNS}^{IPv6} = Size_{IPv6} * d_{MH,DNS}$$

3.5 Data Packet Delivery Cost (DPC)

In this section, we calculate data packet delivery costs in a HIP-based network, a LISP-based network and an ILNP-based network.

3.5.1 HIP Data Packet delivery Cost

Once the base exchange is performed, the initiator starts sending HIP data packets to the responder. HIP packets are ESP encapsulated packets. Thus, DPC (HIP) is expressed as follows:

$$DPC(HIP) = \mu_s * N_{CH}(C_{HIP}^{packet}) \quad (3.4)$$

Where :

$$C_{HIP}^{packet} = d_{MH,CH} * Size_{HIP}$$

3.5.2 LISP Data Packet delivery Cost DPC(LISP)

As explained in Section, LISP is a map-and-encap protocol. It means that, the LISP node sends normal IPv6 data packets to the ITR. This latter encapsulates them in an additional IPv6 header containing the RLOCs of ITR and ETR as source address and destination address. DPC (LISP) is calculated as follows :

$$DPC(LISP) = \mu_s * N_{CH} (C_{MH,ITR}^{packet} + C_{ITR,ETR}^{packet} + C_{ETR,CH}^{packet}) \quad (3.5)$$

Where :

$$C_{MH,ITR}^{packet} = d_{MH,ITR} * Size_{IPv6}$$

$$C_{ITR,ETR}^{packet} = d_{ITR,ETR} * Size_{LISP}$$

$$C_{ETR,CH}^{packet} = d_{ETR,CH} * Size_{IPv6}$$

3.5.3 ILNP Data Packet delivery Cost

The data packets in an ILNP network are IPv6 packets with specific ILNP header.

$$DPC(ILNP) = \mu_s * N_{CH} (C_{MH,CH}^{packetILNP}) \quad (3.6)$$

Where :

$$C_{MH,CH}^{packetILNP} = Size_{ILNP} * d_{MH,CH}$$

3.6 Mobility Signaling Cost (MSC)

3.6.1 Mobility Signaling Cost of HIP MSC (HIP)

In HIP, upon a handover, the MN sends UPDATE packets to each of its CHs to inform them with its new location. It then sends UPDATE messages to its

RVS to update its location. We assume that there is one RVS serving all the network hosts. Then, the SC in HIP is expressed as follows :

$$MSC(HIP) = \mu_c (C_{RVS}^{update} + N_{CN} * C_{CN}^{update}) \quad (3.7)$$

Where :

C_{RVS}^{update} is the cost of updating the RVS with the new location of MN. It is calculated as follows.

$$C_{RVS}^{update} = d_{MH,RVS} * (Size_{updatemsg1} + Size_{updatemsg2} + Size_{updatemsg3})$$

C_{CH}^{update} is the cost of updating a CH with the new location of MH. It is calculated as follows.

$$C_{CH}^{update} = d_{MH,CH} * (Size_{updatemsg1} + Size_{updatemsg2} + Size_{updatemsg3})$$

3.6.2 Mobility Signaling Cost of LISP

For each new RLOC obtained by the LISP-MN, the node has to inform about the new EID-to-RLOC binding to its Map-Server. In order to do so LISP node sends the Map-Register signalling message that includes the EID and the RLOC. The message may include multiple RLOCs if the node is multi-homed and LISP supports any combination of IPv4 and IPv6 for EIDs and RLOCs. The LISP-MN and the Map-Server share a pre-configured key. This key is used to sign the Map-Register to ensure authentication. Once the Map-Server receives a valid Map-Register containing an EID-to-RLOC mapping it will make it accessible throughout the Mapping-System. Thus, MSC(LISP) is expressed as follows:

$$MSC(LISP) = \mu_c (C_{Resolver}^{update}) \quad (3.8)$$

Where :

$$C_{Resolver}^{update} = d_{MH,Resolver} * Size_{Map-Register}$$

3.6.3 Mobilty Signaling Cost of ILNP

$$MSC(ILNP) = \mu_c (C_{DNS}^{update} + N_{CH} * C_{CH}^{update}) \quad (3.9)$$

Where :

C_{DNS}^{update} is the cost of updating the DNS

C_{CH}^{update} is the cost of updating the CH

3.7 Numerical Results

Based on the cost models given in the previous section, we now compare the numerical results. In Table 3.2, we present the messages sizes which we have obtained from the protocols specifications [MN06][FFML10][AB12] .

Message	Size in bytes
$Size_{IPv6}$	120
$Size_{Map.request}$	80
$Size_{Map.reply}$	80
$Size_{I1.to.RVS}$	60
$Size_{I1.via.RVS}$	100
$Size_{R1}$	144
$Size_{I2}$	172
$Size_{R2}$	88
$Size_{update.msg-1}$	112
$Size_{update.msg-2}$	100
$Size_{update.msg-3}$	76
$Size_{HIP}$	136
$Size_{LISP}$	184
$Size_{MapRegister}$	88

Table 3.2: Numerical Values of Messages Size

For parameters' values, we set the following default values : $d_{MH,Resolver} = 20$, $d_{MH,CH} = 15$, $d_{MH,DNS} = 30$, $d_{MH,RVS} = 20$, $d_{ITR,Resolver} = 18$, $d_{MH,ITR} = 2$, $\mu_c = 4mn$, $R = 3950m$

3.7.1 Impact of N_{CH}

Figure 3.5 investigates the impact of the number of correspondent hosts on the connection establishment cost in the case of a HIP-network, a LISP-network and an ILNP-network. We vary the number of N_{CH} from 0 to 20. As N_{CH} is increasing, it appears clearly that CEC is increasing too in the three cases. This appears to be an obvious result because if we increase the number of hosts, it means we increase the number of sessions and thus, we increase the cost of establishing sessions. However from Figure 3.5, we can see that ILNP

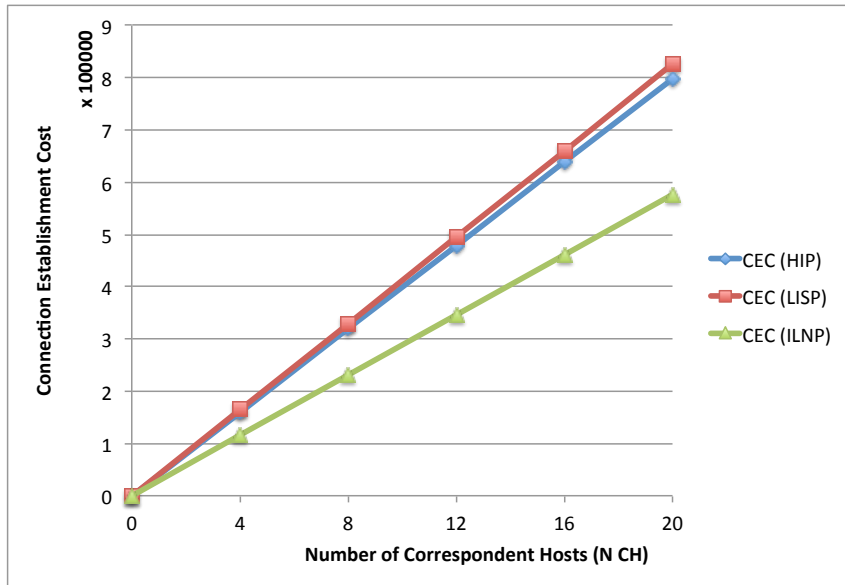


Figure 3.5: Impact of N_{CH} on Connection Establishment Cost

outperforms HIP and LISP. For instance, the resolution mechanisms in HIP and LISP are two-level systems. Both HIP nodes and LISP nodes start a session by a DNS lookup. Then in the HIP case, the node performs a base exchange with its CH via its RVS. The RVS in this case provides the second level of the mapping since it provides the IP address of the CH. In the LISP case, the ITR contacts the corresponding resolver server to get the RLOC of the CH. We can say that the resolver plays the role of an RVS in a HIP terminology. These resolution procedures are repeated each time the MH starts a new session with a CH.

In the ILNP case, the resolution is only one-level. The ILNP node queries the DNS and directly gets the CH's identifiers and locators. It is why the cost of establishing an ILNP session is lower.

Thus, we can conclude that the CEC does not depend on the type of the used split approach. Host-based approaches and network-based approaches may have similar performances if they use the same number of resolution levels.

Now let us investigate the impact of CNs on DPC. We present the variation of this parameter as illustrated in Figure 3.6. As N_{CH} is increasing, the DPC is dramatically increasing for the three Identifier/Locator split protocols. However, host-based approaches, i.e. HIP and ILNP outperform clearly the

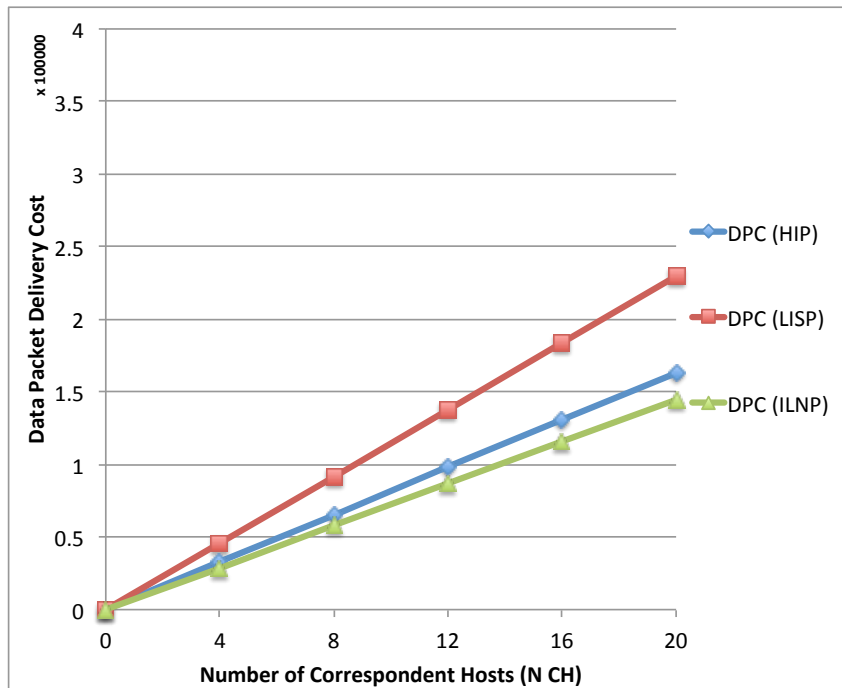


Figure 3.6: Impact of N_{CH} on Data Packet Processing Cost

network-based approach, i.e. LISP. This is because in a host-based approach, the data packets flow directly between the two communicating hosts. They do not undergo additional operations on the path which is the case of LISP data packets for instance. In fact, each packet sent by a LISP-MH is encapsulated when it arrives at the ITR. This operation makes the processing cost heavier in the routers' levels and increases the transmission cost as the size of data packets is increased due to the encapsulation.

We can conclude that host-based approaches have the advantage of providing lower packets transmission costs comparing to network-based approaches.

3.7.2 Impact of Network Scale

In this section, we investigate the impact of the network scale on CEC and DPC. For that, we set the N_{CH} value to 4 and we vary the network scale value from 1/30 to 1. As we presented above, δ corresponds to the ratio between distance MH,CH and MH,DNS. It does not affect the distance between MH,RVS and ITR,resolver and MH, resolver. Thus, the biggest δ is the biggest distance MH,CH is. Figure 3.7 investigates the variation of DPC. An interesting observation is that δ does not influence both ILNP and LISP. It can be explained by the fact that in both ILNP-based networks and LISP-based networks, MHs and their CHs are not involved in the control plane. Only data packets flow between the nodes.

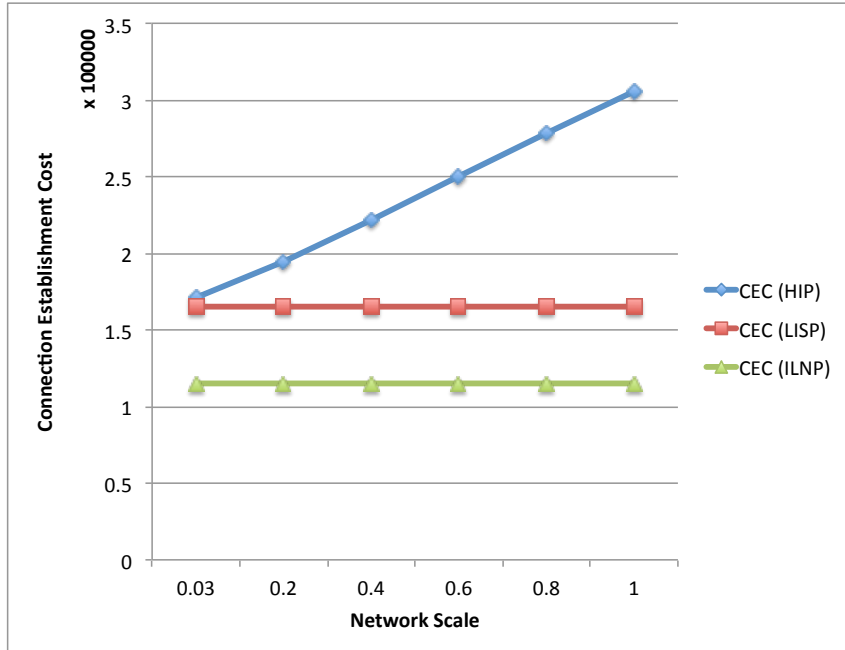


Figure 3.7: Impact of Network Scale on Connection Establishment Cost

The situation is different in HIP. The initiator and the responder perform the base exchange protocol before they start the data session. That is why, increasing the distance between HIP nodes obviously increases the connection establishment cost.

In Figure 3.8, we investigate the impact of δ on DPC. We observe that host-based approaches outperform LISP. In addition, the performance gap is small between HIP and ILNP. This latter is due to the difference between the

size of HIP data packets and the size of ILNP data packets. As presented in Table 3.2, the difference is about bytes.

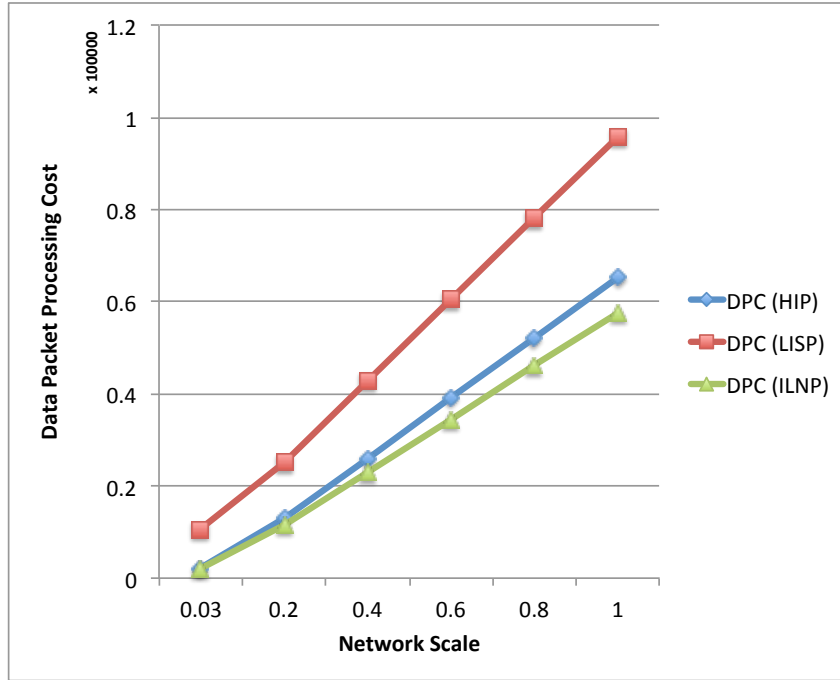


Figure 3.8: Impact of network scale on Connection Establishment Cost

LISP performance in this analysis is dramatically influenced due to the size of LISP data packets. Having encapsulated data packets and long routing paths between MHs and CHs increases the DPC.

3.7.3 Impact of Velocity

Handling high mobility requirements in future networks is a key performance metric of future naming architectures. That is why we investigate here the behavior of the three protocols depending on the nodes' velocity. We vary v from 1m/s to 20m/s. Figure depicts the results of this analysis. LISP largely outperforms ILNP and HIP. In LISP-MN, the MH acts as an ITR. Upon a mobility scenario, it updates its resolver server. However, in host-based approaches, the mobility signaling is higher. In ILNP case for instance, the MH updates its records within the DNS and informs its CHs with its new location. HIP has the worst performance in this analysis. In fact, when an MH undergoes a mobility scenario, it first update its CHs. The update

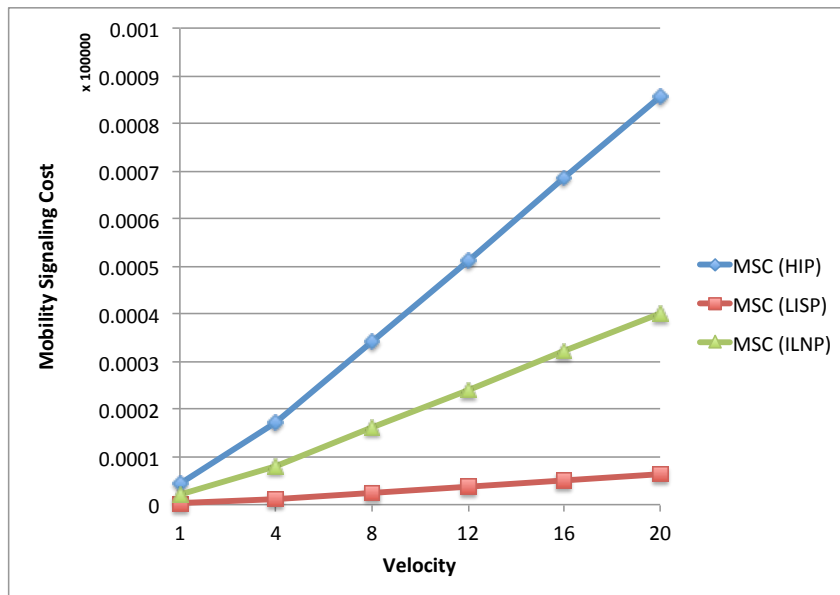


Figure 3.9: Impact of velocity on Mobility Signaling Cost

mechanism in HIP is based on the exchange of three cryptographic messages as HIP provides mechanisms against IP address spoofing. The MH performs a similar update mechanism with its RVS. We can say there is a tradeoff between high level of security and performances.

3.7.4 Impact of Cell's Radius

Figure 3.10 shows the variation of MSC against the cell's radius. Here, we vary L from 600m to 3600m. In the three cases, as we increase the cell's radius, the probability of handover decreases and thus, MSC decreases too.

We obtain almost the same performance results as in the previous section.

3.8 Chapter Conclusion

In this chapter, the Identifier/Locator split proposals presented in Chapter 2 including HIP, LISP and ILNP have been analyzed and compared in terms of connection establishment cost, data packet delivery cost and mobility signaling cost. From the conducted analysis results, the followings are confirmed : The increasing number of CHs decreases dramatically the performances of both host-based and network-based approaches in terms of connection establishment

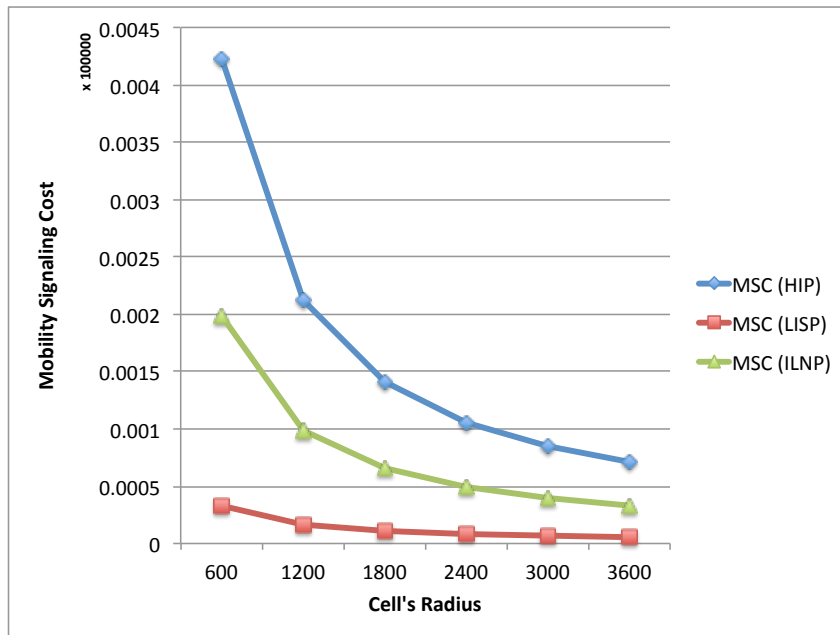


Figure 3.10: Impact of Cell radius on Mobility Signaling Cost

costs and packets delivery costs. There is a tradeoff between the security level and the performances. HIP is a very secure protocol but it presents high costs.

There is an interesting conclusion to be shown from these analyses. In all the cases, the number of hosts in the network is key performance parameter. Adding a new node in the network implies additional costs on different metrics, including the mapping updates, the registration process and the mobility signaling. It is because of the host-centric character of all the approaches presented above. One may ask about the performances of such host-centric approaches in future networks where users are multi-homed, very mobile and multi-deviced.

In Chapter 4, we present the requirements of future networks from a user-level perspective. We present common usage scenarios in the future, such as user multi-homing and user mobility. Based on the analysis results obtained in this chapter, we show how host-centric naming approaches have shortages regarding additional user-level requirements.

Chapter 4

Towards User-level Naming Architectures

4.1 Introduction

Internet has evolved from a network that connects end hosts to exchange information to a network that connects users with different profiles and preferences. Today using Internet, users need to join other users to communicate or to share a service independently from their locations and the devices they are using. It is also becoming increasingly popular that one user has access to a multitude of terminals with different service offering capabilities. For instance, Alice may prefer to use her laptop in the office, 3G tablet when she is outside and in-car telephone when driving.

Reachability will be one of the most desired features. A typical scenario is that Alice can contact Bob whenever and simply by using Bob name independently of which device is used in the communication. Moreover, users may want to switch their ongoing sessions from their smartphones to their IP TV for example. More precisely, the most desired features in the future can be summarized in the following points.

- The future Internet will be a network that mainly **interconnects users instead of hosts**. Special attention should be paid to user-to-user networks and **device-independent communications**.
- **Multi-device support for users** will be an important characteristic and a desired feature of the future communications.

The current Internet architecture lacks of such support. Because naming is the basis of any networking design, we believe that in order to provide support for such desired features we should start by rethinking the naming part of the architecture.

In Chapter 2 we have presented a sample of Identifier/Locator split solutions. As we have explained before, this concept presents a step toward evolving the naming architecture of the Internet. However, all the proposed schemes have a host-centric approach. Actually, they are good candidates to solve network-layer problems but, their performances in a user-centric network need further study.

In this chapter, we study the naming problem from a different perspective. We provide new naming requirements from a user-level perspective. We show that from this perspective, users and services should be considered as main and independent networking entities. As a consequence, they should be identified independently from hosts. We also analyze the shortcomings of Identifier/locator separation architectures to provide a complete solution to the naming problem.

This chapter is organized in three main parts. In the first section we enumerate new user-oriented emerging use cases and we express them in terms of user-level naming requirements. The second section presents the shortcomings of host-centric Id/Loc solutions in supporting these requirements. The third section presents a sample of recent naming proposals that have considered users and services identification.

4.2 New Use Cases and User-level Requirements

4.2.1 The user as Endpoint of Communications

Data transmission in today's Internet is based on addresses or devices. Historically, Internet was built on a host-centric design in which it was believed that the main goal of networking is to interconnect hosts. In such architectures, the host is the central component and is the final endpoint in communications. Because of this host-centric character, users, services and data are not considered as independent components. They are almost all the time tightly coupled with hosts. For example, if a user wants to download an MP3 file, the network

resolves this request into the location of the server where this file is hosted. However, it is clear that users want only to get the MP3 file regardless of its location in the network.

Another relevant example is user-to-user communications. Actually, with more and more users who access the Internet through all kinds of mobile and fixed devices, current communication mode is becoming somewhat an obstacle to the information sharing between users. To contact one person, we need to maintain the relationships between the person and a large number of ways to reach him/her. From the user's point of view, what they really care about are the other users, not the devices or addresses they reside in.

To summarize, the identification of users and their services must be a central point in a future architecture. Thus if we translate the use cases described above in terms of naming and name bindings, we get the following requirement.

Req_1: Users and services should be identified independently of the hosts they are using or they are hosted in.

4.2.2 User Multi-homing

Initially in the traditional communication model, it is recognized that a single user is connected to its operator/Internet Service provider (ISP) network via one device though one access technology.

Nowadays, every user typically owns several devices like handsets, smart phones, laptops, PCs, etc, each of them equipped with different connectivity technologies such as 2G, 3G, LTE, WIFI, Bluetooth, etc. As an indicative guide, by 2020 more than five billion consumers worldwide will be connected to the Internet and cloud via 20 billion wired and wireless devices [Anab]. It means that for the future Internet, real-world user multi-device scenarios will be largely widespread. As devices are expected to converge in their functionalities and capabilities, a single user will then be presented with a vast array of communication options and alternatives. Reachability will be at the center, which intuitively means that a given user should be served regardless of access networks and owned devices.

From an architectural view, there is an urgent need to integrate these new facts in the naming systems. Thus, we provide the second requirement.

Req_2: User multi-homing among different devices should be supported

by naming architectures.

4.2.3 Handover between Devices/ User-level Mobility

Nowadays it is becoming more and more common that a user wishes to switch his/her ongoing session from one device to another. Home networks are typical examples of this use case. When arriving home, users prefer to use their WIFI devices instead of 3G devices to get a better QoE and QoS.

Figure 4.1 depicts a handover scenario between two devices belonging to the same user A.

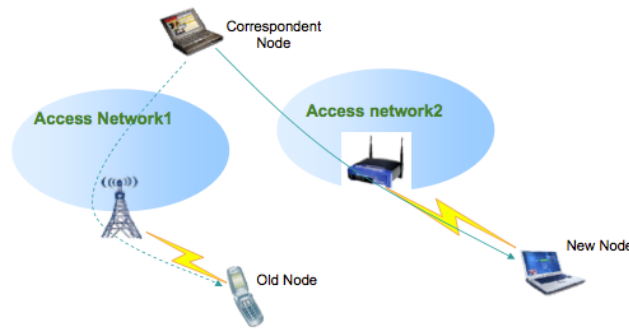


Figure 4.1: User Session Handover between two devices

User A starts a communication with a device. During the communication, the user may want to switch to another device to get a better QoE for example. The communication/the service in use should be able to handover between networks or from one device to another. It is a challenging point to keep the application layer of the correspondent host agnostic about this handover.

Req_3: Handover between devices is agnostic to applications of the correspondent node

4.2.4 Selection of a Proper Device / a Proper Network

As we explained above, users likely have multiple devices with different capabilities and properties. These different capabilities meet different requirements depending on the situation and the context. Figure 4.2 describes a user-oriented communication scenario. Alice wants to share a video with Bob

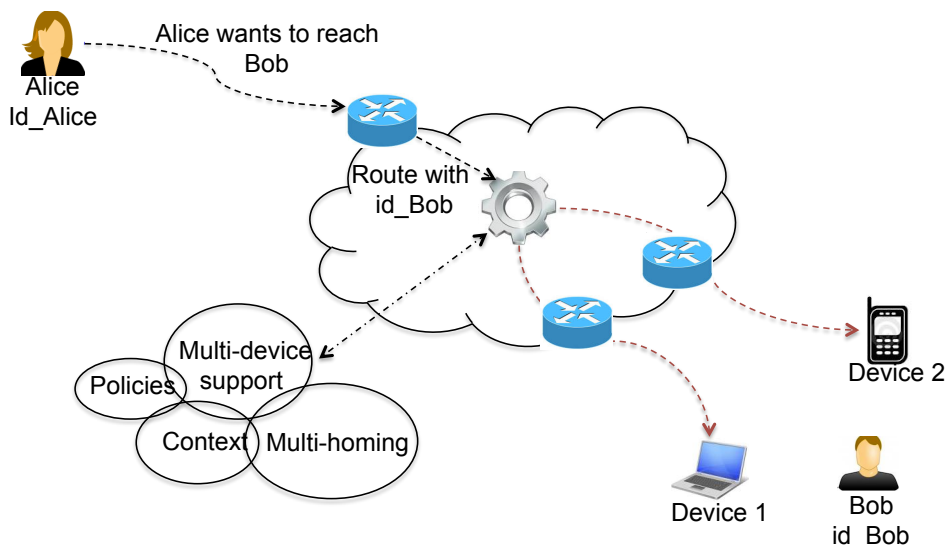


Figure 4.2: Selection of a Proper Device in User Multi-homing Case

who is connected to the network via two devices with different capabilities. The network routes the request using Bob’s identifier. In order to choose the best device to select for this communication, several parameters are taken into consideration. Among them, there are Bob’s context, Bob’s preferences, network policies, pricing, etc.

Req-4: Giving the network the ability to select a proper device for each given communication context

In the next section, we analyze the adequacy between the above-stated requirements and the previously presented Identifier/Locator split approaches.

4.3 Do Host-based and Network-based Id/Loc Split Solutions meet User-level Requirements?

In Section 2.7 we have summarized the different answers provided by three representative host-based and network-based Id/Loc split solutions, i.e. HIP, ILNP and LISP, to the host-level requirements expressed by the RRG. In this section, we investigate the behavior of these approaches with respect to the

four user-level requirements that we have enumerated above.

- **Req_1: Identification of users and services**

Solutions like HIP, ILNP and LISP implement intrinsically Identifier/Locator split. They are mainly built in the light of end-host problems. Their basic design focuses on providing efficient support for network-layer problem, namely achieving end-host mobility and multi-homing. These approaches can be criticized for being host centric which obviously excludes any interest on users or services. In fact, despite the technical differences between host-based and network-based approaches, all of them introduce an additional level of identification for hosts only. There is no consideration to users nor services.

- **Req_2: User Multi-homing**

This use case results in a set of different and independent terminals' identifiers although they belong to the same user. In this case, the network does not have any knowledge that these identifiers are just different ways to reach the same user. Figure 4.3 depicts a user multi-homing scenario in a HIP network. Bob maintains two devices with two different HITs, i.e. HIT_device1 and HIT_device2. Alice wants to contact Bob. As Bob does not have a separate identifier, the request of Alice to the DNS should contain the name of one of Bob's devices. It means that the network does not recognize HIT_device1 and HIT_device2 as being representative of the same user identity. As a consequence, these approaches lack an integrated user identity in the network.

- **Req_3: Handover between Devices is Agnostic to Applications**

The user session transfer between different terminals is not natively supported since communications in Identifier/Locator split relates to the identity of the terminal and not to the user. In HIP for example, sessions are identified using HITs. If we move a session from one terminal to another, it means we change HITs and thus, we break the session.

- **Req_4: Selection of a Proper Device for each communication**

In all the cases, the resolution from a name to its identifier is done in an early step of the communication. That is, if there are many identifiers corresponding to the same user, there is not any way to choose the most

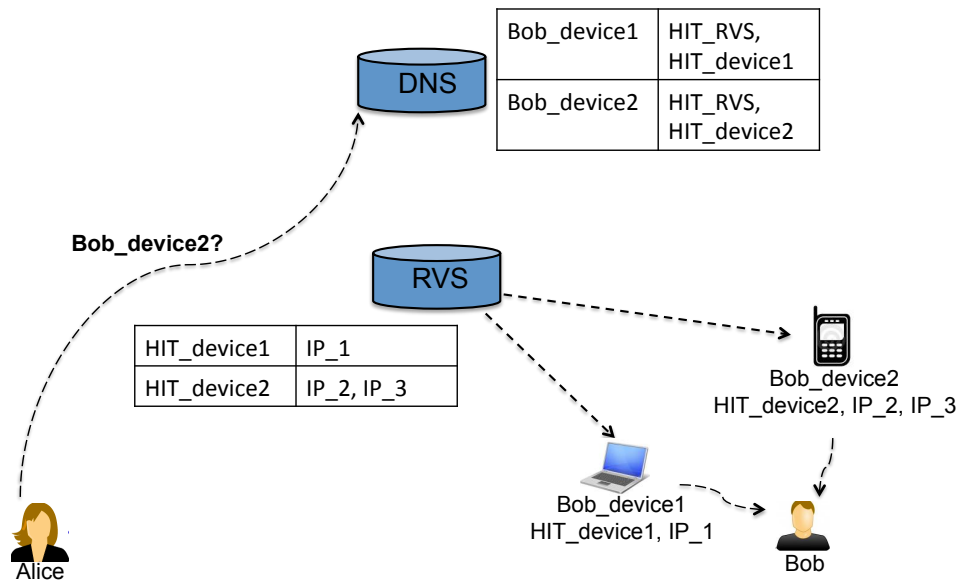


Figure 4.3: User Multi-homing Case in a HIP Environment

suitable host for this type of communications. As illustrated in Figure 4.3, the choice of which device to use is determined since the first request in the communication establishment.

4.4 Evolution of Naming Models

The internet naming model is based on a two-level mapping scheme as depicted in Figure 4.4a. Domain names are resolved into IP addresses. The Id/Loc split adds an additional indirection level to the basic naming model of Internet. It results into a three-level mapping naming model as shown also in Figure 4.4b. Recently and in order to bring answers to new requirements related to users and data identification, some proposals add a second indirection level above the Id/Loc split model. It results in a fourth-level naming model presented in Figure 4.4c. These category of solutions move a step toward user and data identification and enlarge the scope of Identity/Location split solutions. They introduce additional namespace (s) for users and/or services. In Section 4.5 we present three examples of this category namely the Layered Naming Architecture (LNA) [BLR⁺04a], the User Identity Routing Architecture [LPL⁺10] and the Policy oriented Naming Architecture (PONA) [PJPB08b]. In the existing architecture, services are tied to hosts. Moreover, services and data in current

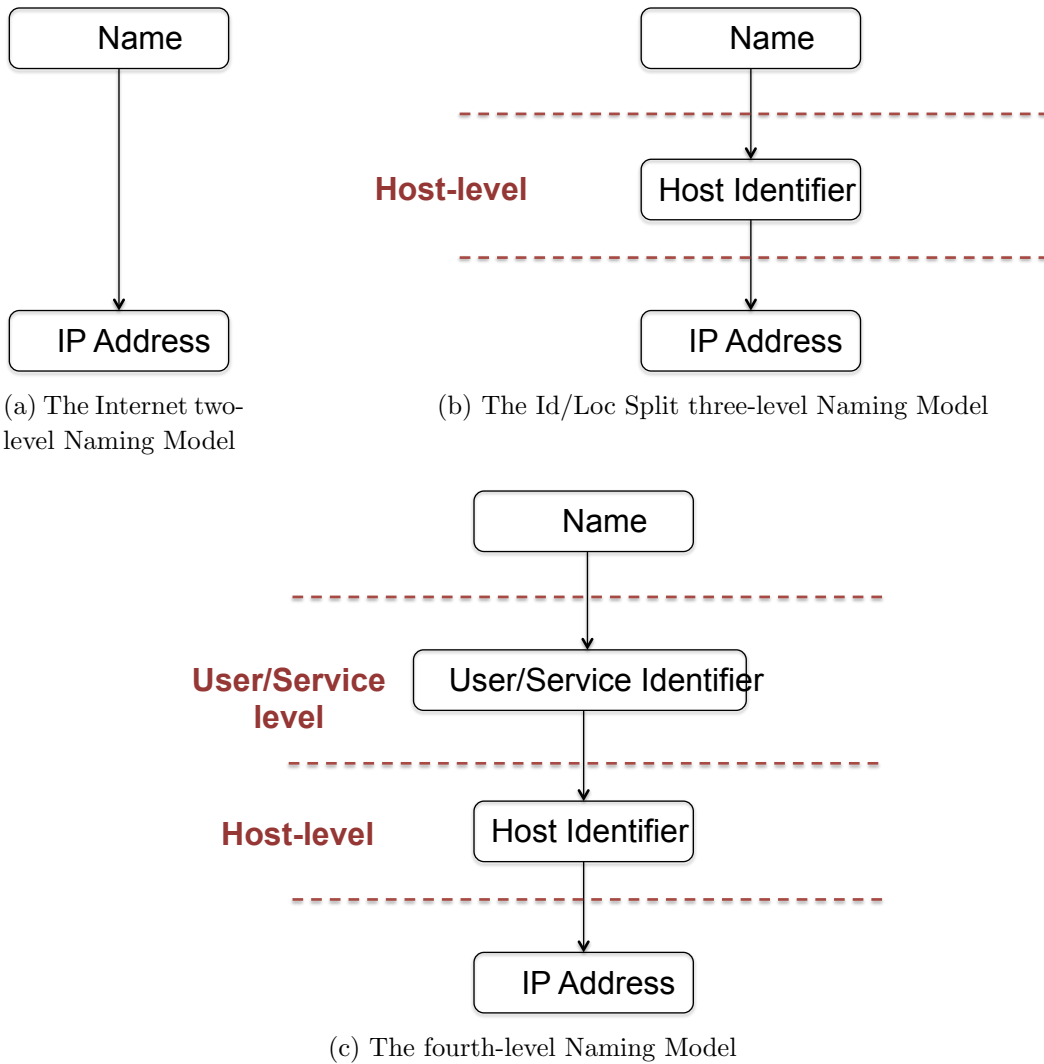


Figure 4.4: The Different Naming Models

4.5 Users and Services identification in Recent Naming Proposals69

Internet are named relatively to the hosts they are running on. This makes services totally tied to endpoints and therefore issues like services migration and composition become hard to achieve. LNA solution reviews the Internet naming issues as an attempt to remedy the Internet ills.

4.5 Users and Services identification in Recent Naming Proposals

4.5.1 Layered Naming Architecture (LNA)

LNA design is mainly inspired from the following three architectures: HIP, i3 and Semantic Free Referencing (SFR) [WBS04]. The novelty of LNA as a naming architecture is that it is one of the first architectures that apply Saltzer's ideas [Sal78]. In 1982, Saltzer published an interesting paper about naming and addressing principles. It is indicated in this paper that the following bindings should exist in a naming architecture:

- The binding of a service to a node
- The binding of a node to a network attachment
- The binding of a (routing) path between two network attachments

LNA inherits these ideas and hence, identifies services independently from hosts they are running on.

4.5.1.1 Namespaces

The first principle of LNA as described in [BLR⁺04a] stands for considering services as independent network objects. LNA requires that services are named independently from hosts they are running on. For this purpose LNA proposes the introduction of Service Identifiers (SIDs) namespace to name services. SIDs are host-independent data names that remain persistent even when the designated service migrates from one host to another. SIDs give an application the possibility to refer to a service that is not tied to a specific server.

LNA also uses Endpoints Identifiers (EIDs) namespace in the line of other Identifier/Locator separation solutions. EIDs are location-independent host names.

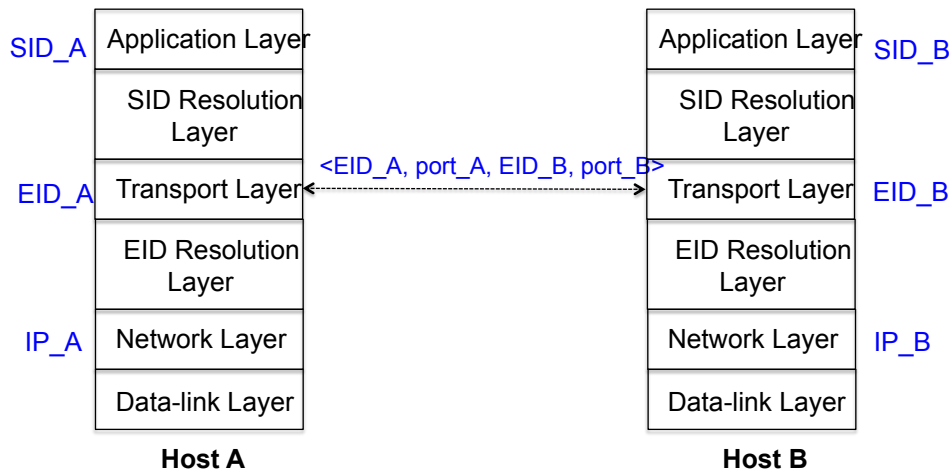


Figure 4.5: LNA Namespaces

The two namespaces are global and flat. The protocol stack of an LNA-based host is shown in Figure 4.5. In an LNA-based network, applications use SIDs as data handles and transport connections are bound to EIDs.

4.5.1.2 Resolution Mechanisms

As we explained in Section 4.4, the resolution mechanism of LNA follows four levels. Moreover in order to resolve SIDs and EIDs, LNA advocates the use of a Distributed Hash Table (DHT) [X1111].

Let us assume that host A wants to use the service identified as `SID_s` and hosted in host B. Figure 4.6 depicts the flow messages required for a communication establishment. LNA assumes the existence of a User Level Descriptor (ULD) that resolves a given name of a service to the corresponding SID. ULDs are for example, e-mail addresses, search strings, etc. Host A gets `SID_s` via the ULD. Then, host A contacts the DHT infrastructure to map `SID_s` into an EID. As a result, the DHT returns one or more EIDs on which an instance of `SID_s` is running. The EID resolution layer chooses one among the provided EIDs and sends a second mapping request to the DHT to get the IP address (es) of the destination host.

4.5.1.3 Answers to User-level requirements

The whole spirit of LNA is to support mobility of data and services. Whenever a host is mobile, it may just change the EID IP mapping in the EID mapping

4.5 Users and Services identification in Recent Naming Proposals⁷¹

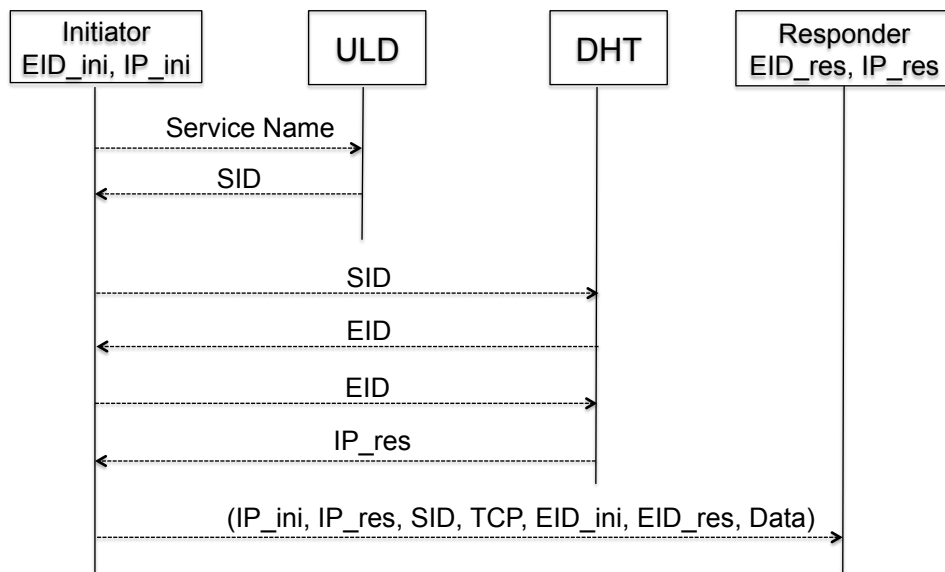


Figure 4.6: LNA Connection Establishment Flow

infrastructure. Also, during communication, If the IP of a host changes then the transport layer of the peer layer can re-initiate a lookup and rebind.

- **Req_1: Identification of users and services**

LNA provides identifiers for services but does not solve the identification problem of users.

- **Req_2: User Multi-homing**

LNA does not enable user multi-homing feature as it identifies all the hosts of the same user separately using difference EIDs.

- **Req_3: Handover between Devices is Agnostic to Applications**

Transport layer sessions are tied to EIDs. It means that changing the device impacts sessions' continuity.

- **Req_4: Selection of a Proper Device for each communication**

The dynamic binding between SIDs and EIDs can fulfill this feature in LNA.

Let us give the following example as shown in Figure 4.7. Alice wants to send an email to Bob who works in a company called Y. The name of the organization has changed to Z but Alice does not know about it.

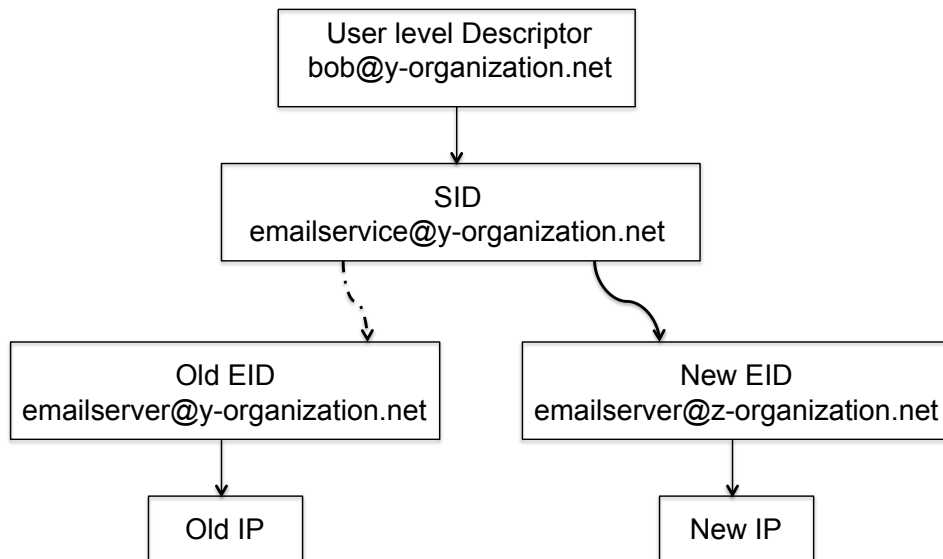


Figure 4.7: Email Example in an LNA-based Network

This affects the email domain name of Bob. The old email server has been mirrored. When Alice sends the email to her friend, her email application looks up the ULD to find the corresponding SID. After this, the obtained SID is used to lookup the EID which will point to the new domain name. The service layer in this example ensured to find a working EID so that the user will not be aware of the new circumstances.

4.5.2 User Id Routing Architecture (UIR)

The User Id Routing Architecture is a domain-based network architecture. It is based on a routing architecture that uses users' identifiers. In the following, we present in more details the namespaces and the resolution mechanism of this architecture.

4.5.2.1 Namespaces

UIR introduces two new namespaces. In the line of other Id/Loc split architectures, hosts in UIR are identified using a new host-based namespace. A second new namespace is used to identify users. The architecture specifies two types of locators : local and global. Local locators are relative to a domain and have meaning only within this domain while global ones have global scope

4.5 Users and Services identification in Recent Naming Proposals⁷³

and are routable.

4.5.2.2 Resolution Mechanisms

UIR maintains the mappings between the user identifier and its terminal's locators thanks to the Domain Router (DR) [6] and the Subscriber Location Server (SLS), which are two new introduced resolution entities.

Figure 4.8 shows the UIR network architecture.

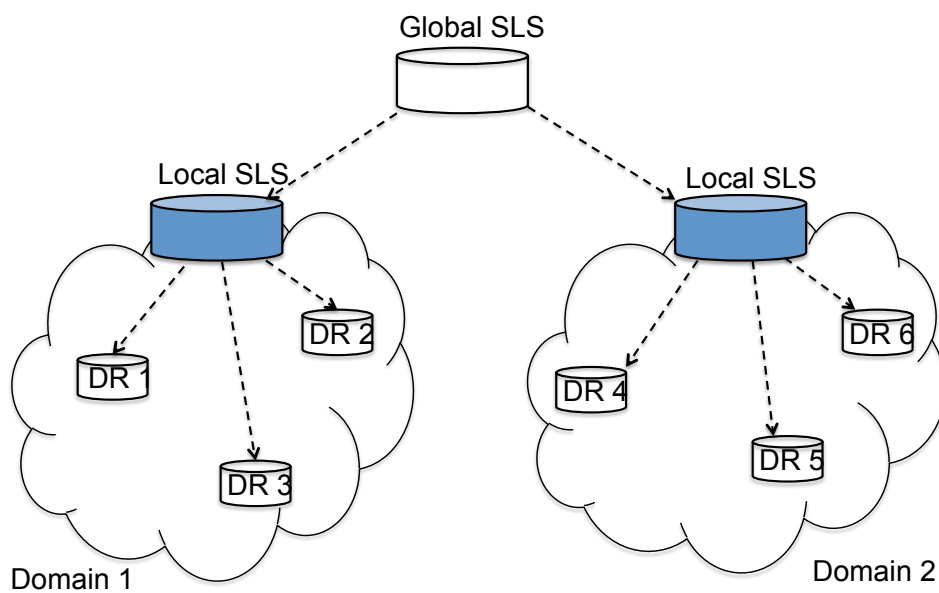


Figure 4.8: UIR Architecture

The design model is built around domains where there should be at least one DR and one SLS per domain. Each global SLS stores a mapping table of User IDs and their corresponding home SLSs as every user ID relates to one home SLS. Home SLSs however maintain mapping tables of their subscribed User IDs and their corresponding resident DRs. DRs have mapping tables of their resident User IDs and their corresponding locations within this DR domain. The architecture specifies two types of locators : local and global. Local locators are relative to a domain and have meaning only within this domain while global ones have global scope and are routable. The architecture also describes mechanisms for user mobility and user session transfer between different terminals. The connection establishment call flow between two UIR-based hosts is described as follows.

The initiator sends a first data packet to its DR. This packet contains the locator of the initiator, the locator of the responder and the identifier of the user who maintains the initiator host. In order to get the global locator of the DR to which the responder is connected, the initiator's DR first queries the local SLS. If the mapping information is not present locally, the request is forwarded to the global SLS. Once the DR global locator is obtained, the initiator's DR substitutes the initiator's locator with its global locator and sets the destination locator to the retrieved locator and forwards the packet.

4.5.2.3 Answers to User-level requirements

- **Req_1: Identification of users and services**

UIR provides identifiers for users but does not solve the identification problem of services.

- **Req_2: User Multi-homing**

UIR enables user multi-homing feature as it identifies all the hosts of the user with the same user identifier.

- **Req_3: Handover between Devices is Agnostic to Applications**

As sessions are tied to EIDs, handover between devices is possible with UIR but it is not transparent to applications.

- **Req_4: Selection of a Proper Device for each communication**

Either the local SLS or the global SLS can decide which device to select. In fact, SLS can collect information like attributes, context and policy of various destination devices. It then can choose the proper device to use for each type of communications.

4.5.3 Policy Oriented Naming Architecture (PONA)

PONA extends MILSA architecture's ideas [PJPSI10] [PPJB08] to bring together the user-centric, the data-centric and the host-centric communication models in one naming architecture. As shown in the figure, PONA proposes a layered naming design based on realms of users, data and hosts and where users and data realms are at a higher layer than hosts' realms. The architecture is built around the following basic principles. First, PONA enlarges the definition of communication entities from hosts only to encompassing other

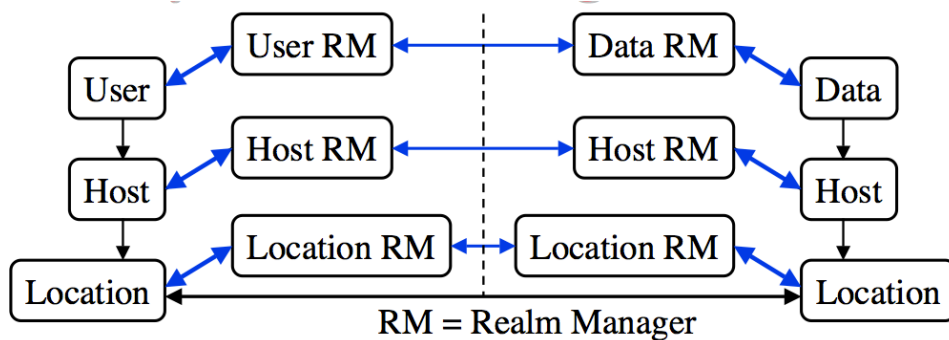


Figure 4.9: PONA Architecture

nonelectronic objects like users, data and services. This assumption joins the ideas of LNA and User ID Routing Architecture in that users and data have separate identifiers independent from the hosts they are using or running on. As in MILSA, PONA uses the concepts of realms and zones and extends their scope to users, data and hosts. Thus it helps the support for policy enforcement where each realm can be assigned a different policy and it is the role of realms managers to negotiate and store the policy rules. In addition, PONA realizes many levels of policy enforcements, such as user-to-data, host-to-host and user-to-host, etc. PONA stands also for using directives rather than addresses in resolution. Contrarily to the current existing resolution mechanisms where almost the time we have a resolution from a name or an identifier to a single address, resolutions in PONA may result in sets of bindings of the desired object to a host address or identifier, a service ID or data ID, etc. These bindings are refined by the architecture till the target location is found. PONA envisions also a new protocol stack as shown in Figure 4.9.

4.6 Discussions

In Table 4.1, we summarize the different results of our analysis.

In the above sections, we have presented a survey of the evolution of naming resolution models and we compared them against host-level and user-level ideas. In the two-level naming model of Internet, DNS names and IP addresses are used both to name hosts. In Chapter 2, we have presented the problems faced by this design to support host-level networking problems like host mobility and host multi-homing. Moreover, we can add other shortcomings to

	LNA	UIR	PONA
Req.1	only services	only users	Yes
Req.2	No	Yes	Yes
Req.3	No	No	No
Req.4	Yes	Yes	Yes

Table 4.1: Answers to User-level Requirements

the existing architecture, which are related to data and users identification. Actually, there is no common way to name data from transport or network layers. Almost the present solutions are application layer solutions. Today, Data in Internet is bound to protocols. URLs schema for instance contain user information, user password and host name. URLs are almost tied to http protocol and to the web server that is hosting the data. If directory structure is modified, URLs become unusable and the user has to find an alternative way to find the required information.

As a consequence, we can confirm that a two-layer resolution model is unsuitable for both network-level problems and user-level problems.

Solutions that implement intrinsically identifier/Locator split are based on an additional level of indirection. Although different implementation approaches have been proposed in the literature, they are all based on a three-level resolution model. Application names are resolved to host identifiers, and then host identifiers are resolved to locations. These approaches can be criticized for being host centric. Let us for instance consider the scenario of user multihoming. This type of approaches results in a set of different and independent terminals' identifiers presenting the same user. In this case, the network does not have any knowledge that these identifiers are just different ways to reach the same user. As a consequence, this aspect results in the absence of an integrated user identity in the network.

Moreover, in almost all cases, different devices used by the same user can have similar functionalities. Identifying terminals separately in this case breaks any possible logical link between services and functionalities run by the same person. Besides, user session-transfer between different terminals is not natively supported since communications in Identifier/Locator split relates to the identity of the terminal and not to the user. In HIP for example, sessions are identified using HITs. If we move a session from one terminal to the other, it means we change the host identifier and thus, we break the session.

Another disadvantage of this approach is its scalability. Actually, if we apply such approaches intuitively to the future Internet, it results in an increase in the number of terminals' identifiers that must be managed by the resolution infrastructure and severely stressing the scaling properties of these schemes. Upon each arrival of a new terminal in the network, an update of the mappings in the resolution system is necessary. This is a heavy operation to do especially in highly dynamic networks.

To solve some of these problems, solutions like LNA, UIR and PONA have been proposed. They advocate a new four-level naming model. LNA for instance provides benefits regarding service mobility, they still have shortcomings in supporting user multi-device scenario. They already do not consider identifiers for users, which again leads to independence between services own by the same user. Moreover, a service migration in LNA requires the solicitation of a global resolution system, i.e. DHT to maintain the mappings between services and terminals update. UIR assigns a separate namespace for users, but it still inherits the drawbacks of Identifier/Locator solutions since it still considers identifiers for terminals. PONA can be criticized for being just a high-level concept. The authors do not provide enough details on how their solution can be implemented. It considers identifiers for both users and services, but it does not specify how it can manage the relations between users and their services.

We argue that a naming scheme should present a single coherent and integrated view of the user and that all of a user's devices should be presented relatively to the identity of the user and the types of services they can offer. The three studied resolution models bring solutions to the naming problem from different angles, but none of them presents a complete solution.

The challenge we are proposing to solve in this thesis is the following:

Can we propose a new naming solution that 1) complements the above related work? 2) presents an integrated vision of users and their services? 3) brings optimizations in the resolution mechanisms?

4.7 Conclusion

In this chapter, we have highlighted the importance of evolving the naming schemes to meet the different new requirements of user-level communications. It is clear that the first ideas of splitting host identifiers and locators, although useful to solve the traditional problems of mobility, multi-homing and routing,

are not sufficient to cover additional aspects of the naming problem, mainly like users and data identification. We tried to present the most interesting solutions proposed in the literature.

To complement the previous research work, we present in Chapter 4 our main contribution. It is a new naming architecture, called Service Aware Naming Architecture (SANA).

Chapter 5

SANA: A Service-Aware Naming Architecture for Future Internet

5.1 Introduction

Chapter 4 has emphasized the host-centric character of Id/Loc split solutions and their shortcomings in supporting user requirements. Two of the most important future requirements are the increasingly diverse and dynamic environment expected for users and the enormous proliferation of mobile terminals. Consequently, as we have shown in previous chapters, special attention should be paid to person-to-person communications and multi-device support in future naming schemes' design. Therefore, we propose a new naming solution that takes into account user-level requirements. In this naming solution, we believe that it is mandatory that an independent namespace for users shall be used.

SANA (Service-Aware Naming Architecture) [ABB11] is a novel naming proposal for next generation Internet which embraces direct naming of users for clean separation of user's identity and their terminals locations. SANA provides a uniform identification for users and an integrated service model.

In this chapter, we present the main components of SANA. Our solution is built around the following three key points.

- We challenge the traditional Identifier/Locator split paradigm by **get-**

ting rid of terminals identifiers and promoting users and services identification.

- We provide a **transparent multi-device support** to the network.
- We make **users sessions switching between different terminals agnostic to applications and networks**.

By covering these aspects intrinsically, our solution can be considered a significant candidate for future naming systems with respect to user-level requirements.

The remainder of this chapter is organized as follows. Section 5.2 provides the design principles that motivates our architecture. In Section 5.3 we present a general description of the proposed architecture including the namespaces and the resolution system. Section 5.4 presents a detailed description of data plane and control plane in SANA. We provide as well a detailed description of the protocols associated with SANA. In Section 5.5 we present a detailed description of the communication scenarios in SANA. Finally Section 5.6 concludes the chapter.

5.2 Design Principles Behind SANA

The design principles of SANA summarize the essence of our understanding of the naming problem. In addition to the network-level requirements and the user-level requirements presented in the previous chapters, we add further design points. We believe that these points have relevant impacts on the overall performance of SANA.

- **Emergence of Person-to-person communication:** The main objective of future networks is to interconnect users by the means of various equipments connected to heterogeneous access technologies (WLAN, 2G/3G, etc). The only requirement to start a communication is to know the identifier of the corresponding user. This feature facilitates an easy access to the network.

Moreover, the network should have the ability to select the appropriate equipment on which a user can be joined taking into account the equipment's hardware characteristics and the variable network environment's indicators. This refers to the capacity of performing efficient resolutions in order to deliver the best quality of service.

- **Network Awareness of what types of traffic** are flowing across the data delivery infrastructure: One major concern of operators today is to be able to efficiently manage and control their networks. Understanding networks traffic help operators fulfilling this purpose. Naming systems should play an important role to this respect.
- **Scalability of resolution systems:** The resolution infrastructure is one of the core ingredients of a naming architecture. Maintaining scalable resolution systems requires fast mappings. At present, main research in this field consider DHT-based solutions. They have good scalability but they suffer from high resolution latency. In this thesis, we take a different approach to meet the demand of scalability. The question that we try to answer is the following. What types of identifiers should be stored in resolution systems? Can a service-based approach brings possible optimizations comparing to host-based approaches?
- **Late bindings between identifiers and locators:** Almost the previous work focus on how to resolve a given identifier to its corresponding locator. However, we think that deciding when the resolution is done in the connection establishment process is also an important feature to consider. Allowing a late binding between an identifier and its locators enables the resolution system to return the most adequate locator especially in the multi-homing case.

A possible application of this feature can be pushing the choice of the locator at the access network level.

- **Redundancy of available services on different devices of the same user:** What if we identify the available types of communications independently of the hosts serving it ? The user can be presented with his/her service offering capabilities rather than with the devices he/she is using. It means that we make abstraction of hosts.
- **Make the relation between the identifiers of the same user explicit in the naming system**
- **Manage user multi-homing operations locally:** The main idea is to reduce the signaling cost due to multi-homing and to make multi-homing as transparent as possible to correspondent hosts.

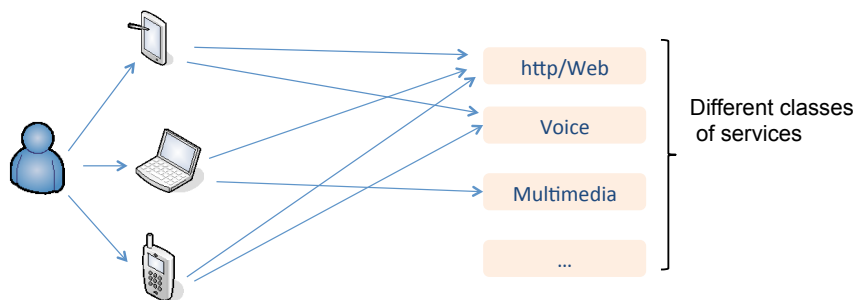


Figure 5.1: Services among the devices

5.3 General Design of SANA (Service-Aware Naming Architecture)

In this section we present a general description of the proposed architecture. We firstly introduce in Section 5.3.1 the terminology used in our architecture. Then in Section 5.3.2 we emphasize the difference between a host-centric naming model and a user-centric naming model. Finally, we introduce the general architecture, the namespaces and the resolution system associated with SANA in Section 5.3.3, Section 5.3.4 and Section 5.3.5 respectively.

5.3.1 Terminology

- **Master Identifier (MId):** It is an identifier that uniquely identifies a user's subscription to an operator. That is, different subscriptions of the same user to the same or different operators result into different MIds. At the same time, different users connected using the same subscription maintain the same MId. An MId refers, for instance, to a home subscription shared by the members of the family. A possible format of this identifier is depicted in Figure 5.2. MIds are generated and maintained



Figure 5.2: A Possible Structure of an MId

by operators and are revoked when the corresponding subscription is canceled.

5.3 General Design of SANA (Service-Aware Naming Architecture) 83

- **Secondary Identifier (SId):** It is an identifier generated from an MId and is associated with a specific class of service. We define the structure of an SId as shown in Figure 5.3. Examples of classes of services include:

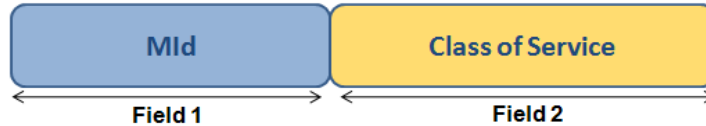


Figure 5.3: A Possible Structure of an SId

'conversational', 'streaming', etc.

- **Private identifier (PIId):** It is a special identifier that is used for secured communications. For compatibility reasons, we assume that MIds, SIds and PIDs are 128-bit length.
- **Master-to-Secondary Identifier Directory (MSID):** It is a dedicated database maintained by operators and storing the mappings between the MIds and their corresponding SIds.
- **Service-Specific Resolution System (SSRS):** It is a resolution structure in which mappings between SIds and access router (AR) locators are stored. A challenging property of an SSRS is its dynamicity since mappings have to be updated when hosts change their ARs. Each SSRS corresponds to a class of service, and thus stores SIds of the same type.

To clarify the relations between the different identifiers we have described above, we propose the following dependency diagram as depicted in Figure 5.4.

5.3.2 User-centric vs Host-centric Naming Architecture

Unlike most of the existing naming proposals which focus on hosts as network first-citizens, SANA focuses on a user perspective. In our proposal, the endpoints of communications are users themselves, instead of addresses or devices as it is the case in the existing Internet architecture. One user may have multiple devices and addresses, but the fact is hidden by the 'User Layer' and invisible to the applications above. Figure 5.5 and Figure 5.6 show the difference between our architecture and host-centric architectures.

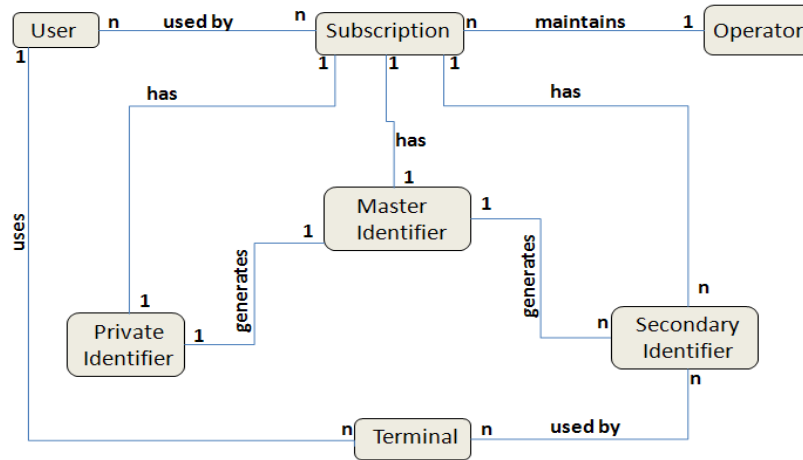


Figure 5.4: Dependency Diagram

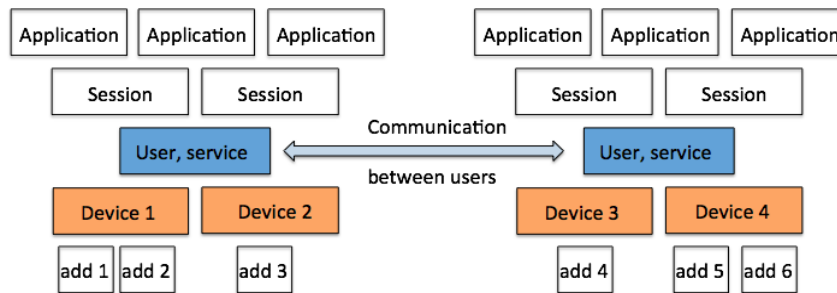


Figure 5.5: User-centric Network Architecture

SANA separates user identity from locations, thus it can not only solve network-level problems like traditional ID/Locator split methods, but also meet the user-level requirements such as multi-homing and mobility across devices. Also, the new namespace will facilitate applications because they do not have to maintain a large number of names and addresses anymore, but use names of the user directly to identify the correspondent.

Further on, the user-centric architecture provides the basis of users' ubiquitous access and information sharing in the near future.

5.3.3 General Architecture of SANA

In this section, we describe the architecture of SANA based on the design considerations discussed in Section 5.2.

SANA architecture is illustrated in Figure 5.7. The architecture is built

5.3 General Design of SANA (Service-Aware Naming Architecture)

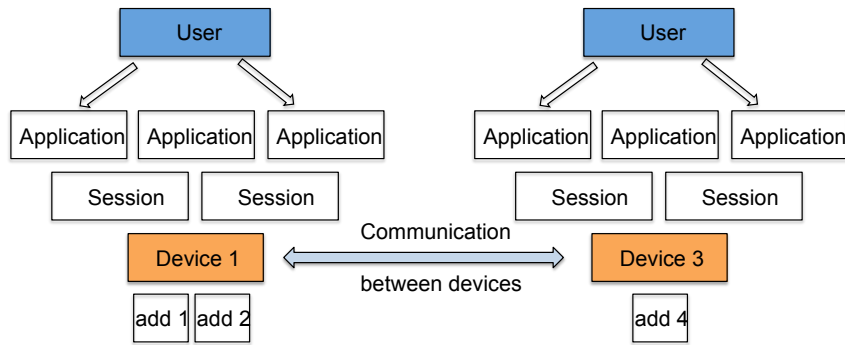


Figure 5.6: Host-centric Network Architecture

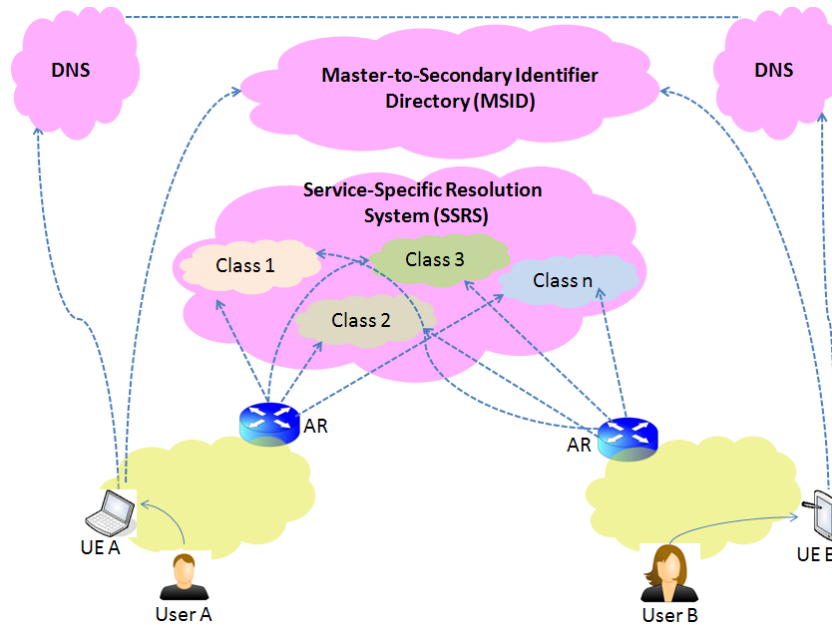


Figure 5.7: SANA General Architecture

around a core-edge separation design. We consider an overall network model which consists of an IP-based backbone network and a wide variety of wireless access networks. ARs are the first access routers of each host. In SANA we consider intelligent ARs. We believe that such routers are essentially required in the future Internet. Each AR performs traditional routing and data delivery functions, but is additionally responsible for other functions related to resolution process and mobility control for example. SANA uses identifier-based communications in the edge networks and locator-based routing in the backbone Internet.

There are four levels of resolution in our proposal. The first resolution is ensured by the DNS structures and finds the MID that corresponds to a name. MSID maintains the second level of resolution and maps the MID to its corresponding SIDs. These two types of resolutions are initiated by User Equipments (UEs). Note that it is possible to group together these resolutions in one structure and avoid the use of DNS in the architecture. SSRS maintains in a third place, the bindings between the SIDs and the locators of the corresponding ARs. Each SSRS is responsible for a specific class of service. SSRSs are queried by ARs, and not by the UEs. ARs maintain mapping tables between the SIDs and UEs IP addresses.

Note that, it is possible to consider a SANA network without intelligent ARs. In this case, the user device maintains the required mapping information, but we lose the concept of multi-device, i.e. one SID in different hosts.

5.3.4 Namespaces

In this section, we present the new namespaces introduced by SANA. We also show the difference between SANA naming model and the Identifier/Locator split naming models. SANA defines two new namespaces. The first namespace

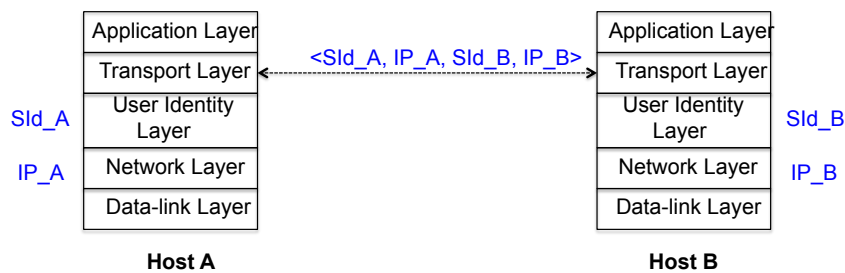


Figure 5.8: SANA Protocol Stack

consists of Master identifiers (MIDs). An MID is a subscription-based identifier that uniquely identifies a user's subscription to a third party, e.g. an ISP, an operator, etc. The idea of proposing such identifiers in SANA aims at providing a uniform level of identification for users above any types of access. Instead of identifying the user's terminals as proposed in the Identifier/Locator split solutions, our naming model takes a different approach. A terminal is seen as a set of access technologies on which a set of services can be offered. For that, we define SIDs that are a combination of a given MID and specific classes

5.3 General Design of SANA (Service-Aware Naming Architecture) 87

of services. Such classes already exist in mobile networks [65309]. We then extend that concept to our solution.

From a protocol stack point of view, we insert a new layer between network and transport layers. We call this layer the User Identity Layer. Thus, session connections in SANA are tied to SIDs as depicted in Figure 5.8.

Master-to-Secondary Identifier Directory (MSID) stores the mappings between an MId and its SIDs. These databases are operator-specific. MSIDs can only be updated by the operator after the user subscribes to a new type of services. The fundamental difference between an SSRS and an Id/Loc split resolution system is that it is based on the introduction of services in the network, and not on hosts. For example, RVS servers in HIP are updated when a new host arrives in the network. The notion of service is transparent to the resolution system.

The Service-Specific Resolution System (SSRS) is the second mapping system that we introduce and it maps SIDs to the IP address of the Access Router (AR) to which the user's terminal holding this SID is connected. We propose that SSRS is separated into different subsystems, each of them responsible of mapping a given class of identifiers. SSRS permit also to implement service policies in choosing the location.

5.3.5 Resolution System

In this section, we clarify how MIDs and SIDs are used in SANA and the underlying rationale.

We assume humans prefer using the easy-to-understand DNS name in the application layer. So we allow the mapping from the user name to the MId. Note that this mapping is not very dynamic. It can be implemented by adding a new Register Record (RR) type into DNS (similar to HIP). After getting the MId for the given user name, it can be further resolved into the corresponding SID.

Figure 5.9 illustrates the three level mapping and the entities involved in processing the mapping. For the mapping from the SID to AR's locators, a cooperation between the control and data plane is possible. Data plane can provide control plane with information helping to choose a given AR. In the same way, mapping SIDs to IP addresses (routing paths) is assisted by network link quality indicators.

Figure 5.10 summarizes the different resolution models presented in previ-

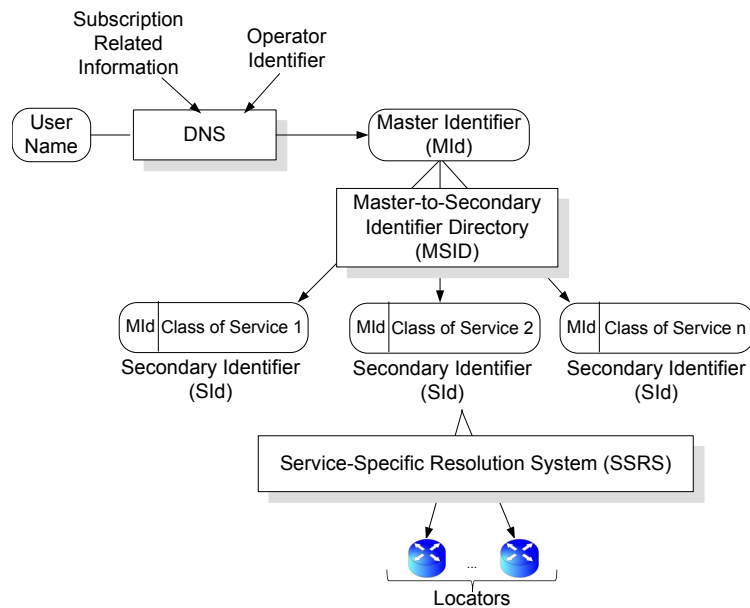


Figure 5.9: Resolution Steps in SANA

ous chapters and compares them to the SANA model.

5.4 Data and Control Planes

Figure 5.11 shows the data plane and the control plane of SANA.

5.4.1 Data Transport Plane

As depicted in Figure 5.12, communications between a host and its AR is governed by the Secondary-identifier Communication Protocol (SCP). Communications between two ARs in the backbone follow the Data Delivery Protocol (DDP). SCP and DDP protocols are the main components of the data plane.

The design of a SCP header is based on conventional IPv6 headers as presented in Figure 5.13. The difference between an SCP header and an IPv6 header is that the former uses SIDs instead of IP addresses. Moreover, we omit IPv6 traffic class field because this notion is already embedded in SIDs.

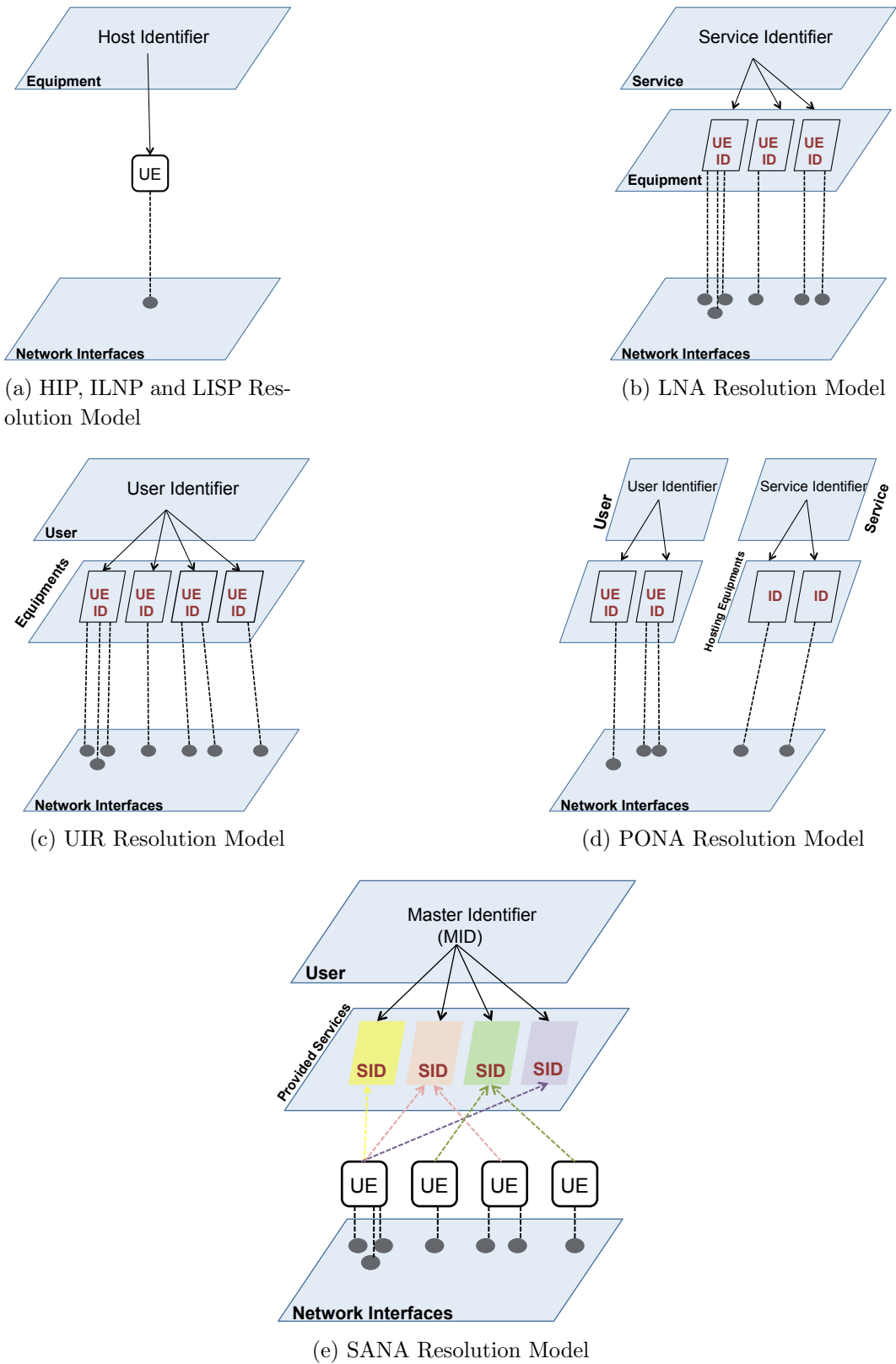


Figure 5.10: SANA Resolution Model vs other Naming Models

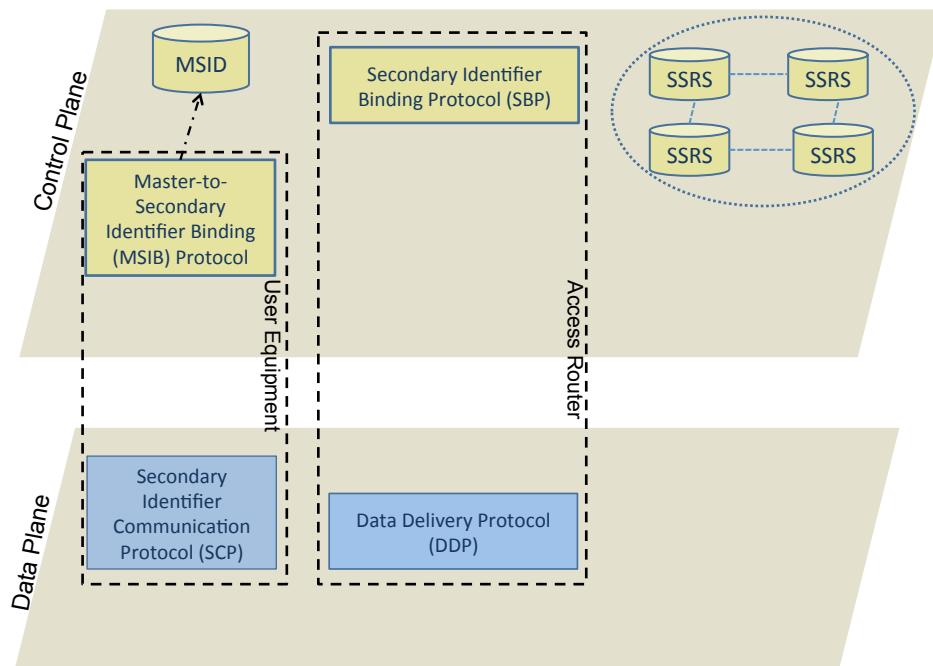


Figure 5.11: Data and Control Planes in SANA

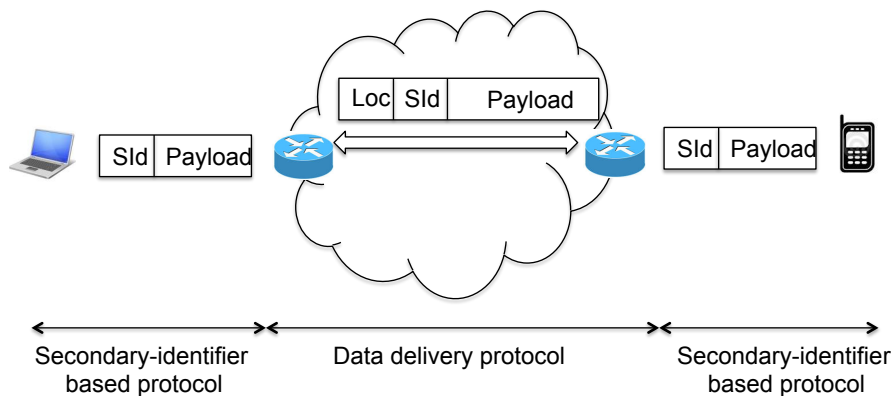


Figure 5.12: User Data Plane in SANA

5.4.2 Control Plane

- **Secondary Identifier Binding Protocol (SBP):** SBP is a control protocol that is used to bind a given SId to the associated locators. SBP is processed between a host and its attaching AR or between an AR and the SSRS.

SBP packet format is shown in Figure 5.14.

Version	Header Length	Payload length	
Source SId length	Dest SId length	Next header	Reserved
Source SId			
Destination SId			

Figure 5.13: Data Packet Format in SANA

Packet Type	Flag	Total Length	
Loc Type	Id Type	Loc length	Id Length
Loc 1			
SId 1			
//			
Loc n			
SId n			

Figure 5.14: SBP Packet Format in SANA

Packet field description:

- **Packet Type (8 bits)** : indicates the type of SBP packet, which are described in Table 5.1
- **Flag (8 bits)** : reserved for future use
- **Total length (16 bits)** : the length of the packet in bits
- **Loc Type (8 bits)** : the type of the locator (e.g. IP address, MAC address)

- **Id Type (8 bits)** : the type of the identifier in use (e.g. SId)
- **Loc Length (8 bits)** : the length of the locator in bits
- **Id Length (8 bits)** : the length of the identifier in bits

The three types of SBP packets are defined as follows:

Packet type	Encoding value	Description
Map_Register_Request	1	From host to AR / from AR to SSRS
Binding_Ack	2	From AR to host / from SSRS to AR
Update	3	From host to AR

Table 5.1: SBP Packets Types

- **Master-to-secondary Identifier Binding (MSIB) Protocol:** It is a control protocol used by the host to retrieve the corresponding SIDs of a given MId. The two types of SBP packets are defined as follows:

Packet type	Encoding value	Description
Map_Request	1	From host to MSID
Map_Answer	2	From MSID to host

Table 5.2: MSIB Packets Types

1. The Map_Request message is sent from the host to MSID to map a given MId into one/a set of SIDs. Its packet format is shown in Figure 5.15.
 2. The Map_Answer message is sent from MSID to the host. It contains the different retrieved SIDs. Its packet format is shown in Figure 5.16.
- **Mobility Update Protocol (MUP):** It is a control protocol used to support mobility in SANA. It is exchanged between ARs. The format of an MUP packet is shown in Figure 5.17.

The list of MUP packets is presented in Table 5.3.

Packet Type	Flag	Total Length	
MId Type	SId Type	MId length	SId Length
MId			
SId			

Figure 5.15: MSIB Map_Request Packet Format

Packet Type	Flag	Total Length	
MId Type	SId Type	MId length	SId Length
MId			
SId			
Correspondent SId 1			
//			//
Correspondent SId n			

Figure 5.16: MSIB Map_Answer Packet Format

5.5 Communication Scenarios

5.5.1 Scenario 1: Registering a new user SId

In this section, we explain how the different mappings of the system are published and updated.

When a new user terminal attaches to the network, it sends an SBP Map register Request to its corresponding AR where it announces its different enabled SIDs with their corresponding IP addresses as depicted in Figure 5.19.

Packet Type	Flag	Total Length	
Id Type	Loc Type	Id length	Loc Length
SId			
Loc			

Figure 5.17: MUP Packet Format

Packet type	Name
1	Routing Update Request (RUR)
2	Routing Update Ack (RUA)

Table 5.3: Types of MUP Packets

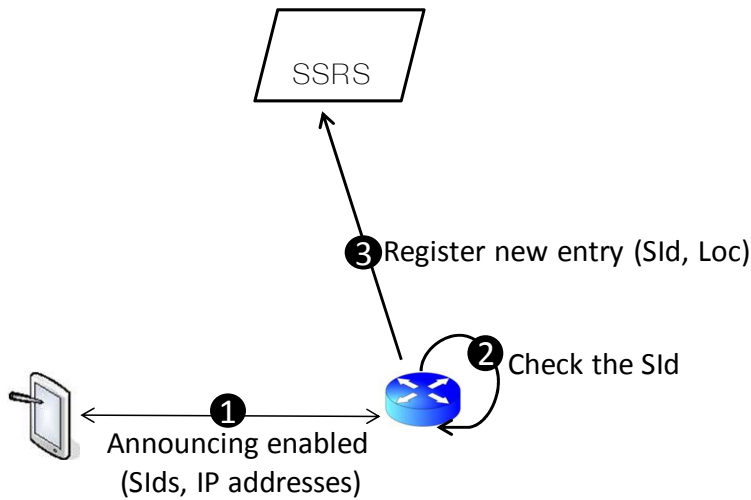


Figure 5.18: Announcing a new SID

Upon receiving this message, the AR checks if the SIDs are already declared by a previous user's terminal. If it is the case, the AR adds the new IP address(es) to the corresponding SID entry. Notice that in such situations, no updates nor new entries are required to SSRS which results in a significant reduction of the SSRS size especially comparing to Identifier/Locator split solutions where each arrival of a new terminal induces systematically a new

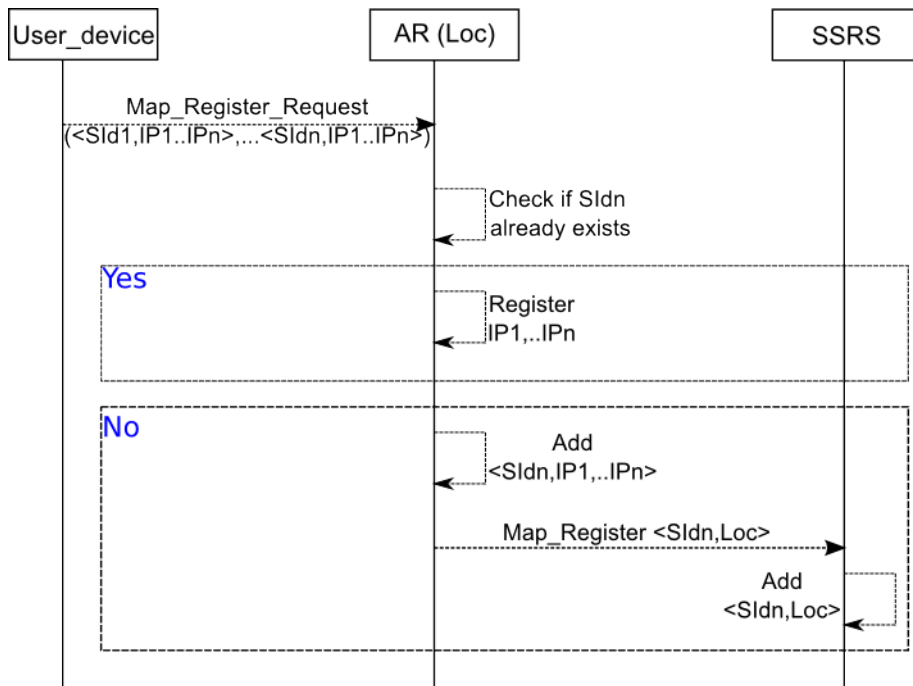


Figure 5.19: Announcing a new SID

identifier entry in the resolution system. For a new SID, the AR creates a new entry in its local forwarding table and associates it with the corresponding IP address(es). At the same time, it sends a request to the SSRS where it announces the new SID and registers the new couple of SID and its locator.

5.5.2 Scenario 2: Communication Process

SANA supports person-to-person communications where the end communication parties are users and not their devices. Let us suppose that user A wants to initiate a chat session with user B. For that purpose, A uses a terminal that holds SID_A which is an SID that can process this type of communications. As shown in Figure 5.20, the following steps are processed by the system.

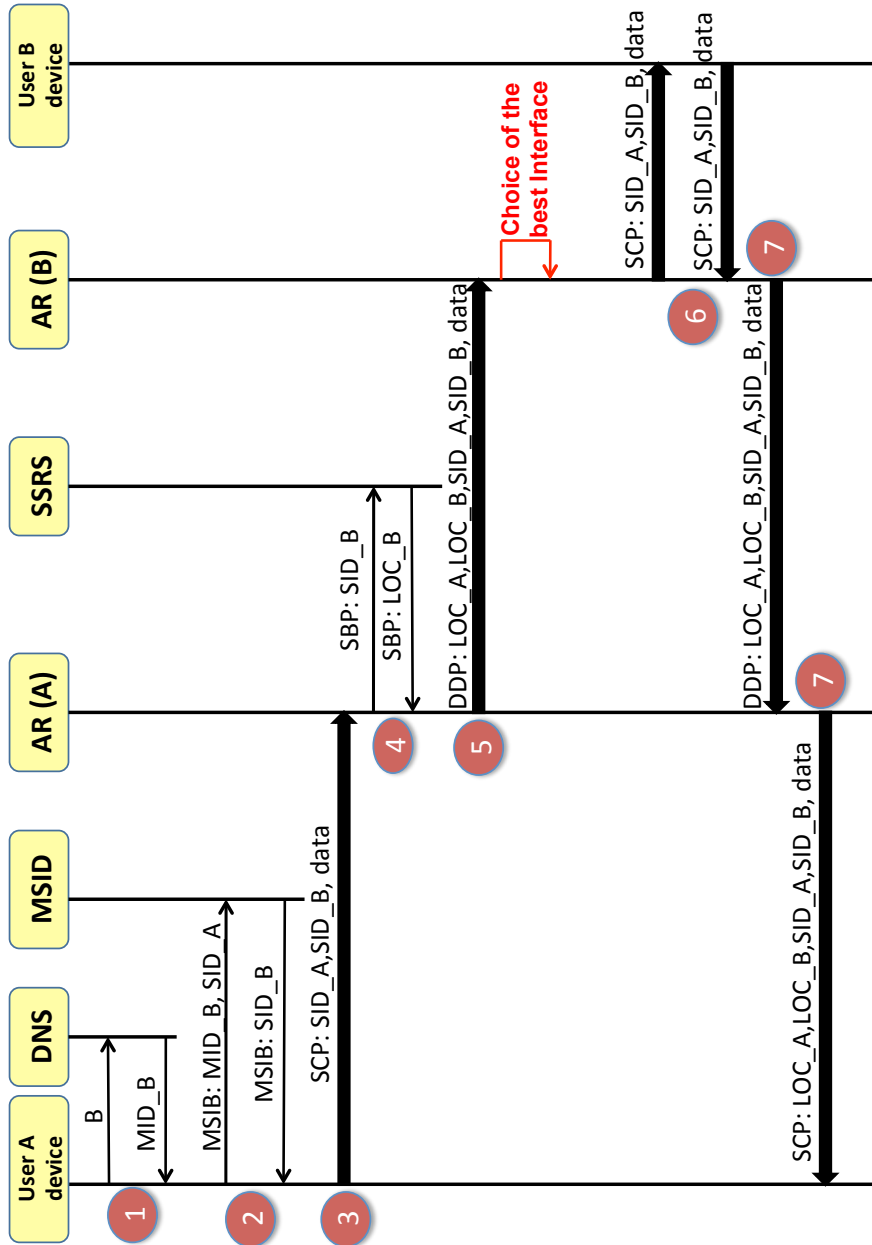


Figure 5.20: Connection Establishment in SANA

1. User A initiates the communication by sending a query message to the DNS structure, which contains the name of the called user B. DNS confirms receipt of this message by replying with the MID of user B, MID_B.
2. On receiving MID_B, user A interrogates the MSID structure to determine the SID of user B via an MSIB Map_Request message. The message contains MID_B and SID_A that corresponds to the SID that will be used by user A in this session. The MSID searches if user B has an SID that matches the class of service requested by A. If it is the case, the MSID returns SID_B in an MSIB Map_Answer message. Unless, the MSID informs user A that user B is unable to process her request.
3. User A sends a data packet which contains SID_A and SID_B to her AR (AR_A).
4. AR_A queries the SSRS structure to determine the IP address of AR_B. It uses for this purpose the SBP Map_Register_Request. The SSRS returns LOC_B.
5. AR_A encapsulates the data packet sent by user A, which contains SID_A, SID_B and data, by adding LOC_A and LOC_B as source and destination addresses.
6. Upon receiving this packet, AR_B decapsulates it, chooses the IP address that best matches the type of the required communication and sends the initial data message to B. The choice can be based on collected network information.
7. In reverse, the packets sent from user B to user A are encapsulated by AR (B).

5.5.3 Scenario 3: Host Mobility

In our architecture, device mobility is equivalent to the mobility of all the SIDs hold by the device. We present hereinafter the details of intra-domain and inter-domain mobility procedures.

- **Intra-AR Host Mobility:**

When a host moves within the area of the same AR, it must update its IP address(es) and SIDs mappings. For this purpose it uses the SBP

update packet in which it specifies the SIDs concerned with the update. The network, SSRS and the correspondent node(s) remain unaware of this change.

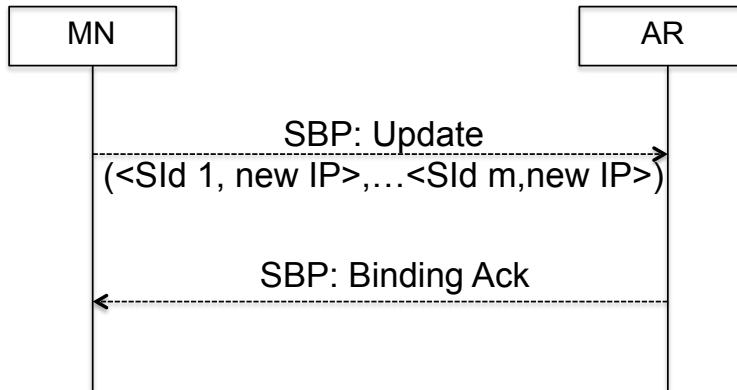


Figure 5.21: Intra-AR Host Mobility in SANA

- Inter-domain Host Mobility

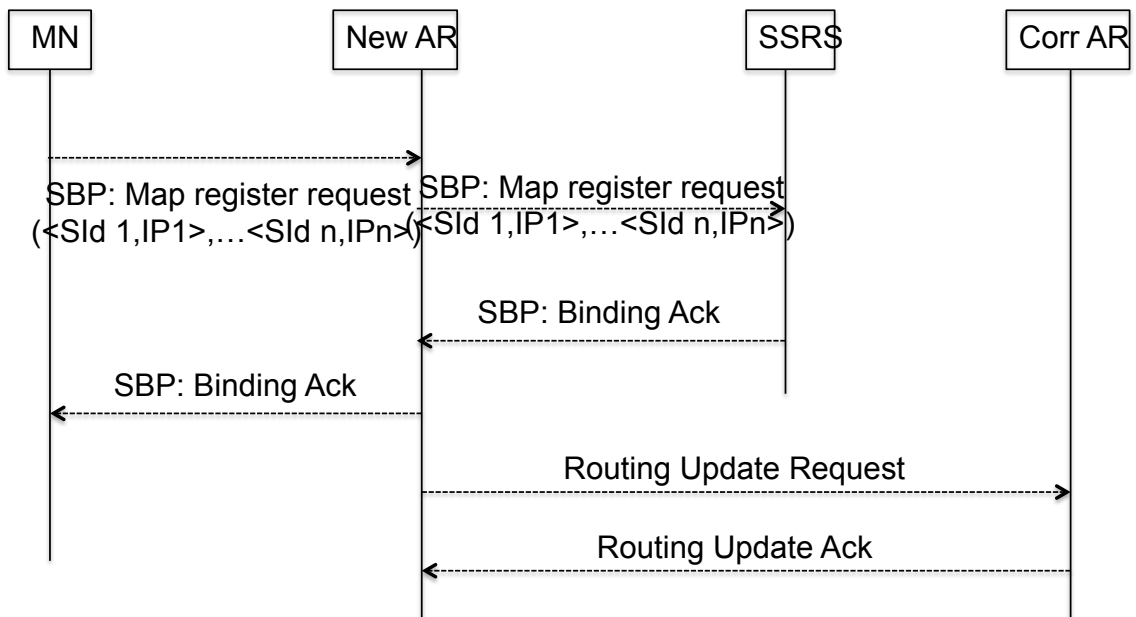


Figure 5.22: Inter-domain Host Mobility in SANA

In the case of inter-domain mobility and when the host attaches to a new AR area, it registers its SIDs with the new AR using the SBP protocol.

The new AR sends a Routing Update Request (RUR) message to the correspondent AR. In response to the RUR message, the correspondent AR sends a Routing Update Ack (RUA) message to the new AR. The data path between the two communicating hosts is now changed to new AR - *correspondent*AR.

5.5.4 Scenario 4: Host Multi-homing

- **Host Multi-homing on one AR:** In this scenario, we assume that user B maintains for instance one device with one SId. The SId is multi-homed on two IP interfaces (IP1, IP2). In the local mapping table of the AR, we can find the following entry : SId – IP1, IP2. When the AR receives a connection demand for this SId, it selects the best IP interface on which it processes the communication. Decision can be made on the basis of the link quality, the QoS, etc.
- **Host(s) Multi-homing on Different ARs:** Two use cases are possible: i) user B uses two hosts, each of them connected to an AR ii) user B uses one multi-homed host connected to several ARs. That is, at the level of the SSRS, two locators are associated with the SId of user B. Various alternatives are possible in order to choose on which AR the query should be processed. Before analyzing these different options, let us review some points about the architecture. The choice of the AR is based on two main criterion: the network links capacities and the appropriateness between the queried type of communication and the IP interfaces maintained at the AR. An ideal choice has to take into consideration these two points together. However, the first option consists of centralizing the choice in the SSRS. That is, SSRSs collect periodically information about the ARs and their networks capacities, and they make the choice based on these information. A first inconvenient of this solution is that it requires additional traffic between the ARs and the resolution structures. It also implies frequent updates for the SSRS. The second option stands for implementing a cooperative mechanism between the ARs in order to select the appropriate AR. This solution implies as well additional traffic between the ARs especially when these latter are geographically distant.

5.5.5 Scenario 5: User Multi-homing vs. Device Multi-homing

We define user multi-homing as a user having simultaneously more than one connected device. In our architecture, the network remains agnostic of such situations. As shown in Figure 5.23 for example, the AR of user A stores

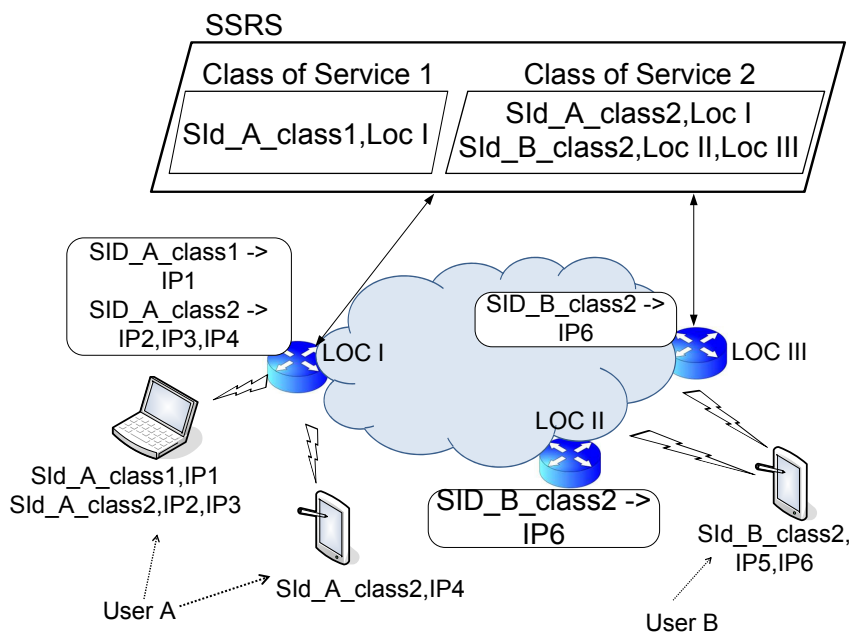


Figure 5.23: User and Device Multi-homing in SANA

the mapping (SId_A_class2, IP2, IP3, IP4) without having the information that these IP addresses belong to different devices. It is equivalent to the case of a multi-homed device having all its interfaces connected to the same AR. In this way, we achieve user's devices transparency to the network which is an important property in future networks.

The case of a multi-homed SID over different ARs is presented as depicted in Figure 5.23 with an entry with different AR locators at the level of SSRS. In such cases, a choice policy of the network to which a specific request has to be directed should be specified. Operators can define policies to direct a given type of applications to a specific type of networks. At the same time, traffic engineering mechanisms and load balancing can be implemented at the level of ARs to ensure that a best choice of the interface that will process a given service. Moreover, with this model we ensure a late binding between the SID

and the IP address since the mapping is only done at a very low level of the architecture. ARs have the best visibility of the network to take over this role.

5.5.6 Scenario 6: User-Session Transfer

We highlighted above the importance of providing a transparent session transfer. In this section we show how we achieve this property in SANA.

From a protocol stack point of view, transport connections and sessions are tied to SIDs in our naming architectures. While migrating a given service from a user terminal to another, the correspondent user's terminal remains agnostic of this operation since the used SID in the communication is not going to change. Moreover, even the network does not know about it because user data

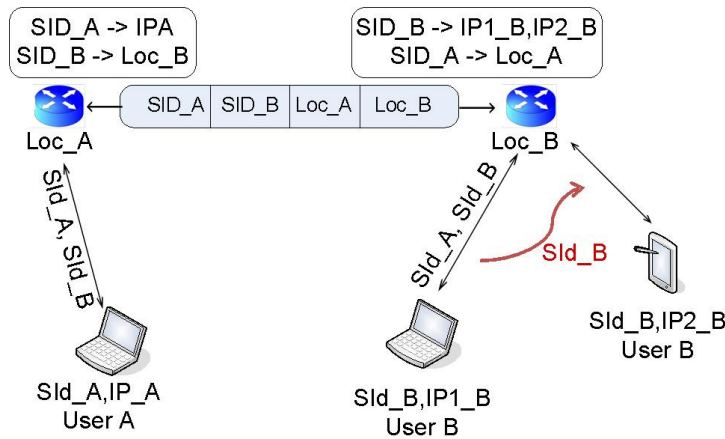


Figure 5.24: Session Transfer in SANA

packets transport SIDs and not terminals identifiers. Only the concerned AR is notified of this change, since it has to redirect the packets to the new IP address. It means that the session transfer is managed locally at the level of the AR which avoids any updates or solicitation for the global SSRS. Note that, it is of course required to transfer the context of the session between the terminals.

5.6 Chapter Conclusion

In this chapter, we have presented a new naming architecture called SANA. Differently from other host-based Identifier/Locator split proposals, our solution highlights user-level requirements. We focus on providing a naming

model that can efficiently handle emerging user multi-device support and mobility of services between terminals of the same user. There are two types of identifiers in SANA, i.e, Master Identifiers (MIDs) and Secondary Identifiers (SIDs). Thanks to MIDs, we provide an integrated presentation of users in the architecture. And with SIDs, we identify services related to the same user independently of location and devices. Moreover, a solution for transparent session transfer over different terminals is provided.

In Chapter 6, we will present qualitative and quantitative evaluations of SANA. We will also compare the performances of SANA and other Id/Loc separation approaches.

Chapter 6

Design Enhancements and Evaluation of SANA Architecture

6.1 Introduction

Chapter 2 and Chapter 4 have presented requirements on naming systems design from a host-level perspective and user-level perspective, respectively. The previous chapter has introduced one main contribution of this thesis: Service Aware Naming Architecture (SANA). As we have explained in that chapter, SANA has been proposed to address the naming and addressing challenges for the Future user-oriented Internet.

In this chapter, we provide further analysis addressing SANA answers to ITU-T requirements and RRG design goals. The chapter is intended to describe how our contribution provides benefits regarding both host-level and user-level design requirements. It also provides synthetic analysis of all the naming models studied so far in this thesis. We compare SANA as a representative four-level hybrid model with host-based solutions, network-based solutions and other four-level models namely LNA and UIR. Although not providing the same functionalities, the comparison between SANA and three-level Id/Loc split schemes can provide an idea on the impact of adding an additional resolution layer.

This chapter is organized in two main sections. The first section presents

a qualitative analysis of SANA. We evaluate our architecture against ITU-T requirements and RRG design goals enumerated in Chapter 2 and user-level requirements described in Chapter 4. We provide a comparison between SANA performances and state of the art solutions in various perspectives.

The second section provides analytical evaluation results of SANA and a comparison with other solutions.

6.2 Architectural Discussions and Design Enhancements

- **Hybrid Design** : In section 2.6, we have classified Id/Loc split solutions into core-edge separation approaches and host-based approaches. SANA provides a hybrid architectural style in which it combines the two approaches. By using PI-PA address indirection, it allows users in the edge to continue to use PI addresses transparently without scalability problem and renumbering cost.
- **Evolutionary or Clean Slate Design?**: In section 2.3, we have investigated the two research trends regarding the design of the future Internet, i.e. Clean slate approach and evolutionary approach. As the Id/Loc split concept is considered to be an inevitable component of the future networks, it is intriguing to answer the following question: Is Id/Loc split a clean slate or an evolutionary approach? More particularly, is SANA a clean slate or an evolutionary approach?

Based on the classification scheme that we have provided in section 2.6, routing on flat identifiers is obviously a clean slate approach. It is because it advocates the redesign of the existing routing mechanisms and the use of new identifier-based routing protocols.

Network-based split solutions are evolutionary approaches. They keep the main core existing architecture and bring modification to routers only. In the same way, host-based split solutions are also evolutionary approaches. Actually, they keep an evolutionary kernel of the current Internet. They keep the use of stack layers although they add an additional resolution layer, and they keep also existing routing infrastructure and end-to-end communications.

SANA is also an evolutionary approach that brings original flexibility to the architecture. Indeed, it allows host-based and network-based Id/Loc split to coexist in the same architecture. It facilitates thus transition phases and provides the advantage of letting the environment select the most suitable approach depending on the context.

- **Optimizing Resolution Mechanisms :** The performance of SANA relies heavily on maintaining up-to-date mapping records at different network locations. The four-step name resolution used in SANA architecture may increase the time needed to retrieve the SId and locator related to a user name. Consequently, optimization is necessary. For this purpose, the resolution process can be converted into a three-step process by having the DNS forward the MId resolution request to the MSID, or by simply having the two entities physically merged. This can reduce the time required to get the locator of the corresponding node.

Similarly, in the events of mobility and multi-homing, we need to minimize the time required to update the host locator in the AR record and the SSRS, to prevent the host from becoming unreachable.

However, the first packets of a new session may suffer from the latency of the mapping system. The mapping from DNS name to MId is done by DNS. Since this mapping is static to some extent, a caching mechanism can help reduce this latency. The mapping from SId to locators is fulfilled by the dedicated SSRS infrastructure that has predetermined location in the backbone network, which can help reduce the latency.

6.3 Integration of SANA domains and Legacy Domains

SANA hosts and legacy hosts will coexist in the Internet. Therefore we discuss in this section possible transition mechanisms of SANA. We distinguish three use cases: Communication between two SANA hosts, communication initiated by a SANA host and communication initiated by a legacy host.

- **SANA hosts to SANA hosts:** Two SANA hosts which implement the new identifiers in their networking stack are able to talk to each other directly using the process presented previously in section 5.5.

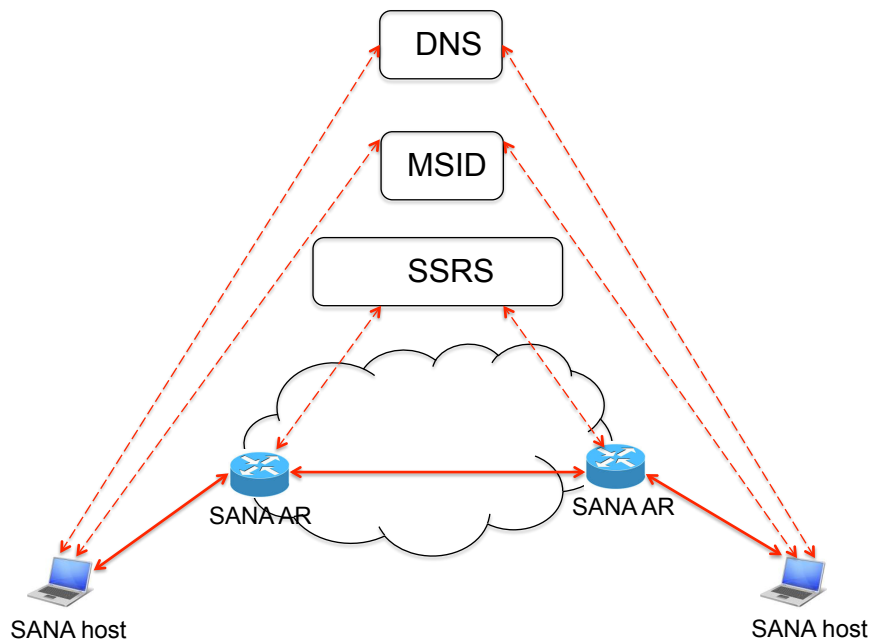


Figure 6.1: Communication between two SANA hosts

- **SANA hosts to legacy hosts:** if SANA host A wants to talk to legacy host B that has a traditional FQDN, it sends a first resolution request to DNS. Instead of receiving the MId of B, A receives an IP address and can thus easily distinguish the legacy address from an MId. A directly sends an ordinary data packet to B.
- **Legacy hosts to SANA hosts:** The legacy host receives an MId instead of receiving an IP address. It forwards the MId to a default SANA-Aware router. The address of this router is pre-configured in the host. The router processes an MSIB Map request on behalf of the legacy host in order to get the SId of the SANA host. The rest of the communication procedure is the same as between two SANA hosts. The default access router hides the fact that the host is not SANA-based.

It means that we implement an asymmetric behaviour. If SANA host initiates the communication, it is aware of the legacy host. If SANA host is the corresponding host, it is unaware of the legacy character of the initiator. We have done this architectural choice because we think that SANA host has more capabilities than a legacy host. It is able to process a legacy communication. However, a legacy host delegates a SANA AR because it is unable to deal with

MIDs as with IPv6 addresses.

As for deployment, we separate it into several gradual steps:

- Deployment of SANA-aware routers at the borders
- Deployment of the user plane identifier and locator split, end-to-end mobility and multi-homing procedures.
- SANA domains management and assignment, deployment of MSIDs and SSRS and DNS names to MIDs mappings registers in DNS.
- implementation of signalling

The deployment is also open to potential new technologies and enhancements.

6.4 Answers to Functional ITU Requirements

In Table 6.1, we summarize the answers of SANA to the ITU-T functional requirements presented in Chapter 2.

6.5 Answers to RRG Design Goals

In this section we investigate whether SANA can meet the RRG design goals expressed in Chapter 2.

- **Routing Scalability:** The new architecture supports scalable routing by adopting a hybrid style including both core-edge separation and host-based separation. It allows to use PI to PA address indirection in the ARs. It makes thus possible to continue using PI addresses on the edge without augmenting the size of the BGP routing table. Only PA aggregated addresses are used in the backbone routing in SANA.
- **Mobility:** SANA inherits the benefits of host-based approaches to provide mobility support. Since sessions are bound to SIDs instead of IP addresses, sessions are portable when hosts are mobile.
- **Multi-homing:** SANA inherits the benefits of Id/Loc split to provide multi-homing support. The relation between an SID and IP addresses is one-to-many. Moreover, multihoming in SANA no longer harms the routing scalability due to the split of identifiers and locators.

Functional ITU-T Requirements	SANA
Req_id 1	Yes
Req_id 2	Yes
Req_id 3	Yes
Req_id 4	Yes
Req_id 5	users and services
Req_id 6	Yes
Prop_id 7	permanent only
Prop_id 8	flat
Prop_id 9	easy but requires the support of the operator
Req_MSF 1	Distributed
Req_MSF 2	No
Req_MSF 3	ref to Section 6.8
Req_MSF 4	ref to Section 6.8
Req_MSF 5	ref to Section 6.7
Req_MF 1	ref to Section 6.7
Req_MF 2	ref to Section 6.3
location privacy	future work
fault tolerance	future work

Table 6.1: SANA Answers to Functional ITU-T Requirements

- Traffic engineering:** In SANA, a secondary identifier can be mapped to different locators to support multihoming. These locators may be preferred with different priority or sequence for load balancing. Both end-host and the AR can participate in the selection of the locator. Thus, the SSRS infrastructure can easily be used for traffic engineering of incoming packet flows.
- Renumbering:** Renumbering is simplified in SANA. In fact, when hosts get new locator blocks, their SIDs remain unchanged. The renumbering will be taken care by the ARs and SSRS infrastructure.

6.6 Answers to user-level Requirements

In this section we investigate SANA answers to user-level requirements described in section 4.2 .

- **Req_1: Identification of users and services** SANA is a new network proposal that is based on considering the future Internet as a network that interconnects users instead of hosts. SANA separates user identity expressed by MIDs from locators and makes abstraction of hosts. It thus enables users to be identified independently from the hosts they are using. It also facilitates applications because it gets rid of application-specific names. All applications can work using unified MIDs. Moreover, by proposing such support for users identifiers, SANA provides the basis of a ubiquitous Internet access and helps information sharing between users.

In SANA, services are identified using SIDs. They are classified into classes of services. Concerning the definition of a 'service' in SANA, it is important to clarify the following points. In general, the use of a service in the network can be classified in two use cases: 1) Entity A requests a given service from entity B 2) Entity A requests a service available in the network (e.g. a user requesting a video on Youtube) In SANA we are mostly concerned with the first use case. For that purpose we have defined SIDs.

Note that, the context of our research is different from machine-to-machine (M2M) networks. In fact, these networks provide automated communications among distributed devices. However in SANA, we put the light on communications inter users.

- **Req _2: User Multi-homing**

In the current Internet, a user has different identifiers for each service he/she is using. For example, he/she can have a messenger identifier when he/she uses MSN messenger and an email address 'user@yahoo.com'. It means that every service is independent. In SANA we define an integrated vision of services. the user has an MID which is a uniform identifier to allow other users to reach him independently from the application he/she is using. We make thus user multihoming possible throughout different hosts.

- **Req_3: Handover between Devices is Agnostic to Applications**

Sessions in SANA are tied to SIDs which are host-independent and application-independent. Therefore users are able to switch ongoing sessions among their devices freely while keeping session survivability. It is clear that SANA facilitates this type of scenarios by making applications get rid of networking constraints, but at the same time it is worth noting that SANA does not solve all the problems related to session transfer.

- **Req_4: Selection of a Proper Device for each communication**

The MId to SID mapping request in SANA allows the selection of a proper device for each type of communications. The MSID look up the related SIDs and decide which appropriate SID should be returned.

6.7 Security

SANA-based functions raise severe security issues because they require securely maintaining dynamic mapping information between names, MIDs, SIDs and locators at various points in the network. Since this architecture requires network nodes such as border SANA routers to send location update signaling messages on behalf of mobile hosts, vulnerabilities could arise if proper security functions are not implemented in the border routers as well as in the hosts. The security issues and their possible solutions are as follows:

- **Authentication of mobile hosts for network access:** When a mobile host arrives in the edge network, it declares its different SIDs. A malicious node can declare fake SIDs. This is why it is necessary that each SANA node authenticate itself or its SIDs before the corresponding AR registers the node information. For this purpose, different alternatives are possible. The node may present some credential, e.g., a certificate received from a mutually trusted certificate agency, to the border router of its SANA domain. On verifying the host's credential, the border router creates an entry in its mapping table and grants network resources (e.g., locators and bandwidth) to the mobile host.
- **Authentication between hosts:** As with certain secured services in the present Internet, the new generation network requires hosts to authenticate each other to access communication services provided by the peer

host. SANA can use similar security services between communicating nodes when required.

- Authentication of border routers: In SANA, not only end hosts but also network nodes such as border routers take part in mobility signaling on behalf of mobile hosts. This creates severe security implications. A malicious entity can send location update messages to hijack communication sessions belonging to other hosts. Therefore, the border routers must be authenticated before any location update messages are accepted by other border routers or hosts. Border routers belonging to the same administrative domain can use a shared secret for this verification purpose. For border routers belonging to different administrative domains, we need to find an effective security mechanism.
- Verification of signaling messages and data packets: We also need security mechanisms to verify that the location update signaling messages have come from the authenticated entity (host or router). Similarly, we should also be able to verify that data packets are from the authenticated host and that the integrity of the packet is intact.

6.8 Optimization of Resolution Performances

We propose to give first hints at the performance of the proposed architecture. First, we describe and discuss the properties of the different mappings used in SANA and their influence on the overall performance of the solution. Then, we analyze the impact of the new proposed naming model on the resolution structures.

Mappings in SANA are organized in a decreasing order in terms of dynamicity and update frequency. The first mapping between the users names and their MIDs is stored as aforementioned in DNS and is a many-to-one record. Since this binding is quasi static and is not frequently updated, using DNS to store MIDs has no impact on the performance of SANA. Actually, the DNS record is updated only after a new subscription to a given operator takes place. For instance in HIP, DNS is more solicited since each arrival of a new terminal in the network requires adding a new DNS record in which the terminal identifier and its correspondent Rendez-Vous server [LE08] locator are published. MSIDs ensure the second level of mappings in the architecture.

The bindings of MIDs to SIDs are one-to-many and their updates frequency depend on the services to which the users are subscribed. These structures are critically important for operators since they store subscription relative information. Consequently they shall be maintained with a high level of trust and security. It is only at the third mapping processed by SSRS that location information are revealed. Actually, one of the motivations behind SANA design is to delay the binding between identifiers and location information and to separate it into two steps. SSRSs first indicate the choice of the correspondent domain that contains the queried identifier. Secondly, the choice of the final destination IP address is distributed over the access routers.

Along with the motivation of integrating the presentation of a single user in the network, SANA is also built around one major goal which is increasing the performance of the resolution system by reducing its total size and decreasing as maximum as possible the number of signalling messages which occur after network events (user arrival, terminal arrival, terminal mobility, session mobility, etc). The new use of SIDs in SANA helps fulfilling these two requirements.

6.9 Summary

Hereafter, we provide a comparison between the requirements answers of all the naming solutions that we have studied so far in this thesis. All the presented proposals pursuents Id/Loc separation structure. They have few architectural similarities. So, the aim of this section is to summarize the comparison of architectural features of all the approaches studied so far. Tables , , and highlight the features of each naming solution. The schemes have been compared using unified attributes such as infrastructure requirements, resolution system and mobility related features.

	Three-level Models			Four-level Models		
	Network-based solution	Host-based solution	Hybrid solution	LNA	UIR	
Clean Slate/ Evolutionary	LISP Evolutionary	HIP Evolutionary	ILNP Evolutionary	SANA Evolutionary	Evolutionary	Evolutionary
Namespaces	No new namespaces	One new namespace	no new namespace	two new namespaces	two new namespaces	two new namespaces
Resolution	1) DNS name → <i>EID</i> 2) <i>EID</i> → <i>RLOC</i>	1) DNS name → <i>HIT</i> 2) <i>HIT</i> → <i>IP</i>	1) DNS name → (<i>EID, Loc</i>)	1) DNS name → <i>MID</i> 2) <i>MID</i> → <i>SId</i> 3) <i>SId</i> → <i>IP</i>	1) Name → <i>SId</i> 2) <i>SId</i> → <i>EId</i> 3) <i>EId</i> → <i>IP</i>	1) Name → <i>userId</i> 2) user Id → <i>terminalId</i> 3) terminal Id → <i>IP</i>
Mapping System	Flat and implementation-dependent (LISP-Alt, LISP-Tree, etc.)	Central	Central(DNS)	Central (MSID) and Flat (SSRS)	Flat (DHT)	Hierarchical

Table 6.2: Summary of all the Naming Schemes (1/4)

	Three-level Models		Four-level Models		
	Network-based solution	Host-based solution	Hybrid solution	LNA	UIR
	LISP	HIP	SANA		
Use of PI/PA addresses	PI/PA (Indirection)	elimination of PI	PI/PA (Indirection)	not specified	not specified
Routing scalability	Yes	No	Yes	No	Yes
Security	No	Yes	Yes	No	No
Mobility	No	Yes	Yes	Yes	Yes
Scalability	Yes	Yes	Yes		
Deployment	very easily adopted	changes in all hosts and applications	very easily adopted	changes in hosts and routers	changes in hosts and infrastructure
Evolvability	No	Yes	No	No	No

Table 6.3: Summary of all the Naming Schemes (2/4)

	Three-level Models			Four-level Models		
	Network-based solution	Host-based solution		Hybrid solution	LNA	UIR
	LISP	HIP	ILNP	SANA		
Changes in DNS	No	Yes	Yes	Yes	No	No
IPv4 support	Yes	Yes	Yes	Yes	Yes	Yes
IPv6 support	Yes	Yes	Yes	Yes	Yes	Yes
Host Mobility	Yes	Yes	Yes	Yes	Yes	Yes
Host multi-homing	Yes	Yes	Yes	Yes	Yes	Yes
Traffic engineering	Yes	Yes	No	Yes	No	No
Renumbering	Yes	Yes	Yes	Yes	No	No
Multicast	No	No	No	No	No	No
NAT traversal	No	Yes				
Mobile networks	No	Yes				

Table 6.4: Summary of all the Naming Schemes (3/4)

	Three-level Models		Four-level Models		
	Network-based solution	Host-based solution	Hybrid solution	LNA	UIR
	LISP	HIP	ILNP	SANA	
Host modification	No	Yes	Yes	Yes	Yes
AR modification	Yes	No	No	Yes	Yes
Tunneling	Yes	No	No	Yes	Yes

Table 6.5: Summary of all the Naming Schemes (4/4)

6.10 Analytical Evaluations

In this thesis, we have categorized the existing Id/Loc split architectures into three-level models and four-level models. We have also introduced SANA as a new hybrid approach. In the previous sections of this chapter, we have shown that SANA can theoretically bring answers to both host-level and user-level requirements.

In this section, we are interested in carrying out a comparative cost analysis of SANA and other architectures. To do so, we use the same analytical models that we have presented in Chapter 3. We calculate the Connection Establishment Cost (CEC) and the Data Processing Cost (DPC) of SANA, LNA and UIR. For that, we recall the same cost definitions that we have already presented in Section 3.2. Moreover, in the literature we do not find evaluation work nor for LNA nor UIR.

6.10.1 Assumptions and Network Model

SANA Network: We assume that we have the network configuration shown in Figure 6.2.

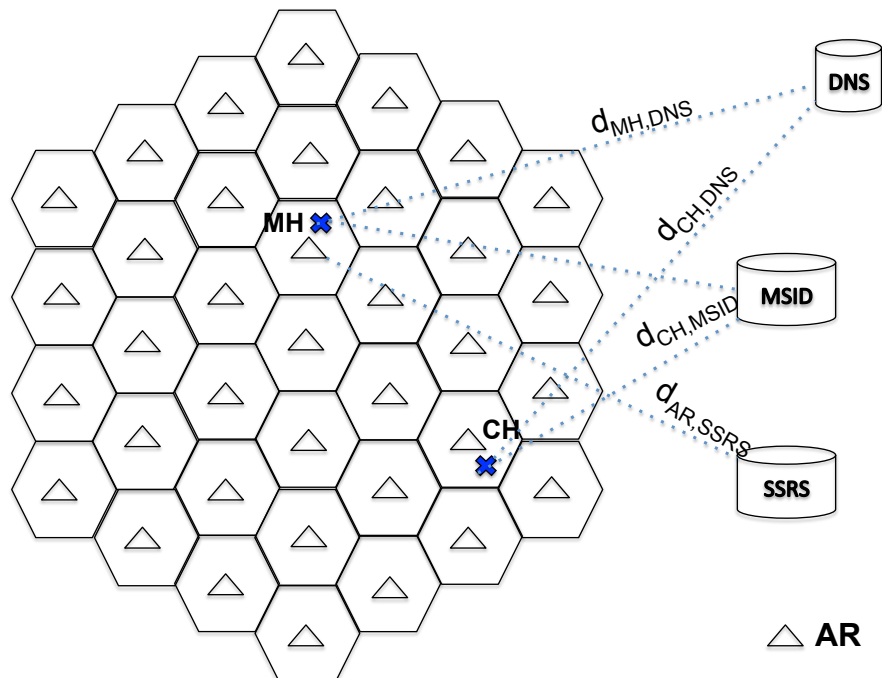


Figure 6.2: SANA Network Configuration

We assume as shown in the figure above that the network hosts are served by one MSID and one SSRS.

LNA Network: LNA network is depicted in Figure 6.3.

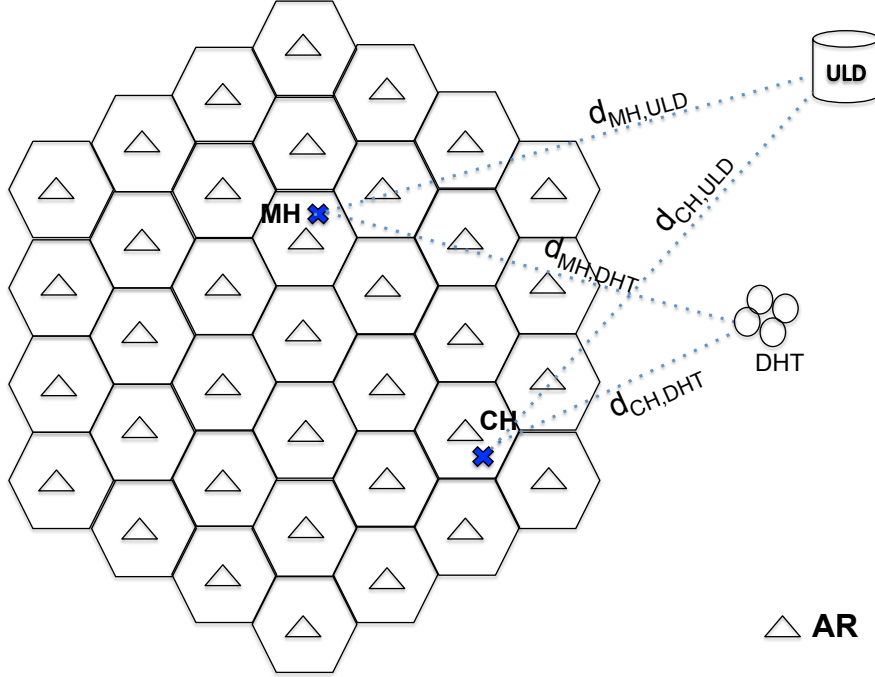


Figure 6.3: LNA Network Configuration

UIR Network: UIR network is depicted in Figure 6.4.

6.10.2 SANA Connection Establishment Cost CEC(SANA)

As described in Section 5.5.2, the resolution messages in SANA consists of: a DNS query to request the MSID, an MSID query to find out the Sid, a control data packet sent from the host to its AR and finally an SSRS query to request the locator of the corresponding AR. Thus, the Connection Establishment Cost of SANA, $CEC(SANA)$ is calculated as follows:

$$CEC(SANA) = \lambda_s(2C_{DNS}^{IPv6} + 2C_{MSID}^{IPv6} + C_{MH,AR}^{SCP} + C_{AR,SSRS}^{Map.request} + C_{SSRS,AR}^{Map.reply}) \quad (6.1)$$

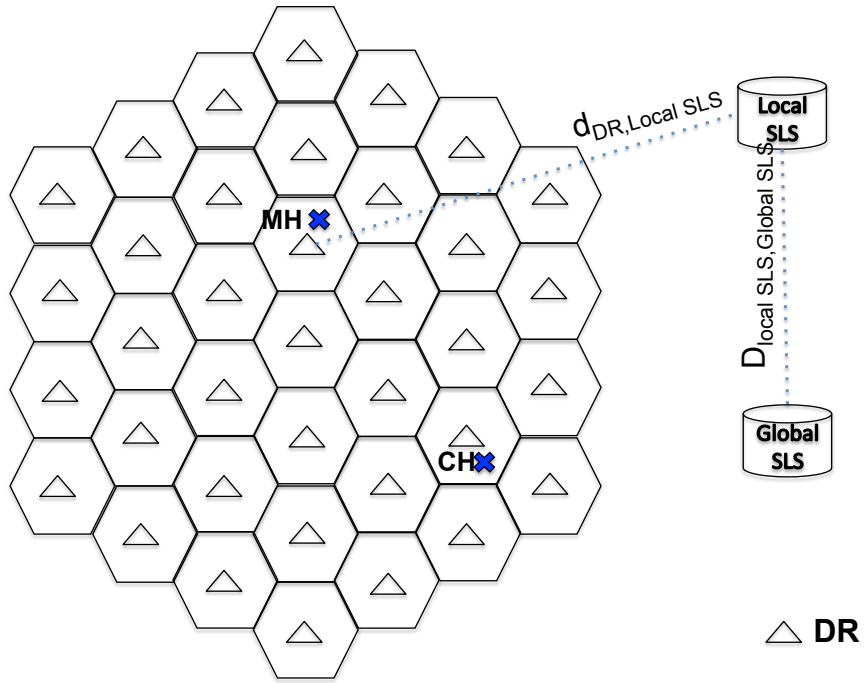


Figure 6.4: UIR Network Configuration

Where :

$$C_{DNS}^{IPv6} = Size_{IPv6} * d_{MH,DNS}$$

$$C_{MH,MSID}^{IPv6} = Size_{IPv6} * d_{MH,MSID}$$

$$C_{AR,SSRS}^{Map_request} = Size_{Map_request} * d_{AR,SSRS}$$

$$C_{SSRS,AR}^{Map_reply} = Size_{Map_reply} * d_{SSRS,AR}$$

C_Y^X is calculated as the product of the size of the packet and the number of hops.

6.10.3 SANA Data Packet Processing Cost DPC(SANA)

The SANA Data Packet Processing Cost DPC(SANA) is calculated as follows:

$$DPC(SANA) = \lambda_s(C_{MH,AR}^{SCP} + C_{AR,AR}^{DDP} + C_{AR,MH}^{SCP}) \quad (6.2)$$

Where :

$$C_{MH,AR}^{SCP} = Size_{SCP} * d_{MH,AR}$$

$$C_{AR,AR}^{DDP} = Size_{DDP} * d_{AR,AR}$$

$$C_{AR,MH}^{SCP} = Size_{SCP} * d_{AR,MH}$$

6.10.4 LNA Connection Establishment Cost CEC(LNA)

As described in Section 4.5.1.2, the session establishment in LNA requires: a ULD query to find out the SID, a first DHT query to find out the corresponding EID and finally a second DHT query to request the corresponding IP addresses. Thus CEC(LNA) is calculated as:

$$CEC(LNA) = \lambda_s(2C_{ULD}^{IPv6} + 2C_{DHT}^{IPv6} + 2C_{DHT}^{IPv6}) \quad (6.3)$$

Where :

$$C_{ULD}^{IPv6} = Size_{IPv6} * d_{MH,ULD}$$

$$C_{DHT}^{IPv6} = Size_{IPv6} * d_{MH,DHT}$$

6.10.5 UIR Connection Establishment Cost CEC(UIR)

Based on the resolutions steps described in Section 4.5.2.2, the connection establishment cost of UIR is calculated as follows:

$$CEC(UIR) = \lambda_s(2C_{MH,DR}^{IPv6} + 2C_{DR,LocalSLS}^{IPv6} + 2C_{DR,GlobalSLS}^{IPv6}) \quad (6.4)$$

Where :

$$C_{MH,DR}^{IPv6} = Size_{IPv6} * d_{MH,DR}$$

$$C_{DR,LocalSLS}^{IPv6} = Size_{IPv6} * d_{DR,LocalSLS}$$

$$C_{DR,GlobalSLS}^{IPv6} = Size_{IPv6} * d_{DR,GlobalSLS}$$

6.11 Numerical Results

In Table 6.6, we present the messages sizes that we have obtained from the protocols specifications.

Message	Size in bytes
<i>Size_{IPv6}</i>	120
<i>Size_{Map.request_MSIB}</i>	40
<i>Size_{Map.reply_MSIB}</i>	40
<i>Size_{Map.Request_SBP}</i>	92
<i>Size_{Map.Reply_SBP}</i>	92
<i>Size_{SCP}</i>	40
<i>Size_{Size_DDP}</i>	92

Table 6.6: Numerical Values of Messages Size in SANA

For parameters' values, we set the following default values : $d_{MH,AR} =$, $d_{MH,CH} = 15$, $d_{MH,DNS} = 30$, $d_{MH,MSID} = 20$, $d_{AR,SSRS} = 18$, $\mu_c = 4mn$, $R = 3950m$.

6.11.1 Impact of Correspondent Nodes

In this section, we study the impact of the number of correspondent nodes on the Connection Establishment Cost and the Data Processing Cost. Figure 6.8 illustrates the Connection establishment Cost of SANA, HIP, LISP and ILNP. More generally, it means that we compare in this figure the performances of three-level approaches and a four-level approach in terms of Connection

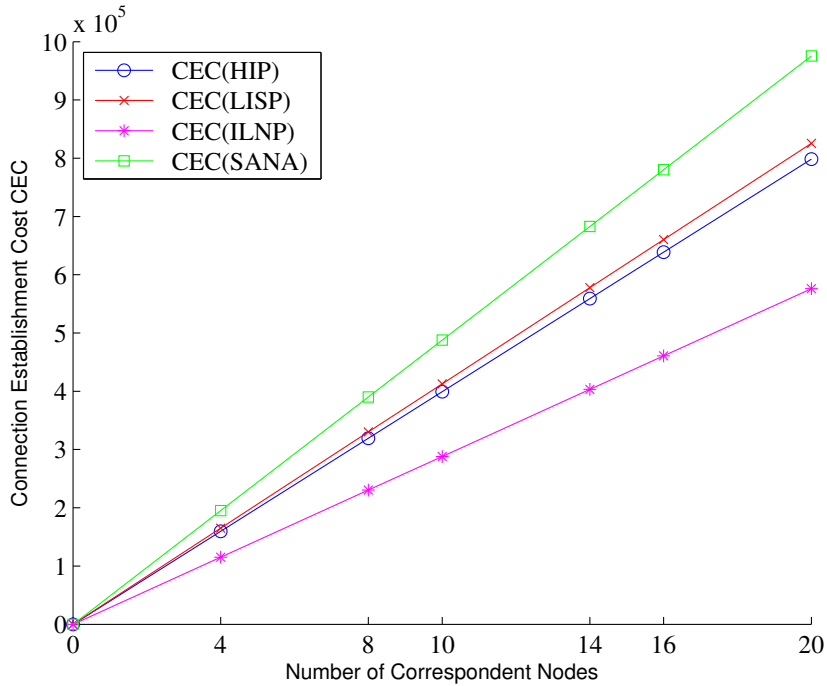


Figure 6.5: Connection Establishment Cost/Correspondent Nodes

Establishment Cost. The CEC increases linearly for both SANA and other approaches. Besides and as expected, the signaling cost required by SANA is bigger than the one of traditional Id/Loc split architectures. As an indicative number, the ratio between CEC(SANA) and CEC(HIP) is equal to 1.22. Actually, this result is expected because additional resolution levels are required in the case of four-level solutions.

In Figure 6.6, we consider the problem from a different perspective. We compare the CEC of all the four-level solutions that we have presented in this thesis. We also consider two sub-scenarios for an LNA-based network, i.e. a DHT with 50 nodes and a DHT with 100 nodes. From the results presented above, we can see that SANA and UIR have nearly the same performances. However, we can see that an LNA-based network presents the highest CEC. It is due to the latency caused by DHT-based resolution [PMTZ06].

In Figure 6.7, we compare DPC(SANA) with host-based solutions and network-based solutions.

As an investigation of packet delivery cost, the performance of SANA is better than LISP and worse than HIP and ILNP. It means that the impact

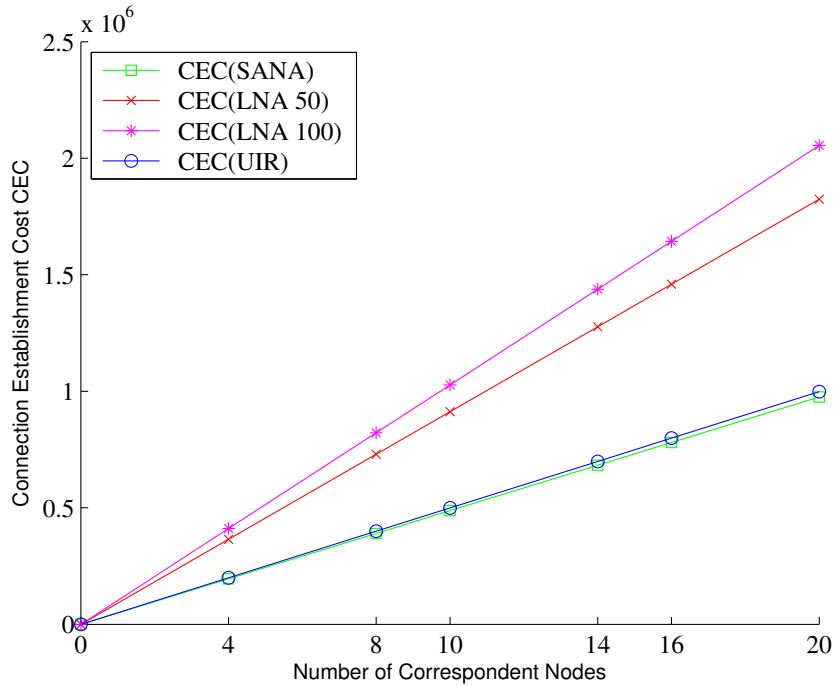


Figure 6.6: Connection Establishment Cost/Correspondent Nodes

of the number of correspondent nodes remains the biggest for encapsulation approaches and the smallest for host-based approaches.

6.11.2 Impact of Network Scale

In this section, the impact of the network scale is investigated. Figure 6.8 and Figure 6.9 present the evolution of the Connection Establishment Cost as a function of the network scale. As we have explained before, LISP and ILNP are not impacted by the variation of the network scale. However, the interesting observation that we can find out from this Figure is that SANA although being a fourth level approach generally outperforms HIP. In networks with a network scale included between 0.33 and 0.2, CEC(HIP) is smaller than CEC(SANA). However, when we increment the network scale, we remark that CEC(SANA) is slightly impacted. It remains almost the same. From Figure 6.9, we can see that CEC (LNA) is not impacted with the network scale. It can be explained by the fact that LNA connection establishment is based on DHT. CEC(UIR) increments linearly however. SANA outperforms these two architectures by

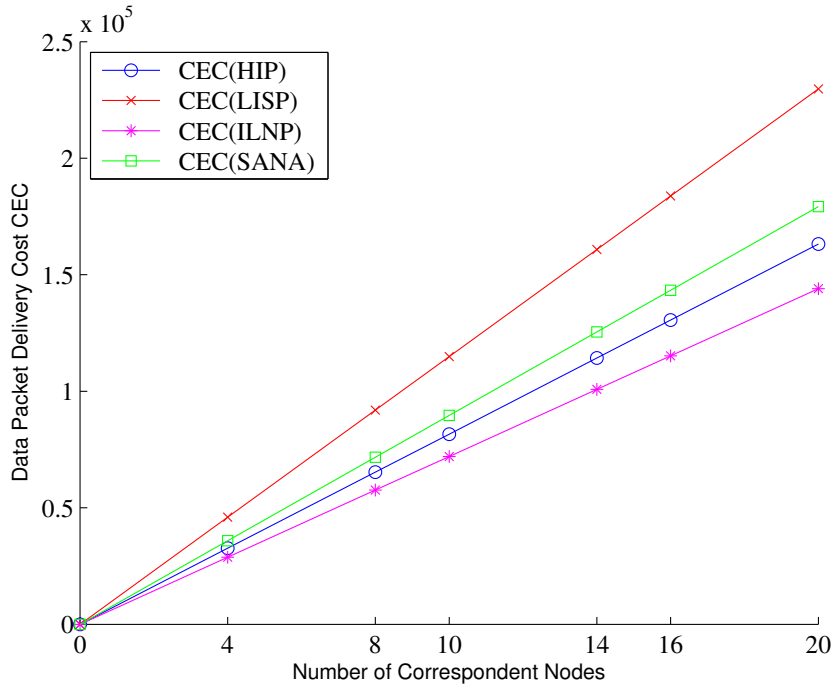


Figure 6.7: Data Packet Delivery Cost/Correspondent Nodes

presenting the lowest CEC even for highly distributed networks.

6.12 Resolution System Performance: SANA vs Id/Loc split architectures

As a complementary evaluation study, we choose to quantify the performance of SSRS and to compare it to a traditional Identifier/Locator split resolution system which stores the mappings between terminals identifiers and their IP addresses.

For that, we define the following scenario. We consider a network in which users arrival times are modeled using a Poisson process with a parameter λ , where λ is the mean of arriving users. We classify the services into four classes:

- Conversational
- Internet
- Gaming

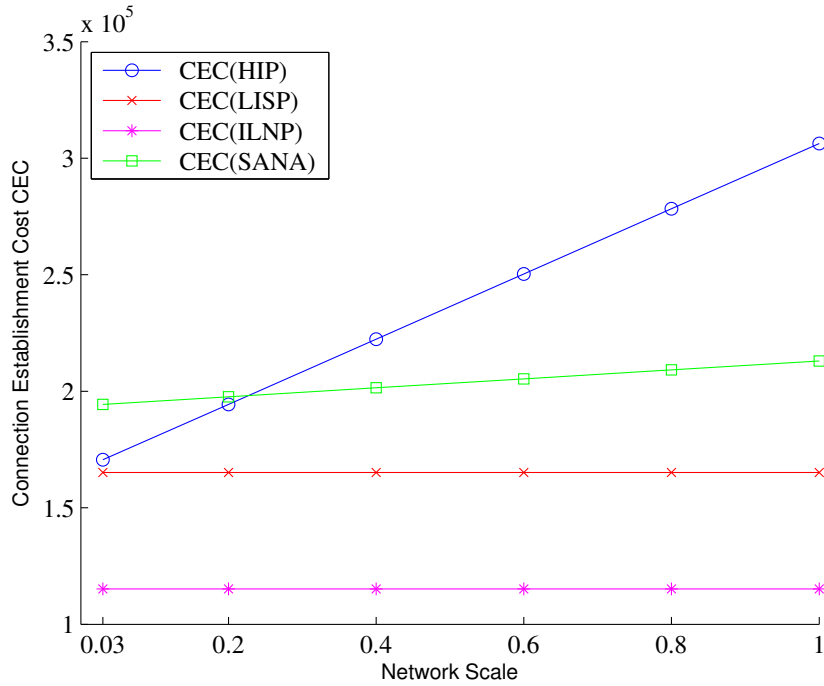


Figure 6.8: Connection Establishment Cost/Network Scale

- Video

We suppose that we have seven types of terminals having different service capabilities varying between 1 and 4. We grow the number of users in the network by increasing the parameter from 10 to 50. We consider three cases:

- **Case 1:** A network where each user can have at most two devices
- **Case 2:** A network where each user can have from three to four devices behind the same AR
- **Case 3:** A network where each user can have from four to seven devices behind the same AR

We study the impact of these different parameters on the size of the resolution structure in both SANA-based network and Identifier/Locator split based-network.

The results of the simulations are shown in Figure 6.10.

For the first scenario case and as depicted in Figure 6.10a, the size of SSRS in SANA grows more than a traditional resolution system. This is due to

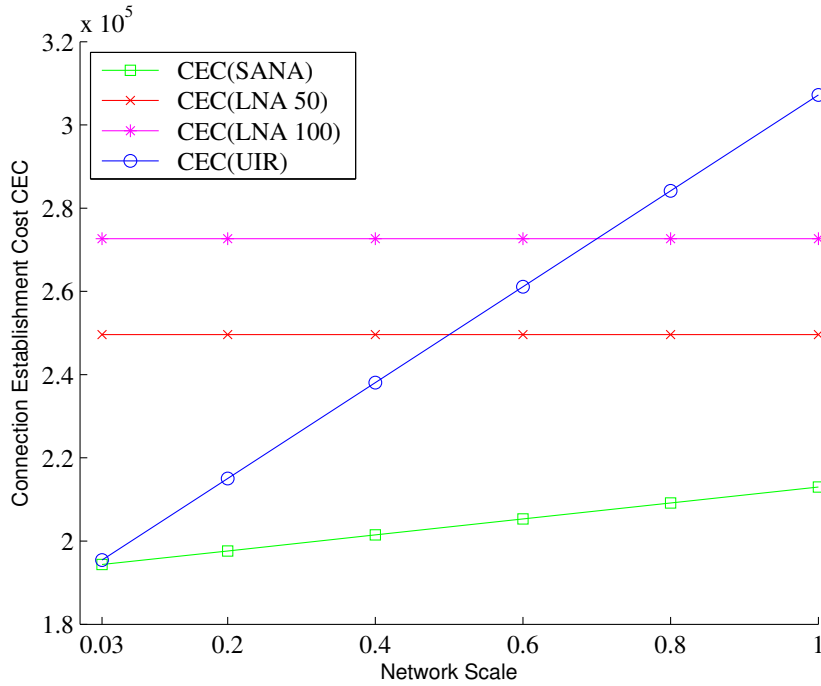
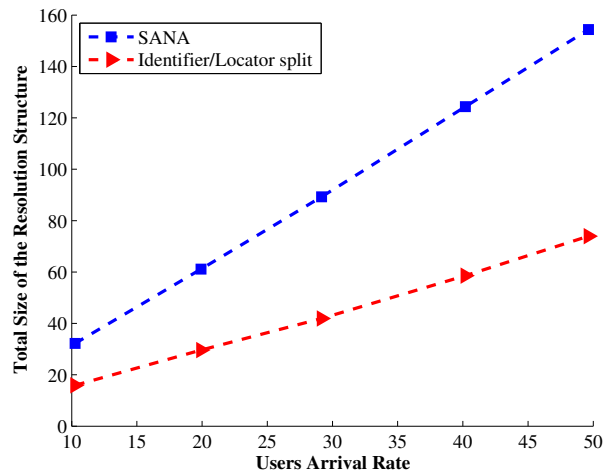
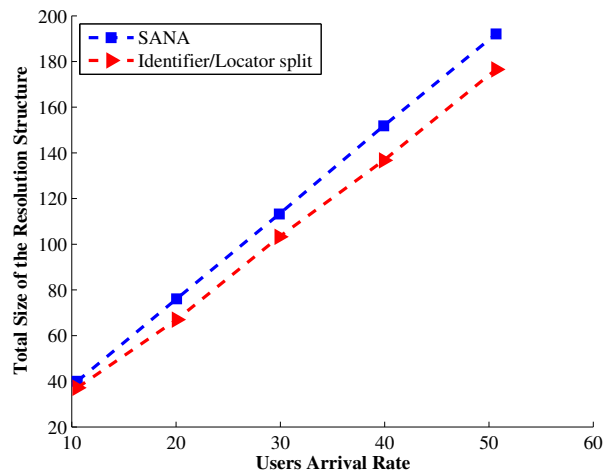


Figure 6.9: Connection Establishment Cost/Network Scale

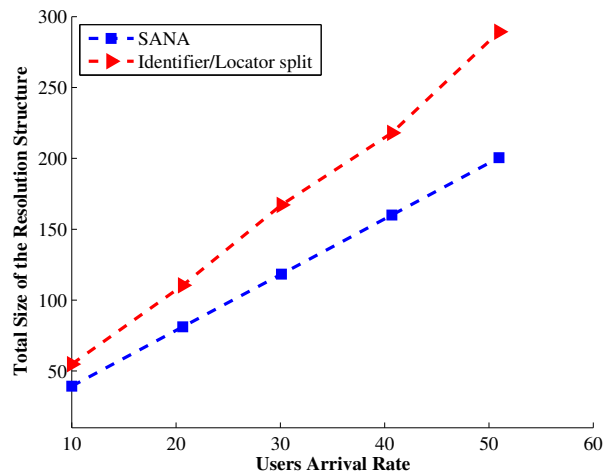
the fact that the number of services announced exceeds the number of devices connected per user. But the assumption that a single user has only one or two connected devices does not fit the new trends of communications and even the current usages where a user has more than two devices (e.g. mobile phone, PC, laptop, etc). In the second case as depicted in Figure 6.10b the two approaches' performances tend to be closer to each other. This is due to the fact that the number of devices is almost equal to the number of announced services. The performance of SANA in such a scenario depends heavily on the type of devices owned by the user and the number of announced services. In the third scenario which represents the expected future trends of communications in terms of multidevice support and as shown in Figure 6.10c, SANA outperforms clearly the Identifier/Locator split approach since the number of devices exceeds the number of published services. Given the statistics presented in [15] and [16], there is today an average of 2.5 connected devices per user and an average of four and five devices per user is expected in the future. Based on these statistics, we believe that SANA can be a useful solution for multi-device support in the future.



(a) Users with maximum two devices



(b) Users having between three and four devices



(c) Users having between four and seven devices

Figure 6.10: Total Size of Resolution Structure in SANA and Identifier/Locator Split Approach

A reduction in the number of the required signalling messages after the arrival of new terminals in the network. Actually in Identifier/Locator split approaches, a signalling procedure is required to register the new identifier. For instance in HIP, the registration process of a terminal to a Rendez-Vous server [14] requires 4 exchanged messages and a message to update the DNS.

To compare this approach with SANA in terms of number of signalling messages required upon the arrival of a new terminal to the network, we define a scenario where we vary the number of connected devices per user from 1 to 7. In SANA, we consider that a signalling message is equivalent to the message sent from the AR to the SSRS to register an SId. For the Identifier/Locator split network, we consider that only one message is required to register a new terminal identifier to the resolution system. This assumption allows us to have the lowest number of messages required, which is equivalent to the best performance of these approaches. The results are shown in Figure 6.11.

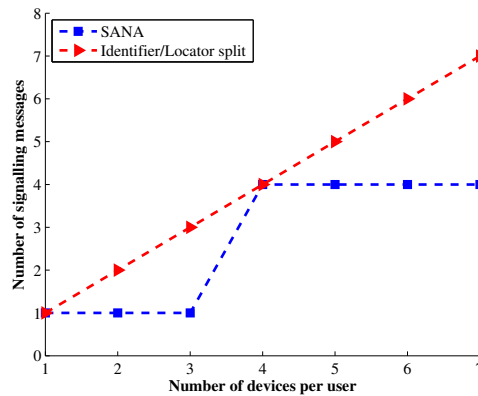


Figure 6.11: Number of Signaling Messages According to the Number of Terminals

In SANA the number of signaling messages required per user converge to 4 which is the number of classes of services. That is once the user announces all the classes, there is no need to update the SSRS again. The form of the curve presenting the signaling in SANA may vary from one scenario execution to another because it depends on the types of devices connected by the user. But in all the cases, the curves are asymptotic. In the other case, the number of messages increases linearly.

6.13 Chapter Conclusion

This chapter has presented how the main contribution of this thesis has been evaluated toward several host-level and user-level requirements. SANA has been proposed to overcome the shortcomings already identified.

The first part of the chapter has summarized the answers of SANA and other Id/Loc split solutions towards RRG design goals. The results assure us to say that SANA as a hybrid solution is capable of bringing a quite complete naming solution to both host-level and user-level requirements.

The second part of the chapter has presented numerical results to find out the impact of various network parameters, such as the number of correspondent nodes and the network scale. The cost-based evaluation model has been developed to compare our contribution with other state of the art solutions using the proposed network model. The presented results confirm that SANA consumes low cost compared to LNA and UIR in terms of connection establishment cost and data processing cost based on the network configuration presented in this chapter.

Chapter 7

Conclusion & Perspectives

Naming and addressing are fundamental aspects of network architecture and so the number of research work in this area is enormous. In this thesis, we have addressed the naming and addressing problem while focusing on users. Therefore, we have proposed a user-level naming architecture called SANA. Beside architecture design, we have also dedicated a significant part of our work for the comparative performance analysis of the existing naming schemes and our proposal. As we intend in our research work to study the naming problem with respect to users scenarios, we have followed the following rationals.

The first part of this thesis is dedicated to review thoroughly the existing naming architecture of the Internet. The future Internet is supposed to face various exciting and innovative features. The main output of this study is that the idea of overloaded IP addresses presents many shortcomings. We have then studied the Id/Loc split concept as it was proposed in the literature as a solution to Internet naming shortcomings. We have prepared a survey of the most interesting properties of this concept. We have also provided a summary and categorization of the past work in this field. Therefore, we have focused on some of the recent naming and identity/locator splitting proposals. The second output of this survey is to qualitatively study the pros and cons of network-based solutions and host-based solutions.

As we intend in this thesis to investigate in more details the existing naming schemes, we have dedicated the second part of our work to analytical evaluations. First, we have defined an analytical evaluation model for naming schemes modeling. In this analytical work, we have developed the analytical models and their parameters and defined the analysis criteria and their expres-

sions. Then, we have carried out a comparative analysis between the following representative protocols: Host identity Protocol (HIP), Identifier/Locator Network Protocol (ILNP) and Locator/Identifier Separation protocol (LISP). Based on the conclusions of these analyses, we have emphasized the host-centric property of these schemes.

In the third part of this thesis, we have introduced the user-level point of view in our naming study. We have presented use case scenarios. In summary, we have shown throughout these scenarios that with the rapid growing of Internet users and mobile devices, it is becoming increasingly popular that one user can have multiple devices. Moreover, it is a foreseeable need that the end-points of communications will become mobile across the network addresses they are using, or the devices they reside in. The main output of this part is that current Internet and proposed Id/Loc split schemes lack such support. Based on these conclusions, we have defined the requirements and objectives of a new user-level proposal.

We have proposed a novel naming architecture called Service-aware Naming Architecture (SANA). SANA focuses on user-to-user communications in the Internet to meet the requirements of user-level multi-homing and mobility. We show the general design of SANA by introducing two new namespaces and describing the interworking between layers in the new protocol stack. We use a service-based mapping and resolution way. We also discuss details of both network-level and user-level multi-homing and mobility in SANA.

After proposing the new scheme, we have carried out a qualitative analysis and a quantitative analysis. We have discussed the advantages of SANA compared to the existing protocols and other proposed schemes. We have studied SANA answers to the host-level and user-level requirements.

We have also shown that SANA reduces signaling costs comparing to other user-level schemes. Although it covers a larger scope than host-level solutions, it presents good performances in comparison with these schemes.

Moreover and similarly to any research work, different architectural choices have been done and several assumptions have been taken while designing SANA. It is true that we base our work on a user-level point of view. This is why we have focused our research on user communications scenarios. However, research about the future Internet includes an umbrella of networking technologies such as Content Centric Networks (CCNs), Internet of Things (IoT).

CCN is a novel design for the next generation Internet that aims at over-

coming the current limitations of the existing networks, by providing new protocols centered around the data itself. The CCN paradigm proposes to change the addresses of the packets which should point directly to the data that has to be retrieved rather than the location where such data is stored.

IoT is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. The basic idea of this technology is to identify devices.

The implementation of SANA can be adapted to such future Internet technology. We can for instance, form the basis of a virtualization framework using SANA. Virtual MIDs can be used and can refer to various SIDs. We believe that such a virtualization approach can open the way for diverse scenarios over SANA.

Another challenge of SANA is the management of home-based networks. We believe that SANA can be adapted to such scenarios. For instance, we can define a use case where the home access router is SANA enabled. All the user devices will be behind the same AR. Several policies based on QoS constraints for instance can be implemented.

Software defined networking (SDN) is a new paradigm of networking. It is the current trend to separate control and data planes and to provide a more flexible architecture. SDN makes the network programmable, giving the operator more control on its infrastructure for customization and optimization. Several work is needed in order to study the impact of SDNs on Id/Loc split solutions. A combination between these two technologies is possible but needs further analysis and evaluations. Moreover, implementations should be tested to validate these schemes.

On the other hand, one of Id/Loc split solutions challenges (including SANA) is the economic cost. Despite enormous efforts from both academia and industry in defining technical aspects, an economic model of the adoption process of Id/Loc split paradigm lacks. What are the drivers of this adoption? Who will adopt it? how the adoption and deployment process will evolve? In [IL10] the authors shed the light on this problem, but still much work in this direction is needed.

Last but not least, possible implementation of SANA under a 3GPP network is possible.

H2020 european research programs are preparing studies about 5G networks. Because mobile communications has prominent demands for user-level multi-homing and mobility, SANA can be used in such networks. Further studies about a possible integration of SANA in an LTE network is to be done in the future.

Appendix A

Résumé de la Thèse

Les tendances actuelles dans les réseaux fixes ainsi que les réseaux mobiles se dirigent davantage vers une très forte croissance du nombre des utilisateurs et des terminaux connectés. A titre indicatif, à l'horizon 2020, il est prévu que cinq billions d'utilisateurs à travers le monde seront connectés à Internet à travers vingt billions de terminaux fixes et mobiles [cis]. En même temps, avec l'évolution de la taille et la complexité de l'industrie des télécommunications, les offres de services destinées aux utilisateurs finaux sont de plus en plus variées et complexes.

Avec l'émergence de nouveaux besoins de communication, de nouvelles technologies ont vu leur apparition dans le monde des réseaux d'accès, dans l'industrie de fabrication de terminaux et aussi dans le marché des applications et des services. Ces progrès se manifestent en premier lieu à travers la succession des générations de réseaux qui amènent des débits de communication de plus en plus hauts et des services de plus en plus sophistiqués. Les technologies de la 4G qui sont déjà déployés aujourd'hui à travers le monde seront bientôt suivies de la 5G où les technologies du 'tout IP' et les aspects d'ubiquité et de convergence fixe/mobile seront mis en place. Les évolutions actuelles se dirigent vers une convergence des environnements hétérogènes afin de faciliter l'expérience des utilisateurs en premier lieu et des opérateurs et fournisseurs de services en second lieu.

L'hétérogénéité existe aussi dans l'industrie de fabrication de terminaux, récemment révoltée par l'apparition des nouvelles générations de smartphones. Avec cette multitude de moyens d'accès, l'utilisateur peut accéder aux services n'importe quand, n'importe où et avec n'importe quel terminal.

Il en est de même pour les services, qui se dirigent aussi vers une convergence à travers les réseaux d'accès. Avec les nouveaux besoins en matière de mobilité des utilisateurs non seulement à travers les réseaux d'accès mais aussi à travers les terminaux, la continuité et l'omniprésence des services seront capitaux pour les réseaux du futur.

Face à ce paysage, il y a un vrai besoin de repenser les principes de bases de l'Internet, y compris les problèmes liés au nommage et à l'adressage des entités connectées dans le réseau.

Le nommage est un principe fondamental de l'Internet. Aujourd'hui, il est convenu de l'industrie ainsi que du monde académique, que la majorité des limites de l'architecture actuelle telles que la gestion inappropriée de la mobilité et de la multi-domiciliation, l'explosion de la taille des tables de routage et la sécurité est due à des failles dans le système de nommage utilisé actuellement.

En particulier, il est question de pouvoir mettre en place des schémas de nommage adéquats avec les nouvelles évolutions des réseaux et de leurs usages. Cela comprend la définition de nouveaux formats de noms et d'adresses tout en identifiant clairement les relations entre les entités nommées et en fournissant des systèmes de résolution appropriés et efficaces.

Pour résumer, si nous essayons de traduire en termes de nommage les verrous que nous renvoyent les différentes exigences décrites ci-dessus et qui restent à prendre en considération dans la conception des réseaux de nouvelles génération, nous pouvons citer les points suivants:

- Une identification des utilisateurs indépendante des terminaux
- Une identification des utilisateurs qui prend en compte la convergence de services, la convergence de réseaux et la convergence de terminaux
- Une identification qui facilite l'expérience des utilisateurs quand ils sont mobiles ou quand leurs sessions sont mobiles

Les travaux de recherche dans notre thèse vont alors se focaliser sur l'étude du problème de nommage tout en se focalisant sur les besoins des utilisateurs nomades et sur l'amélioration de la QoE (Quality of experience) dans une

session en cours de type 'user centric' ou dans le cadre de transfert de sessions entre terminaux appartenant au même utilisateur. Nous nous intéressons en particulier à la vue de l'utilisateur pour analyser les problèmes auxquels les solutions de nommage doivent fournir une solution.

Des travaux de recherche autour du nommage existent déjà. Mais bien que nombreuses dans la littérature, les propositions existantes sont soit principalement basées sur des sessions 'host-centric' soit mettant le plan d'identification des utilisateurs en dessus de celui des terminaux.

A partir de l'analyse de l'état de l'art des mécanismes de nommage déjà existants et des différentes approches de gestion de la mobilité des utilisateurs et de leurs sessions, notre première contribution consiste à définir les limites de ces schémas et de justifier le besoin d'une approche intégrée de nommage des utilisateurs qui prend en compte l'hétérogénéité des technologies d'accès, des terminaux et des services.

La deuxième contribution de cette thèse est une solution de nommage de niveau utilisateur qui se base sur une vue convergente des réseaux et des services et une banalisation des terminaux en faveur de leur capacités de communication.

Cette thèse est organisée en sept chapitres dont l'introduction au premier chapitre et la conclusion dans le dernier chapitre. Le chapitre deux présente un état de l'art des mécanismes de nommage dans les réseaux IP. Depuis son début, l'Internet utilise des adresses IP pour représenter à la fois l'emplacement ainsi que l'identité des noeuds. Ce choix de conception a été motivé en partie par deux raisons :

- Lorsque Internet a été développé, la plupart des noeuds étaient des noeuds statiques, donc leur emplacement et leur identité étaient confondus.
- La structuration hiérarchique des adresses IP [Int81][DH95] ainsi que l'information topologique de localisation qui y est intégrée, permettent un routage plus efficace et une mise à l'échelle plus facile.

Les problèmes fondamentaux du protocole IP proviennent de cette surcharge sémantique [MZF07] et d'une combinaison de deux fonctionnalités distinctes sur l'adresse IP. L'une est son utilisation comme localisateur, par exemple comme une adresse qui désigne un emplacement dans la topologie du réseau et spécifie un point de raccordement au réseau. La seconde est celle d'un

identificateur qui décrit l'identité du noeud. Avec la prolifération rapide des terminaux mobiles connectés à l'Internet, et avec l'introduction de la multi-domiciliation avec laquelle un noeud donné peut avoir plusieurs identifiants, ce double rôle d'adresses IP devient de plus en plus problématique. Suite à cette étude, le chapitre introduit le concept de séparation identifiant/localisateur [MZF07] qui a été défini comme solution pour les problèmes actuels de nommage. Dans ce chapitre, nous présentons aussi une classification des approches de séparation identifiant/localisateur. Enfin, une analyse des recommandations émises par les deux standards ITU [20911] et RRG [LE11] est présentée.

Le chapitre trois présente la seconde contribution de cette thèse ou un nouveau modèle d'analyse quantitative des coûts des différentes solutions de séparation de l'identifiant et du localisateur est proposée. Cette analyse a pour but d'étudier les avantages et les inconvénients de chaque type de solution. Plus exactement, nous mettons l'accent sur les trois solutions suivantes: HIP (Host identity Protocol) [MNJH08], LISP (Locator/Identifier Separation Protocol) [FFML10] et ILNP (Identifier/Locator network protocol) [RA12]. Les coûts étudiés dans ce chapitre sont le coût d'établissement de connexion, le coût de transmission d'un paquet et le coût de signalisation pour la mobilité [ABB14].

Le chapitre quatre décrit l'évolution des modèles de nommage en mettant en évidence l'importance des utilisateurs dans les futurs réseaux. Il dresse une liste de besoins de niveau utilisateur. Ceci met clairement en évidence les limites des approches décrites dans le troisième chapitre et qui sont orientés vers les hôtes. Ce chapitre introduit aussi les premières solutions de la littérature qui ont tenté de mettre l'utilisateur au centre de leur conception. Il s'agit des solutions LNA (Layered Naming Architecture) [BLR⁺04b], UIR (User Identity Routing Architecture) [LPL⁺10] et PONA (Policy Oriented Naming Architecture) [PJPB08a]. Une comparaison entre ces différentes solutions met en évidence certaines lacunes de conception, ce qui justifie la conception d'une nouvelle architecture de nommage proposée dans le cinquième chapitre.

Le chapitre cinq détaille la troisième contribution de cette thèse qui est la proposition d'une architecture de nommage orientée utilisateur et nommée SANA (Service-Aware Naming Architecture) [ABB11]. Dans cette thèse, nous considérons une nouvelle approche de nommage dans laquelle nous nous focalisons à atteindre les objectifs suivants:

- Lier l'identification à l'utilisateur et non pas au terminal

-
- Assurer un accès transparent et omniprésent au réseau
 - Autoriser l'accès même en cas de déplacement à travers différents terminaux (favoriser la mobilité des utilisateurs, plutôt que la mobilité des terminaux)
 - Simplifier la gestion et le contrôle des informations privées liées au même utilisateur sur toutes les plateformes

Pour se faire, différents aspects qualitatifs sont pris en considération.

- La joignabilité des utilisateurs indépendamment des terminaux et des accès (user availability)
- La possibilité de déterminer la localisation de l'utilisateur à tout moment et à tout lieu (user location)
- La possibilité de déterminer les capacités d'un utilisateur donné par rapport à ses types d'accès disponibles (user capabilities) : Il s'agit de pouvoir décider si l'utilisateur est apte à recevoir une communication à un instant donné ou non
- Une flexibilité dans la gestion des sessions utilisateurs (faire abstraction des terminaux pour permettre un support flexible du transfert de sessions du même utilisateur)

Nous cherchons à séparer l'identité de l'utilisateur de sa localisation. Ce type d'approche permet non seulement de résoudre les problèmes traditionnels identifiés par l'approche de séparation identifiant/Localisateur, mais aussi de répondre aux exigences de niveau utilisateur tels que la multi-domiciliation et la gestion de mobilité à travers les terminaux. En outre, le nouvel espace de nommage permettra de faciliter le fonctionnement des applications du moment où elles n'ont plus à maintenir une multitude de noms, et utiliseront directement les noms des utilisateurs. Ce type de solution centrée sur l'utilisateur pourra ensuite fournir une base pour un accès et un partage d'information universels pour les utilisateurs. Dans ce chapitre, la conception détaillée et la spécification des différents scénarios de communication sont présentées.

Enfin, nous présentons une évaluation de SANA comme étant la dernière contribution de cette thèse. Nous menons une évaluation analytique de la proposition SANA et nous la comparons avec les résultats obtenus dans les

chapitres précédents. Cette partie nous a permis de quantifier les performances de notre proposition et d'identifier ses points forts surtout dans des scénarios centrés sur les utilisateurs.

Appendix B

List of Publications

Conference Papers

- Nahla Abid, Philippe Bertin, Jean-Marie Bonnin: SANA: A Service-Aware Naming Architecture for future Internet. *IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, Dec. 2011, Amman, Jordan [[ABB11](#)]
- Nahla Abid, Philippe Bertin, Jean-Marie Bonnin: Requirements on naming schemes design for future wireless Internet. *15th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2012, Taipei, Taiwan [[ABB12](#)]
- Nahla Abid, Philippe Bertin, Jean-Marie Bonnin: A Comparative Cost Analysis of Identifier/Locator Split Approaches. *IEEE Wireless Communications and Networking Conference (WCNC)*, 2014, Istanbul, Turkey [[ABB14](#)]

Patents

- Nahla Abid, Philippe Bertin: Method of resolving subscriber identifiers. *Publication No. WO/2013/011214* [[AB14](#)]

Talks

- Nahla Abid, Philippe Bertin, Jean-Marie Bonnin: Naming schemes design in future wireless Internet: Survey and Challenges. *25th meeting of Wireless World Research Forum (WWRF)*, 2010, Kingston University, London, UK

Bibliography

- [20911] Terms and definitions for next generation networks, 2011.
- [65309] 3GPP TS 23.203. Policy and charging control architecture (release 9), v9.2.0, December 2009.
- [AB12] RJ Atkinson and SN Bhatti. Optional Advanced Deployment Scenarios for the Identifier-Locator Network Protocol (ILNP). RFC 6748, November 2012.
- [AB14] N. Abid and P. Bertin. Method of resolving subscriber identifiers, April 3 2014. US Patent App. 14/008,928.
- [ABB11] N. Abid, P. Bertin, and J. Bonnin. Sana: A service-aware naming architecture for future internet. In *Applied Electrical Engineering and Computing Technologies (AEECT), 2011 IEEE Jordan Conference on*, pages 1–6, 2011.
- [ABB12] Nahla Abid, Philippe Bertin, and Jean-Marie Bonnin. Requirements on naming schemes design for future wireless internet. In *WPMC*, pages 11–15, 2012.
- [ABB14] Nahla Abid, Philippe Bertin, and Jean-Marie Bonnin. A comparative cost analysis of identifier/locator split approaches. In *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, pages 2946–2951, April 2014.
- [ABH09] Randall Atkinson, Saleem Bhatti, and Stephen Hailes. Inp: mobility, multi-homing, localised addressing and security through naming. *Telecommunication Systems*, 42(3):273–291, dec 2009.
- [Anaa] Devices knowledge center. Internet.

- [Anab] Devices knowledge center. Internet.
- [Atk95] R. Atkinson. Security Architecture for the Internet Protocol. RFC 1825 (Proposed Standard), August 1995. Obsoleted by RFC 2401.
- [AW02] I.F. Akyildiz and Wenyue Wang. A dynamic location management scheme for next-generation multitier pcs systems. *Wireless Communications, IEEE Transactions on*, 1(1):178–189, 2002.
- [BCF⁺08] S. Brim, N. Chiappa, D. Farinacci, V. Fuller, D. Lewis, and D. Meyer. Lisp-cons: A content distribution overlay network service for lisp. Internet Draft, April 2008.
- [BGT02] T. Bu, Lixin Gao, and D. Towsley. On characterizing bgp routing table growth. In *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, volume 3, pages 2185–2189 vol.3, Nov 2002.
- [BLFM05] T. Berners-Lee, R. Fielding, and L. Masinter. Rfc 3986, uniform resource identifier (uri): Generic syntax. Request For Comments (RFC), 2005.
- [BLMM94] T. Berners-Lee, L. Masinter, and M. McCahill. Rfc1738: Uniform resource locators (url). 1994.
- [BLR⁺04a] Hari Balakrishnan, Karthik Lakshminarayanan, Sylvia Ratnasamy, Scott Shenker, Ion Stoica, and Michael Walfish. A layered naming architecture for the internet. In *SIGCOMM '04*, 2004.
- [BLR⁺04b] Hari Balakrishnan, Karthik Lakshminarayanan, Sylvia Ratnasamy, Scott Shenker, Ion Stoica, and Michael Walfish. A layered naming architecture for the internet. In *SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 343–352, New York, NY, USA, 2004. ACM.
- [Cae07] Matthew Chapman Caesar. *Identity-based routing*. PhD thesis, EECS Department, University of California, Berkeley, Sep 2007.

- [CAF10] B. Carpenter, R. Atkinson, and H. Flinck. Renumbering Still Needs Work. RFC 5887 (Informational), May 2010.
- [CBFP03] David Clark, Robert Braden, Aaron Falk, and Venkata Pingali. Fara: reorganizing the addressing architecture. In *FDNA '03: Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture*, pages 313–321, New York, NY, USA, 2003. ACM.
- [CCK⁺06] Matthew Caesar, Tyson Condie, Jayanthkumar Kannan, Karthik Lakshminarayanan, and Ion Stoica. Roff: routing on flat labels. *SIGCOMM Comput. Commun. Rev.*, 36(4):363–374, August 2006.
- [CGK⁺02] A.T. Campbell, J. Gomez, Sanghyo Kim, Chieh-Yih Wan, Z.R. Turanyi, and A.G. Valko. Comparison of ip micromobility protocols. *Wireless Communications, IEEE*, 9(1):72–82, Feb 2002.
- [cis] Cisco visual networking index: Global mobile data traffic forecast update, 2013–2018. Internet.
- [Day08] John Day. *Patterns in Network Architecture: A Return to Fundamentals*. Prentice Hall, December 2008.
- [DH95] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 1883 (Proposed Standard), December 1995. Obsoleted by RFC 2460.
- [DH98] S. Deering and R. Hinden. *RFC 2460 Internet Protocol, Version 6 (IPv6) Specification*, 1998.
- [DMM08a] John Day, Ibrahim Matta, and Karim Mattar. Networking is ipc: A guiding principle to a better internet. In *Proceedings of the 2008 ACM CoNEXT Conference, CoNEXT '08*, pages 67:1–67:6, New York, NY, USA, 2008. ACM.
- [DMM08b] John Day, Ibrahim Matta, and Karim Mattar. Networking is ipc: a guiding principle to a better internet. In Arturo Azcorra, Gustavo de Veciana, Keith W. Ross, and Leandros Tassiulas, editors, *CoNEXT*, page 67. ACM, 2008.

- [EF09] Chip Elliott and Aaron Falk. An update on the geni project. *SIGCOMM Comput. Commun. Rev.*, 39(3):28–34, June 2009.
- [FFM⁺13] D. Farinacci, V. Fuller, D. Meyer, D. Lewis, and Cisco Systems. Cisco systems, 2013.
- [FFML10] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis. Locator/id separation protocol (lisp). draft-ietf-lisp-07, April 25 2010.
- [FFML11] V. Fuller, D. Farinacci, D. Meyer, and D. Lewis. Lisp alternative topology (lisp+alt), June 2011.
- [FKK96] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The ssl protocol — version 3.0. Internet Draft, Transport Layer Security Working Group, November 1996.
- [GA92] P. Gross and P. Almquist. IESG Deliberations on Routing and Addressing. RFC 1380 (Informational), November 1992.
- [Hai00] T. Hain. Architectural Implications of NAT. RFC 2993 (Informational), November 2000.
- [HLFT94] S. Hanks, T. Li, D. Farinacci, and P. Traina. Generic Routing Encapsulation (GRE). RFC 1701 (Informational), October 1994.
- [HS01] M. Holdrege and P. Srisuresh. Protocol Complications with the IP Network Address Translator. RFC 3027 (Informational), January 2001.
- [Hus01] G. Huston. Commentary on Inter-Domain Routing in the Internet. RFC 3221 (Informational), December 2001.
- [IL10] Luigi Iannone and Tapio Levä. Modeling the economics of loc/id split for the future internet. In *IEEE Signal Process. Lett.*'10, pages 11–20, 2010.
- [Int81] Internet Engineering Task Force. *RFC 791 Internet Protocol - DARPA Internet Programm, Protocol Specification*, September 1981.
- [ITU] General requirements for id/locator separation in ngn.

- [Jai06a] R. Jain. Internet 3.0: Ten problems with current internet architecture and solutions for the next generation. In *Military Communications Conference, 2006. MILCOM 2006. IEEE*, pages 1–9, 2006.
- [Jai06b] Raj Jain. Internet 3.0: Ten problems with current internet architecture and solutions for the next generation. In *Military Communications Conference, 2006. MILCOM 2006. IEEE*, pages 1–9, 23-25 2006.
- [JCAC⁺10] Loránd Jakab, Albert Cabellos-Aparicio, Florin Coras, Damien Saucez, and Olivier Bonaventure. Lisp-tree: a dns hierarchy to support the lisp mapping system. *IEEE J.Sel. A. Commun.*, 28(8):1332–1343, October 2010.
- [JPA04] D. Johnson, C. Perkins, and J. Arkko. *Mobility Support in IPv6*. IETF, June 2004. [Standards Track RFC 3775].
- [JSBM02] Jaeyeon Jung, Emil Sit, Hari Balakrishnan, and Robert Morris. Dns performance and the effectiveness of caching. *IEEE/ACM Trans. Netw.*, 10(5):589–603, 2002.
- [KIF11] Juhoon Kim, Luigi Iannone, and Anja Feldmann. A deep dive into the lisp cache and what isps should know about it. In *Proceedings of the 10th international IFIP TC 6 conference on Networking - Volume Part I, NETWORKING'11*, pages 367–378, Berlin, Heidelberg, 2011. Springer-Verlag.
- [KJ05] Kyandoghere Kyamakya and Klaus Jobmann. Location management in cellular networks: classification of the most important paradigms, realistic Simulation framework, and relative performance analysis. *IEEE Transactions on Vehicular Technology*, 54:687–708, 2005.
- [LC10] Jong-Hyouk Lee and Tai-Myoung Chung. How much do we gain by introducing route optimization in proxy mobile ipv6 networks? *Annales des Télécommunications*, 65(5-6):233–246, 2010.
- [LE08] J. Laganier and L. Eggert. Host Identity Protocol (HIP) Rendezvous Extension. RFC 5204 (Experimental), April 2008.

- [LE11] T. Li and Ed. Design Goals for Scalable Internet Routing. RFC 6227 (Proposed Standard), May 2011.
- [LKE08] J. Laganier, T. Koponen, and L. Eggert. Host Identity Protocol (HIP) Registration Extension. RFC 5203 (Experimental), April 2008.
- [LPJX08] Burness L., Eardley P., Sheng Jiang, and Xiaohu Xu. A pragmatic comparison of locator id split solutions for routing system scalability. In *Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on*, pages 1024–1028, Aug 2008.
- [LPL⁺10] Hong Li, Chenghui Peng, Bojie Li, Yuhua Chen, Wei Zhang, Jianjun Wu, and Hua Huang. User id routing architecture. *Vehicular Technology Magazine, IEEE*, 5(1):62–69, 2010.
- [LWW11] Ke Li, Sheng Wang, and Xiong Wang. Edge router selection and traffic engineering in lisp-capable networks. *Communications and Networks, Journal of*, 13(6):612–620, Dec 2011.
- [MN06] R. Moskowitz and P. Nikander. Host identity protocol (hip) architecture. RFC 4423, May 2006.
- [MNJH08] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. RFC 5201 (Experimental), April 2008.
- [Moc83] P.V. Mockapetris. Domain names: Implementation specification. RFC 883, November 1983. Obsoleted by RFCs 1034, 1035, updated by RFC 973.
- [Moc87a] P. Mockapetris. Domain names — concepts and facilities. Internet RFC 1034, November 1987.
- [Moc87b] P. Mockapetris. Domain names — implementation and specification. Internet RFC 1035, November 1987.
- [MZF07] D. Meyer, L. Zhang, and K. Fall. Report from the iab workshop on routing and addressing. RFC 4984 (Informational), September 2007.

- [NAO04] P. Nikander, J. Arkko, and B. Ohlman. Host identity indirection infrastructure (hi3). In *The Second Swedish National Computer Networking Workshop*, November 2004.
- [NB09] E. Nordmark and M. Bagnulo. Shim6: Level 3 Multihoming Shim Protocol for IPv6. RFC 5533 (Proposed Standard), June 2009.
- [NHVA08] P. Nikander, T. Henderson, C. Vogt, and J. Arkko. End-Host Mobility and Multihoming with the Host Identity Protocol. RFC 5206 (Experimental), April 2008.
- [Nik07] P. Nikander. Evolution of networking: Current problems and future directions. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, pages 518–518, 2007.
- [NJPC⁺13] Alberto Rodríguez Natal, Loránd Jakab, Marc Portoles-Comeras, Vina Ermagan, Preethi Natarajan, Fabio Maino, David Meyer, and Albert Cabellos-Aparicio. Lisp-mn: Mobile networking through lisp. *Wireless Personal Communications*, 70(1):253–266, 2013.
- [O’D96] Mike O’Dell. 8+8 - an alternate addressing architecture for ipv6, 10 1996.
- [Per02] Charles Perkins. *IP Mobility Support for IPv4*. IETF, August 2002. [Standards Track RFC 3344].
- [PJPB08a] Subarthi Paul, Raj Jain, Jianli Pan, and Mic Bowman. A vision of the next generation internet: A policy oriented perspective. In Erol Gelenbe, Samson Abramsky, and Vladimiro Sassone, editors, *BCS Int. Acad. Conf.*, pages 1–14. British Computer Society, 2008.
- [PJPB08b] Subharthi Paul, Raj Jain, Jianli Pan, and Mic Bowman. A vision of the next generation internet: A policy oriented perspective. In Erol Gelenbe, Samson Abramsky, and Vladimiro Sassone, editors, *BCS Int. Acad. Conf.*, pages 1–14. British Computer Society, 2008.

- [PJPSI10] Jianli Pan, Raj Jain, Subharthi Paul, and Chakchai So-In. Milsa: A new evolutionary architecture for scalability, mobility, and multihoming in the future internet. *IEEE Journal on Selected Areas in Communications*, 28(8):1344–1362, 2010.
- [PKCP09] Sangheon Pack, Taekyoung Kwon, Yanghee Choi, and Eun-Kyoung Paik. An adaptive network mobility support protocol in hierarchical mobile ipv6 networks. *Vehicular Technology, IEEE Transactions on*, 58(7):3627–3639, 2009.
- [PMTZ06] Vasileios Pappas, D. Massey, A. Terzis, and Lixia Zhang. A comparative study of the dns design with dht-based alternatives. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–13, April 2006.
- [Pos80] J. Postel. DoD standard Transmission Control Protocol. RFC 761, January 1980.
- [PPJ] Subharthi Paul, Jianli Pan, and Raj Jain. A survey of naming systems: Classification and analysis of the current schemes using a new naming reference model.
- [PPJ11a] J. Pan, S. Paul, and R. Jain. A survey of the research on future internet architectures. *Communications Magazine, IEEE*, 49(7):26–36, 2011.
- [PPJ11b] Subharthi Paul, Jianli Pan, and Raj Jain. Architectures for the future networks and the next generation internet: A survey. *Comput. Commun.*, 34(1):2–42, January 2011.
- [PPJB08] Jianli Pan, Subharthi Paul, Raj Jain, and Mic Bowman. Milsa: A mobility and multihoming supporting identifier locator split architecture for naming in the next generation internet. In *GLOBECOM*, pages 2264–2269. IEEE, 2008.
- [RA12] SN Bhatti RJ Atkinson. Identifier-locator network protocol (ilnp) architectural description. RFC 6740, November 2012.
- [RL94] Y. Rekhter and T. Li. A Border Gateway Protocol 4 (BGP-4). RFC 1654 (Proposed Standard), July 1994. Obsoleted by RFC 1771.

- [RMKdG94] Y. Rekhter, B. Moskowitz, D. Karrenberg, and G. de Groot. Address Allocation for Private Internets. RFC 1597 (Informational), March 1994. Obsoleted by RFC 1918.
- [RS04] Venugopalan Ramasubramanian and Emin Gün Sirer. The design and implementation of a next generation name service for the internet. *SIGCOMM Comput. Commun. Rev.*, 34(4):331–342, 2004.
- [Sal78] Jerome H. Saltzer. Naming and binding of objects. In *Operating Systems, An Advanced Course*, pages 99–208, London, UK, 1978. Springer-Verlag.
- [Sal93] J. Saltzer. Rfc 1498: On the naming and binding of network destinations, August 1993. Status: INFORMATIONAL.
- [SAZ⁺04] Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana. Internet indirection infrastructure. *IEEE/ACM Trans. Netw.*, 12(2):205–218, 2004.
- [SE01] P. Srisuresh and K. Egevang. Traditional IP Network Address Translator (Traditional NAT). RFC 3022 (Informational), January 2001.
- [SGF⁺10] Ankit Singla, P. Brighten Godfrey, Kevin Fall, Gianluca Iannaccone, and Sylvia Ratnasamy. Scalable routing on flat names. In *Proceedings of the 6th International Conference, Co-NEXT '10*, pages 20:1–20:12, New York, NY, USA, 2010. ACM.
- [SIBF12] D. Saucez, L. Iannone, O. Bonaventure, and D. Farinacci. Designing a deployable internet: The locator/identifier separation protocol. *IEEE Internet Computing*, 16(6):14–21, 2012.
- [SJR09] Paul Subharthi, Pan Jianli, and Jain Raj. Architectures for the future networks and the next generation internet: A survey. Technical report, WUSTL, October 2 2009.
- [SS04] Jun-Zhao Sun and Jaakko Sauvola. Mobile ip applicability: When do we really need it? In *Proceedings of the 2004 International Conference on Parallel Processing Workshops, ICPPW*

- '04, pages 116–123, Washington, DC, USA, 2004. IEEE Computer Society.
- [Ste07] R. Stewart. Stream Control Transmission Protocol. RFC 4960 (Proposed Standard), September 2007.
- [TMS12] Hasan Tuncer, Sumita Mishra, and Nirmala Shenoy. Review: A survey of identity and handoff management approaches for the future internet. *Comput. Commun.*, 36(1):63–79, December 2012.
- [WBS04] Michael Walfish, Hari Balakrishnan, and Scott Shenker. Untangling the web from dns. In *NSDI'04: Proceedings of the 1st conference on Symposium on Networked Systems Design and Implementation*, pages 17–17, Berkeley, CA, USA, 2004. USENIX Association.
- [WTL07] Yi Wu, J. Tuononen, and M. Latvala. Performance analysis of dns with ttl value 0 as location repository in mobile internet. In *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, pages 3250–3255, March 2007.
- [X1111] Distributed hash table (dht). In David A. Padua, editor, *Encyclopedia of Parallel Computing*, page 573. Springer, 2011.
- [XA02] Jiang Xie and I.F. Akyildiz. A novel distributed dynamic location management scheme for minimizing signaling costs in mobile ip. *Mobile Computing, IEEE Transactions on*, 1(3):163–175, Jul 2002.
- [xin09] Content delivery networks. In Ling Liu and M. Tamer Ozsu, editors, *Encyclopedia of Database Systems*, page 463. Springer US, 2009.
- [YJ12] Taewan You and Heeyoung Jung. A qualitative analysis of mofi, lisp, and hip. In *ICT Convergence (ICTC), 2012 International Conference on*, pages 772–774, Oct 2012.
- [ZPT+11] Theodore Zahariadis, Dimitri Papadimitriou, Hannes Tschofenig, Stephan Haller, Petros Daras, George D. Stamoulis, and Manfred

Hauswirth. The future internet. chapter Towards a future internet architecture, pages 7–18. Springer-Verlag, Berlin, Heidelberg, 2011.

Résumé

Le nommage est un élément fondamental à l'évolution de l'Internet. Les nouveaux scénarios de niveau hôte et utilisateur contraignent le système de nommage initial à deux niveaux de l'Internet. Celui-ci est alors appelé à évoluer pour répondre à ces nouvelles exigences. Plus spécifiquement, une attention particulière devrait être accordée à la communication entre les utilisateurs et au support des multi-terminaux dans la conception des futurs systèmes de nommage.

Cette thèse s'intéresse à l'étude du problème de nommage dans l'Internet du futur en tenant en compte les contraintes à la fois de niveau hôte et de niveau utilisateur. Le concept de séparation Identifiant / Localisateur a été largement approuvé comme une solution pour les problèmes actuels de nommage. Pour cette raison, nous nous concentrons d'abord sur l'étude de plusieurs solutions implémentant cette approche. Nous fournissons une vue d'ensemble qualitative et une analyse quantitative des coûts des approches proposées. En se basant sur les résultats obtenus, nous soulignons que ces solutions sont centrées sur les hôtes et nous montrons qu'elles sont inadéquates avec les exigences supplémentaires de niveau utilisateur.

Afin de compléter les travaux de recherche déjà existants, nous présentons dans cette thèse une nouvelle architecture appelée SANA (Service-Aware Naming Architecture). Notre solution est basée sur trois points clés. Tout d'abord, nous remettons en question le concept de séparation Identifiant/Localisateur en promouvant l'identification des utilisateurs et des services. Ensuite, nous fournissons un support multi-terminaux transparent pour le réseau. Et enfin, nous assurons un transfert de session transparent au réseau et aux applications entre des terminaux du même utilisateur. Les évaluations de SANA montrent que notre solution offre des performances comparables aux celles des approches de séparation Identifiant/Localisateur. SANA dépasse aussi d'autres solutions de nommage de niveau utilisateur en termes de coût de message de signalisation et de la taille des systèmes de résolution. En couvrant ces aspects, SANA peut être considéré comme un candidat potentiel pour les futurs systèmes de nommage en prenant en compte le niveau utilisateur.

Mots-clés : Nommage, Adressage, Mobilité, Séparation Identifiant/Localisateur, Internet du futur

Abstract

Naming is a fundamental element to evolve the current Internet into the next stage. The new host-level and user-level scenarios of the future networks introduce great pressure towards the initial two-level naming system of the Internet, which is requested to evolve in order to answer these new requirements. More specifically, special attention should be paid to person-to-person communications and multi-device support in future naming schemes' design.

This thesis concentrates on the study of the naming research trends considering to improve future Internet's support to both host-level and user-level requirements. The Identifier/Locator split concept has been widely approved as a crucial solution for current Internet's naming problems. This is why, we first concentrate our work on studying several Identifier/Locator split solutions. We provide a qualitative overview and a quantitative cost analysis of the proposed approaches. Based on the results that we have obtained, we emphasize the host-centric character of these solutions and we show that they have shortages regarding additional user-level requirements.

In order to complement previous research work in the naming area, we present in this thesis a new naming proposal that we call Service-Aware Naming Architecture (SANA). Our solution is built around three key points. First, we challenge the traditional Identifier/Locator split paradigm by getting rid of terminals' identifiers and promoting users and services identification. Second, we provide a transparent multi-device support to the network. And finally, we make user's session switching between different terminals agnostic to applications and networks. SANA cost analysis results show that our solution has comparative performances with traditional Identifier/Locator split solutions. It also outperforms other user-level naming solutions in terms of signaling cost and size of resolution systems. By covering these aspects intrinsically, we believe that SANA can be considered a significant candidate for future naming systems with respect to user-level requirements.

Keywords : Naming, Addressing, Mobility, Identifier/Locator split, Future Internet



n° d'ordre : 2015telb0351

Télécom Bretagne

Technopôle Brest-Iroise - CS 83818 - 29238 Brest Cedex 3

Tél : + 33(0) 29 00 11 11 - Fax : + 33(0) 29 00 10 00