Computer Networks 60 (2014) 13–33

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A survey and taxonomy of ID/Locator Split Architectures

W. Ramirez *, X. Masip-Bruin, M. Yannuzzi, R. Serral-Gracia, A. Martinez, M.S. Siddiqui

Advanced Network Architectures Lab (CRAAX), Technical University of Catalonia (UPC), 08800 Vilanova i la Geltú, Spain

ARTICLE INFO

Article history:
Received 3 June 2013
Received in revised form 25 October 2013
Accepted 8 December 2013
Available online 12 December 2013

Keywords:
ID/LOC separation
Internet addressing
Internet architecture
Future Internet

ABSTRACT

The IP-based addressing scheme currently supporting the whole routing architecture embeds some well-known limitations that may significantly hinder the deployment of new applications and services on the Internet. Indeed, it is widely accepted that the unstoppable growth of Internet users is producing two well-known problems: (1) depletion of addresses, motivated by a design limitation of the currently deployed addressing scheme, and (2) the semantic overload of addresses. The main negative consequences of these problems may be summarized as: (i) exacerbating the geometrical growth of the routing tables, and (ii) affecting other network features, such as traffic engineering and mobility, in terms of resilience and disruption tolerant communications.

The relevant consequences that addressing brings to the overall network operation is pushing the networking community to study and propose new addressing architectures that may limit or even remove the negative effects (affecting network performance) stemmed from the currently deployed addressing architecture. To this end, researchers working on this area must have a perfect understanding of the weaknesses and limitations coming up from the nowadays architecture as well as a comprehensive knowledge of the alternatives proposed so far along with the most appealing research trends. Aligned to this scenario, this paper comes up with the aim of assisting the reader to both: (i) get insights about the most prominent limitations of the currently deployed addressing architecture, and (ii) survey the existing proposals based on ID/Locator Split Architectures (ILSAs) including an analysis of pros and cons, as well as a taxonomy aiming at formulating a design space for evaluating and designing existing and future ILSAs.

1. Introduction and motivation

For many years, Internet has been constantly evolving in a wide set of areas e.g., technical, social, etc., what has been demanding a continuous effort from the scientific community to face the technological challenges linked to this unstoppable evolution. The socialization of Internet as well as the rapid dissemination of new user-friendly/appealing services and applications are both fueling network connectivity to become a basic need for users. Thus, it is widely shared among the scientific community that the near future for Internet will draw a network scenario enriched by network features (such as, End to End security, Resilient Communications, Mobility, Traffic Engineering and Multi-Homing), with a huge volume of heterogeneous devices all demanding Internet connectivity anywhere, anyhow and at anytime. It is evident that network protocols supporting the current Internet were not designed to provide such new features, hence the expected evolution towards the Future Internet (FI) must undoubtedly overcome the limitations inherent to the currently deployed network protocols.

Focusing on the addressing strategy, particular research efforts must be devoted to study the limitations caused by the existing IP-based addressing scheme, specifically in reference to two main problems: the depletion of

* Corresponding author. Tel.: +34 610192440.
E-mail addresses: wramirez@ac.upc.edu (W. Ramirez), xmasip@ac.upc.edu (X. Masip-Bruin), yannuzzi@ac. upc.edu (M. Yannuzzi), rserral@ac.upc.edu (R. Serral-Gracia), annym@ac.upc.edu (A. Martinez), siddiqui@ac.upc.edu (M.S. Siddiqui).

1389-1286/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.bjp.2013.12.006

addresses, i.e., the availability of the addressing space, and the semantic overload of addresses, i.e., double functionality of an address. The first refers to the fact that the overall size of the IPv4 address space is definitely not enough to cover the current and expected increase in the density of identifiable nodes in Internet (worth noticing that the IPv4 address space has almost reached the end of its lifetime [1,2]). The second, the semantic overload of addresses, refers to the fact that current (IP-based) Internet addresses act as both locator and identifier. Thus, adopting a double functionality clearly imposes a burden on the current routing system, hence affecting several network features (e.g., roaming users or operator portability could be accomplished smoothly if this double functionality is removed). Preliminary attempts with the aim of proposing solutions facing these two problems were centered in two research lines, IPv6 and clean slate architectures.

IPv6 was proposed as an (evolutionary) alternative to cope with the exhaustion of addresses, conceptually supported by enlarging the addressing space. However, as of today, network providers are reluctant to widely deploy IPv6 mainly because of two reasons [3,4]: (1) the expenditure of resources, referring to the fact that the required tasks to migrate from an IPv4 to an IPv6 core require a considerable amount of time, and represent an operational expenditure not only in terms of firmware updates of network equipment but also on IPv6 training for the operational personnel; (2) the migration process may cause an undesired disruption of the network services. Moreover, while enlarging the addressing space may contribute to solve the depletion of addresses problem, it is clear that this does not have any effect on the semantic overload problem.

Opposite to the evolutionary line of work, disruptive proposals are not thought up as extensions or modifications of current addressing protocols. Thus, clean slate solutions such as [5], may offer a novel addressing scheme explicitly designed to avoid the double functionality of an address. However, disruptive solutions suffer from the inherent risk associated to deploying new technologies on top of an operational network that, as expected, will never permit to put overall network connectivity at risk.

Therefore, despite the efforts devoted so far, yet additional research efforts must be invested to propose an innovative addressing architecture that might be widely accepted and easily deployed (minimizing operational risks) by network manufacturers and providers.

In this line, a new architectural model has been recently positioned as a reference to fix the semantic overload problem. The underlying idea within this reference model, so-called the ID/Locator Split Architectures (ILSAs), aspires to split the double functionality of an address. Hence, bringing together ILSAs (solves the semantic overload problem) along with a new addressing scheme (solves the depletion of addresses), seems to be a suitable solution for handling the current Internet addressing problems. As an example, the use of ILSAs along with an addressing scheme such as IPv6 could reduce the IP-based addressing limitations, especially in network scenarios requiring multihoming, traffic engineering and mobility [6]. Furthermore, ILSAs can smooth the migration of IPv4 to IPv6, what strongly lowers the barrier operators keep to deploy IPv6 on their IPv4 networks [7].

The main objective of this article is first to introduce the reader to the most prominent limitations and unsolved problems existing in the current Internet addressing scheme, so as the reader can get a comprehensive analysis and a complete picture of the overall context on addressing. Then, the reader is moved to the concept of ILSAs, as an architectural reference model, introducing a taxonomy which gathers the existing ILSA schemes and recent literature about this topic. The paper explicitly describes the most outstanding ILSA schemes, indicating pros and cons, strengths and weaknesses, therefore promoting their use in the FI.

The organization of this paper is as follows. Section 2 describes the shortcomings of the current addressing scheme. Section 3 illustrates the preliminary concepts of ILSAs. Section 4 introduces a taxonomy for ILSAs proposals. Sections 5–7 describe Network based, Host based, and Mapping System schemes respectively. And finally, Section 8 offers our insights and vision of the future of ILSA schemes.

2. The current addressing system: the handicaps

Since the early days of the Internet, IP is being deployed as the main underlying technology supporting routing and addressing strategies on the Internet. Despite some of the well-known weaknesses and limitations inherent to an IP-based addressing scheme, traditionally the scientific community has invested much more efforts in routing, in particular in the inter-domain area than in addressing [8,9]. This research preference has been actively promoting routing on top of addressing even knowing that some predictions about the exhaustion of the IP addressing space are as old as itself [1,2].

It was Geoff Houston in [10], who warned the scientific community about the addressing space reality, when he showed that the IPv4 depletion time would be shorter than the one previously foreseen by many organizations (some of them reaching the year 2030). This assessment generated considerable attention in address-allocation policy circles and fueled new initiatives in the addressing area, such as clean slate addressing architectures [11–15], or proposals dealing with security and convergence speed as well [16–18].

In order to familiarize the reader to the problems caused by the current IP-based addressing scheme, we introduce in the following subsections the effects produced on the overall network performance by the exhaustion of addresses and the semantic overload problems.

2.1. Expansion of the Internet: the depletion of addresses

During many years, Internet grew with the unpretentious objective of providing connectivity, or in other words, endowing users with the capacity to reach any destination. At that time, with network features such as Quality of Service (Quality of Experience), mobility, multihoming, and traffic engineering, out of the picture, an addressing scheme in essence providing such a connectivity facility

was more than enough to cover users and networks expectations. However, in the last years many emerging needs made the simple connectivity model not enough. As an example, we can easily observe how Internet has become one of the most used vehicles for large-scale commerce, where end users are connected through (several) ever smaller and smarter devices with increasing demands on mobility and seamless connectivity round the clock. This emerging scenario, based on an apparently unlimited connectivity demand, poses several challenging problems, some of them motivated by the huge addressing space required to provide such high connectivity demands. Hence, the old Internet architectural model must evolve into what is usually referred to as the Future Internet (FI) [19–21], see Fig. 1.

Unfortunately, the IP-based addressing scheme deployed so far (IPv4) does not support the large address space required by the FI model, mainly due to the limited size of its addressing space. Several work-arounds and extensions have been proposed and deployed to defer the exhaustion of IPv4 addresses, including private address blocks or NAT (Network Address Translator) that unfortunately introduced new problems, such as address space hijacking and difficulty in the deployment of NAT sensitive protocols, for instance, SIP and IPsec.

It was more than fifteen years ago that the next generation Internet Protocol group (IPng) [22–24] started developing IPv6 [25] as a solution for IPv4 address depletion. The proposed 128-bit length IPv6 addresses and its aggregatable nature style were designed to provide an address space larger than the one estimated to meet the expected growth of network elements. Nevertheless, network operators are yet reluctant to adopt IPv6, mainly due to the difficulty of migration tasks, thus keeping the depletion of addresses problem yet unsolved.

2.2. Mobility and resilient communications: double functionality

Mobility and resilience are two key network features that must be granted in the FI architecture proposed in Fig. 1. While in the previous subsection, we described how the expansion of Internet motivated the address depletion problem, this subsection describes how the double functionality embedded in the current IP-based addressing scheme affects on mobile and resilient communications. Just as a reminder, the double functionality refers to the fact that the IP address assigned to a network element stands for both a locator and an identifier, the first locating the network element in the Internet and the latter identifying it.

Mobile communications are indeed affected by the double functionality problem. The following real scenario can better illustrate this statement. Nowadays, users are not statically connected to Internet but rather users are demanding connectivity on the move. This novel mobility context imposes some effects on the connectivity. In particular, in the current routing architecture, when a user moves from one network to another one or changes his/her ISP, (because he/she moved to a new geographic location or he/she subscribed to a new ISP), his/her assigned IP address also changes. This IP address modification

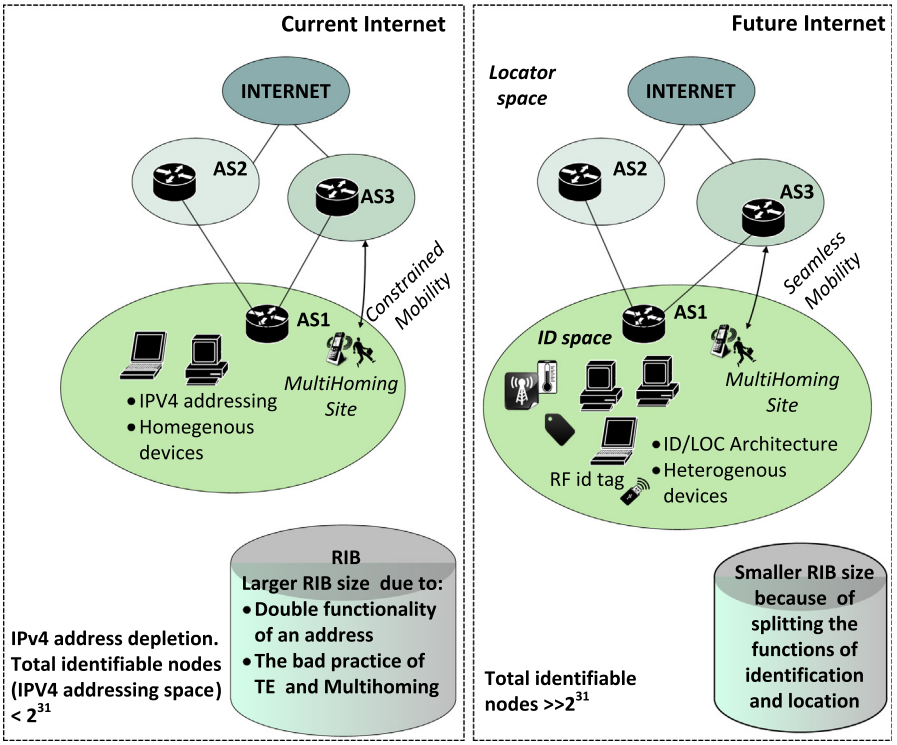


Fig. 1. Evolution of internet.

significantly degrades the communications quality or, even worse, causes a disruption of all established connections that are bound to this IP address. Notice however that, in the first case, the user only changes its location but its identity is certainly the same. Hence, while changes on the user location should be only reported to the routing layer, nowadays represent a change in the overall IP address. It is the routing (network) layer that should be aware of any change in a user's location. Even though there are protocols, such as Mobile IP that enable users mobility in a network, these are only a work-around that do not solve the root-cause of the addressing problems, i.e., the double functionality problem.

Resilient communications are also affected by the double functionality of the IP addresses. Let's assume the case of a data center in which a 1:1 protection is used, therefore having a set of primary and backup servers in different geographic locations. In the case a failure pops up in a primary server, the routing process at the network layer will shift all traffic routed to the failed server towards the backup server. This shifting action has a significant impact on all established connections with the failed server, potentially causing connections disruption.

Moreover, in today's routing architecture it is very hard to use an address to identify multiple hosts. For instance, if address x.x.x.x is assigned to node A, in the case there is a failure in node A, the process of reassign the address x.x.x.x to a node B can be troublesome. Protocols such as Hot Standby Router Protocol (HSRP) can provide support for this, but unfortunately these protocols are vendor dependent, i.e., they operate only among nodes from the same vendor [26].

2.3. Increasing network connectivity: the multihoming paradigm

In the previous two subsections we introduced how the semantic overload and the exhaustion of addresses may impact on several key network features. This subsection now, exposes the effects that a widely deployed connectivity paradigm, so-called multihoming, brings to the current addressing architecture.

Multihoming is a common practice nowadays that significantly fuels the geometrical growth of the routing tables. It basically consists in setting up different alternatives to connect a client to the network. In fact, multihoming comes up as an essential requirement for network administrators mainly due to the two following characteristics: (1) it endows a network with fault tolerant capabilities, and (2) it enables load balancing. These two patent benefits together with the fall of the cost of Internet connections have highly encouraged network administrators to offer and support multihoming.

But, how does a network manage multidomain? To achieve multihoming, a site (autonomous system) acquires a provider independent (PI) or a provider aggregatable (PA) prefix from its providers. It then announces them through all of its providers. PA and PI prefixes are blocks of IP addresses assigned by a Regional Internet Registry (an organization that manages the assignment and registration of IP addresses and AS numbers within a particular region of the world) to a site. The difference between them is that unlike PI prefixes, the PA-prefixes assigned to a site cannot be reused if a site changes its Internet provider.

A multihoming site using PI address space allocates its prefixes in the forwarding and routing tables of each of its providers. Therefore, PI prefixes are not aggregated. For PA prefixes, the Internet provider of a site could aggregate the customer (site) advertisement into a shorter prefix when advertising the prefix to other customers or peers. In the practice of multihoming an ISP has to advertise more specific (less aggregated) IP routing prefix to the Internet and rely on the traditional and problematic longest-prefix match route selection algorithm of BGP [8].

It has been shown in [27] that multihoming strongly contributed to grow the routing table size, this effect is illustrated in the network scenario shown in Fig. 2, where the autonomous system AS1 decides to advertise its prefix

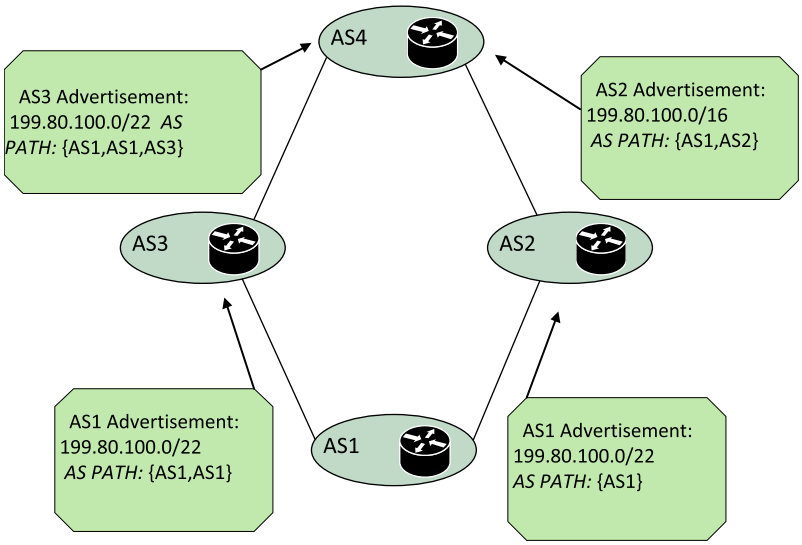


Fig. 2. Multihoming scenario.

199.80.100.0/22 to AS2 and AS3 with the purpose of achieving traffic balancing and fault tolerance capabilities. To this end, AS1 prepends its own AS number to the advertisements send to AS3 (this is done to affect the preference selection of a route on the upstream ASes). Then AS3 advertises the prefix 199.80.100.0/22 to AS4, and AS2 aggregates the prefix 199.80.100.0/22 and forwards the prefix 199.80.100.0/16. This occurs because AS1 advertised by mistake a prefix that belongs to AS2, therefore, AS2 is the ISP of AS1, opposed to AS3 that is just a peer of AS1. As a consequence, AS4 will receive two routes to reach the same destination, hence, having duplicate entries on its routing table.

3. ILSAs: a hope for the current addressing architecture

The concept of ID/Locator Split Architectures (ILSAs) recently came up as a reference model aiming at solving the existing limitations of the current addressing architecture (previously described in Section 2). The ID/LOC concept, first introduced by Chiappa [6], consists in splitting the double functionality of an address, namely location and identification. To this end, the network functions responsible for users' location and identification make use of locators (LOC) and identifiers (ID) respectively for their operation. This novel addressing paradigm has an immediate translation to the network layered model. Thus, the application layer is bound to identifiers, and the network layer is bound to locators.

The main novelty introduced by ILSA schemes regarding the current IP-based addressing architecture is the definition of a separate identifier to differentiate a specific object among a collection of objects. The identifier may be assigned to either a physical object, e.g., computers, mobiles nodes, routers, or a virtual object, e.g., a network group. In fact, while in the current addressing architecture a particular object may have different IP addresses depending on their ISP or geographic location, in an ILSA scheme a unique identifier is assigned to an object regardless its specific location. This is possible because an identifier per se, does not provide any information regarding the location of the object and cannot an object location cannot be inferred from it either [28]. Hence, this novel addressing paradigm is requiring the investment of additional research efforts to overcome the challenges that come up when designing an ILSA scheme. A primary split of these challenges may bring two design areas, the identifier and the locator.

On the one hand, several design issues directly affecting the performance of an ILSA scheme, must be considered when designing an ID scheme. We put our attention to two key parameters, the ID lifetime, and the ID format, that must be carefully handled:

- The lifetime parameter [29] affects the volume of signaling messages necessary for accurately updating the mapping tables (i.e., the information related to the mapping between an ID and a locator). Thus, for example, the shorter the lifetime the greater the accuracy of the mapping information, but the larger the number of signaling messages as well.
- The format of an identifier can be either flat (primitive), or partitioned (descriptive) [30]. A flat identifier (such as UUIDs Universally Unique Identifiers [31]) does not have a semantic structure and hence no information can be inferred from an object only by looking at its ID. A partitioned identifier (such as URLs [32]) instead, does have a semantic structure, what makes partitioned identifiers user-friendly, i.e., they can be easily handled by human users, what would be highly desirable.

On the other hand, a locator could be defined as a label attached to an object providing information about its location. A simple analogy can be made with the postal address of a person. A person will always have the same identity but may have several postal addresses over a period of time, i.e., when his/her location changes. A basic guideline for designing a locator scheme is constrained to both a locator should somehow reflect the network topology and should also support topological aggregation. These two characteristics notably facilitate the routing system operations because if locators are topology dependent, i.e., their assignment and format depend on geographic locations, the routing decisions may be taken from the information provided by a locator (this is not the case in the current addressing scheme).

Whether an addressing scheme supporting topological aggregation and somehow reflecting the network topology, might the desired the performance of the current routing system can be optimized, but only in the case that the routing system does not employ IP-based locators (IP addresses) [33].

Thus far the main actions to be considered when designing identifiers and locators have been pointed out. However, there is a relevant matter referred to their interaction demanding attention as well. In fact, since a locator and an identifier are both needed to address a single object in the network, an ILSA scheme must also include an additional component, responsible for the ID/Locator mapping and vice versa, so called the Mapping System. As it is described later in Section 7, there are different alternatives to implement a Mapping System, each embedding pros and cons, hence directly impacting on the overall performance of an ILSA scheme.

Therefore, the Mapping System, the locators, and the identifiers are the three basic elements of an ILSA scheme, bringing a solution to overcome most of the problems nowadays present in the current addressing architecture. In order to conceptually illustrate the potential benefit introduced by an ILSA scheme, let's analyze its impact on the three handicaps previously discussed in Section 2.

Any tentative implementation of an ILSA scheme would define a single and unique ID for an object that will keep unaltered as long as the object exists. The addressing strategy defined in IPv6 already solved the exhaustion of addresses problem, so there is no reason to doubt about ILSA, as being even simpler.

Moreover, ILSAs may slow down the address depletion issue, even though the latest seems to be solved by the immense address space of IPv6. However, migrating from IPv6 to IPv4 is a task not pleasant for network providers. An ILSA scheme can provide support to the migration process between addressing schemes, see Fig. 3. For example,

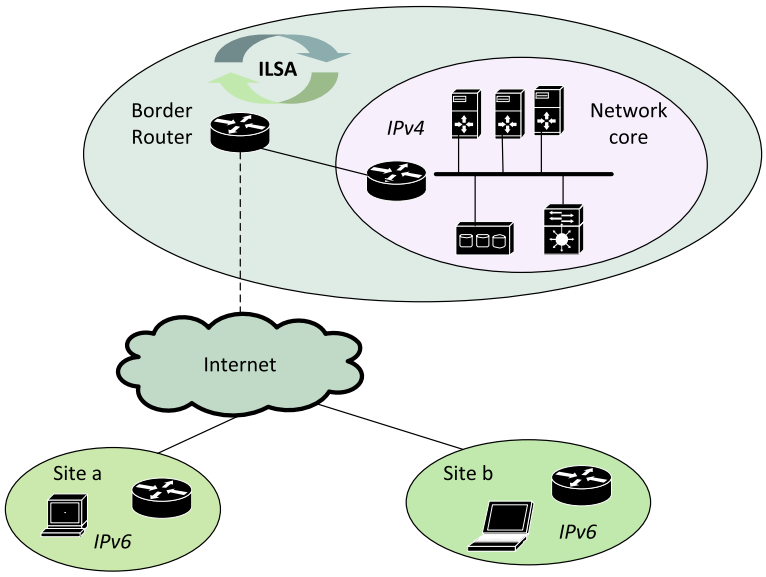


Fig. 3. ILSAs aiming migration from IPv6 to IPv4.

in a network of an ISP, the border routers can have IPv6 addresses assigned while the core routers remain untouched (IPv4). An ILSA solution maps the IPv6 to IPv4 addresses and vice versa, this is a reduction of time and tasks that reflects in OpEx and CapEx. At present, the interoperation between IPv4 and IPv6 using ILSAs is a solution that is already being offered by network-vendors [7].

Let's now consider the "mobility scenario" shown in Fig. 4a, where an ILSA scheme boosts up network features such as mobility. It can be easily observed that, the user device (the object) keeps its same ID even in the case it changes its location site (ISP provider), without impacting on any already established communication (as described in Section 2.2). Furthermore, providers do not have to reassign new IDs to new users, keeping in some cases the hosts configuration untouched.

A highly well positioned real use case for mobility, completely detached from user mobility is drawn nowadays in Virtualized Data Centers. Indeed, Virtual Machines (VMs) can be deployed anywhere (supported by real network infrastructure) regardless the address assigned to the network layer, freely moving (migrating) resources across different geographic locations or different racks within a data center. But VMs migration is not the only added value feature getting benefit from a potential ILSA scheme deployment. Nowadays, a failure in the infrastructure of a data center or a cloud model, will severely impact on the live services offered to the users.

Having tolerant disruption communication in an ILSA scenario also holds true when network failures occurred. Let's consider the "resilience scenario" shown in Fig. 4b, in this scenario a 1:1 protection scheme is employed, i.e., there are two Data Centers, the main and the backup, for the purpose of offering fault tolerant services. In the case there is a failure in the main data center, a protection action is triggered for relocating the affected services to the backup Data Center, which consists in mapping the ID "xxx" to a different locator, the locator "z.z.z.z".

The application layer is not aware of any failure in the network layer, and as mentioned before is bound to IDs. In the case of the example shown in Fig. 4b, the application layer is not aware that the network element with the ID "xxx", is now a different node in a different geographic location. It is important to remark that even though the connections are not disrupted, the quality of delay sensitive communications, e.g., VoIP or video streaming, could be degraded [33].

4. Classifying ID/LOC Split Architectures (ILSAs)

Two high level research challenges, the ID/LOC generation and the Mapping System must be faced when designing an ILSA scheme. As for the first challenge, nowadays, several alternatives may already be found in the recent literature differently handling the ID/LOC generation depending on the network segment they operate at. Thus, Fig. 5 depicts the proposed taxonomy for ILSA schemes, showing the ID/LOC generation challenge, for three sets of ILSAs schemes, namely Network based and Host based schemes, and control plane Mapping Systems.

Network based schemes: Operating at the network level, usually on the border routers at the network backbone, no modifications are required on the end-nodes (host level). Examples of Network based schemes are LISP [34], Six/One [35], GSE [36] among others.

Network based ILSA schemes can be further categorized into: (1) Map–Encap schemes, and (2) Address Rewriting schemes. In Map–Encap schemes, a network packet destined to a certain object (packet with an ID as a destination), is encapsulated into a new packet, whose destination will be a locator. This strategy is widely used in many networking aspects and is usually referred to as tunneling in network jargon. Unlike this tunneling approach, Address Rewriting architectures operate similarly to NAT (Network Address Translation), replacing a packet ID by a locator.

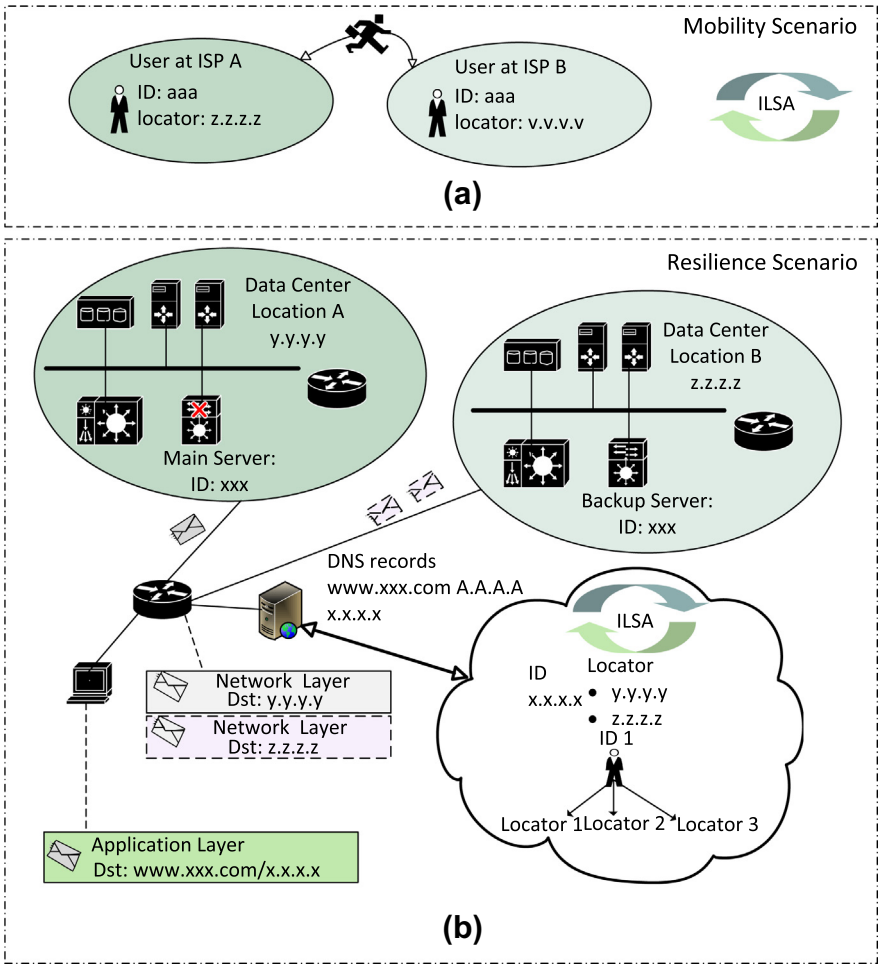


Fig. 4. Mobility and resilience scenario.

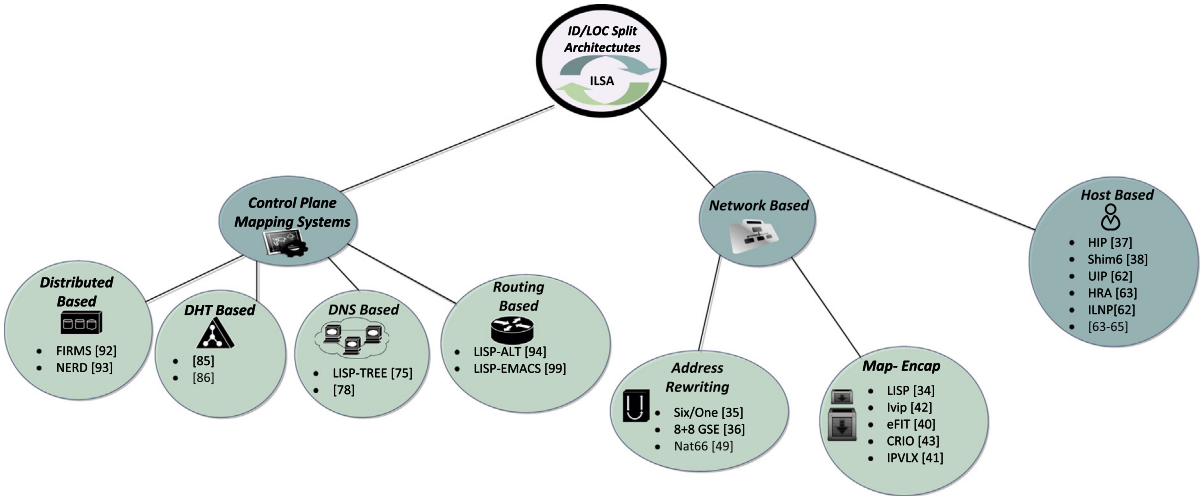


Fig. 5. Taxonomy of ILSA schemes.

Host based ILSA schemes: Operating at the host level, specifically at the end-nodes, no modifications are required at the network level. A Host based ILSA scheme is a more appealing solution than a Network based scheme for network operators since cost investment is not demanded on the network. However, this solution drives software providers to update their products to meet specific requirements of a Host based ILSA scenario, what of course does not sound that attractive for them. Examples of Host based schemes are HIP [37] and SHIM6 [38].

There is a conceptual difference between both approaches that deserves to be mentioned. Unlike a Network based ILSA scheme, where the ID/LOC space (an ID/LOC space is a collection of all valid ID/Locators) is fixed, Host based ILSA deployments are not restricted to use a unique LOC or ID space. This feature could be helpful in some scenarios, for example, a two locators space scenario, may assign one locator space for global routing and the other one for local routing, or a two IDs space scenario, may assign one for the identification of virtual objects (e.g., network groups), and the other one for the identification of physical objects (e.g., computers or mobile nodes). This characteristic increases the addressing granularity.

The second high level challenge refers to the bidirectional mapping between an ID and a Locator ($ID \Longleftrightarrow LOC$). Notice that a different level of mapping is also needed in Host based ILSA schemes between ID spaces (ID_{s1}, ID_{s2}), i.e., an ID could be mapped to another ID which may belong to the same or to a different ID space.

While initial ILSA schemes, such as LISP and Six/One, handled the ID/LOC mapping process over the data plane (Data plane architectures), the current trend on ILSAs design is pushing for control plane architectures, see Fig. 5. In these architectures the mapping process is run by a Mapping System completely decoupled from the data plane, see Fig. 6. The Mapping System is a crucial component on any ILSAs scheme, since it is responsible for the mapping between IDs and locators. Mapping Systems are conceptually supported by different technological approaches, namely DNS, DHT, Distributed Mapping Systems or routing protocols (see Section 7), generating different Mapping System flavors. It can be stated that the chosen flavor of the Mapping System is an important design decision because the Mapping System will adopt most weaknesses and flaws of its parent technology. For example, a Mapping System based on a routing technology such as BGP (Border Gateway Protocol) will inherit most of the yet unsolved problems of BGP.

5. Network based ILSAs

This section deeply describes the two different approaches defined for Network based ILSAs schemes, with

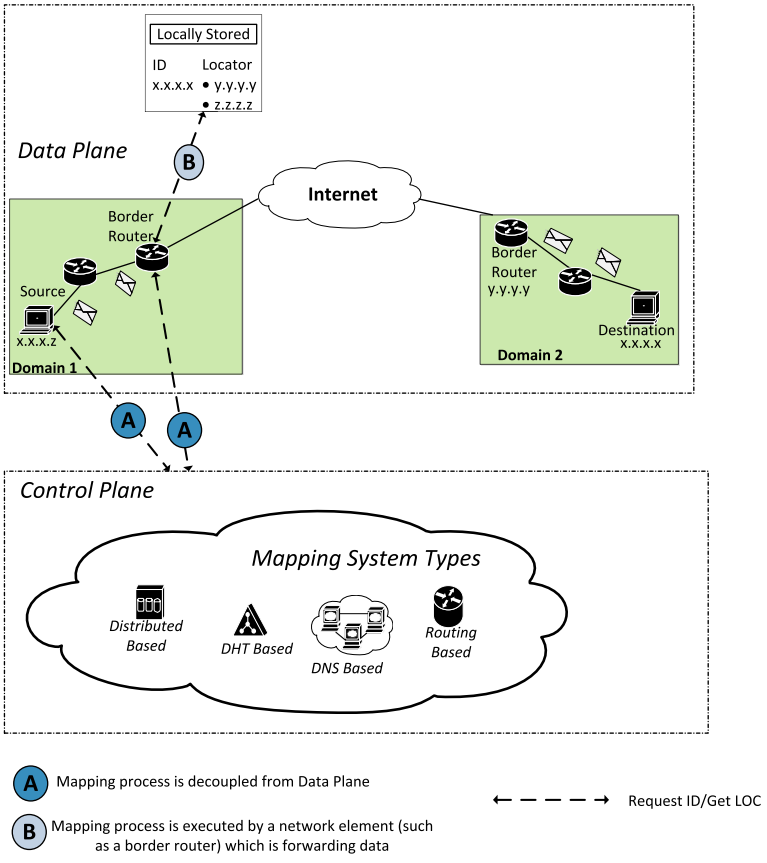


Fig. 6. Decoupling of data and control plane from mapping process.

precise focus on the open issues and weaknesses of each approach.

5.1. Map–Encap schemes

The main concept within any Map–Encap scheme is tunneling techniques. Nowadays several solutions have been already deployed within this approach. The ENCAPS proposal earlier described in [39], inspired several of the current Map–Encap architectures, including: LISP, eFIT [40], IPvLX [41], Internet Vastly Improved Plumbing (Ivip) [42], and CRIO [43]. All these proposals are based on the tunneling concept hence being very similar in the way they operate. Generally speaking, Map–Encap schemes employ at least two address spaces, commonly referred to as EID and RLOC, each used for intra-domain and inter-domain routing respectively, hence clearly showing the fact that depending on its network location a packet may be routed by either the EID or the RLOC.

The general operation for any Map–Encap scheme can be divided into two phases, mapping and encapsulation. The mapping phase is responsible for mapping an EID to an RLOC. To illustrate the operation of Map–Encap schemes let's consider the scenario shown in Fig. 7, in which the node with EID *X.X.X.Z* is sending a packet to the node with EID *X.X.X.X*. This packet is forwarded to the domain border router through its EID. When the packet reaches the border router (that is, the Ingress Tunnel Router or ITR), the mapping phase assigns and a RLOC (*Y.Y.Y.Y*) to the packet. Once the mapping phase is over the packet must be routed and forwarded throughout the network to its final destination. The RLOC may correspond to either a border router in the destination domain or an intermediate router (in a different domain than the destination). In the first case, when the RLOC corresponds to a border router in the destination domain (that is the Egress Tunnel Router or ETR), the ITR encapsulates the received packet into a new packet, that is forwarded using the RLOC as the destination address. This process is applicable on the sender side. Thus, once the packet reaches the ETR, it is decapsulated and then forwarded using the packet's EID, to its final destination.

It is important to remark a RLOC must not necessarily correspond to the address of a border router of the destination domain. For instance, the RLOC of the packet sent by the node with the address *X.X.X.Z*, does not necessarily need to be the address of a border router of Domain 2. A RLOC can also be the address of an intermediate router (a router that is not part of the destination domain). In such a case, the intermediate router changes the destination RLOC for a different one, in order to route the packet to its final destination.

Beyond the basic operations described above, a Map–Encap scheme must also meet several additional design constraints, such as for example:

- The encapsulation phase should be address-agnostic, what definitely enables interoperation among different addressing schemes, e.g., IPv6 and IPv4. In light of this, GRE (Generic Routing Encapsulation) is a protocol that enables encapsulation of a variety of network protocols.
- The mapping phase must include a repository containing the different mapping entries. There are basically two options. On the one hand, the mapping entries can be stored in a mapping table stored locally at the ITR. On the other hand, a mapping entry could be also obtained by querying an external Mapping System. Both options are further elaborated later in this document.

5.1.1. LISP

One of the most prominent Map–Encap ILSA schemes is LISP (Locator Identifier Separation Protocol). LISP, originally proposed by Cisco, is currently being promoted as an open standard at the IETF [34], and is already embedded within the Cisco IOS. Although the main goal of LISP is twofold, simplifying routing operations and improving scalability, other possible use-cases for LISP can be found in [7].

The key elements in LISP architecture are the ITRs, the ETRs and the Mapping System. ITRs and ETRs are responsible for both the encapsulation and decapsulation actions as well as the EID to RLOC lookups. Concerning the mapping phase, LISP only defines the required messages to query the Mapping System, leaving the door open for novel

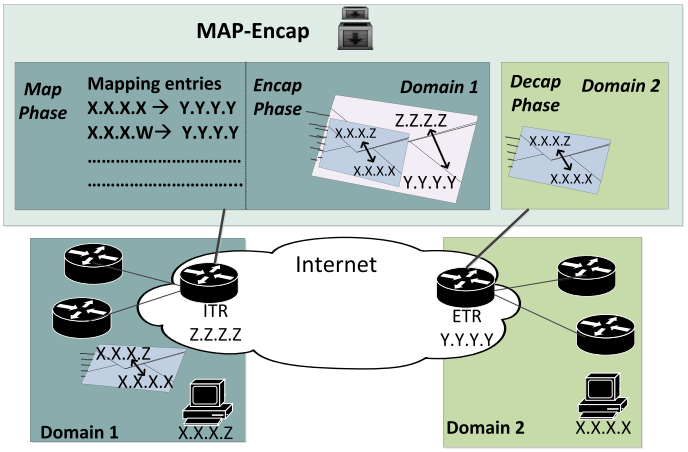


Fig. 7. The operation of Map–Encap schemes.

Mapping System proposals. The set of defined messages to query the Mapping System includes:

- Map-Request: message sent by an ITR to a Mapping System to either get a mapping entry or update a mapping entry information.
- Map-Reply: message sent in respond to a Map-Request message.
- Data Probe: message sent by an ITR to "probe" or request a Map-Reply from the Mapping System.

A challenging problem in the LISP architecture concerns to security, mainly referred to both the authenticity of the LISP messages, and the authentication of the mapping entries. Some approaches came up recently (such as LISP-SEC [44]), with the aim of endowing LISP with security mechanisms for authenticating and authorizing the mapping entries requests (i.e., map-reply messages). Unfortunately, LISP-SEC does not provide any solution for mapping entries authentication yet, hence attacks such as man in the middle may still produce a security problem in LISP.

5.1.2. eFIT

eFIT is a Map–Encap scheme introducing a clear separation between *users network* (host level or end-users) and *providers network* (network level). From the eFIT perspective, users network are "domains", each one interconnected through a "transit wire" (eFIT jargon), consisting in the Internet transit core and a Mapping System. Routers within the transit wire must be only aware about the addresses of other transit routers, hence drastically reducing the size of the routing tables on the border routers.

Regarding the mapping phase operation, two approaches are deployed by eFIT, flooding and distributed services. The former is limited by its scalability as requiring large volume of signaling messages. The latter looks more interesting as relying on third party systems such as a DNS system, or a DHT scheme. However, contrary to LISP there are no specifications regarding the integration of eFIT and a Mapping System.

5.1.3. Other approaches

CRIO, Ivip and IPvLX are also Network based ILSA schemes all implementing tunneling techniques for their operation and all based on the same design principles of LISP or eFIT. However, some differences come up. While the main target for IPvLX and Ivip is to foster IPv6 and IPv4 coexistence, CRIO is a solution thought up to deal with the scalability issue, hence mainly aiming at reducing the size of the Internet routing table.

Pointing to the mapping phase operation, IPvLX and Ivip both define new methods for packet encapsulation; however, CRIO uses standard encapsulation procedures, including GRE or MPLS tunnels (as LISP also does). Moreover, in IPvLX the mapping phase is not limited to any particular implementation of a Mapping System, rather is open for future solutions. It must be noticed that the CRIO architecture does not employ a Mapping System, hence, the mapping entries are stored in the border routers. On the contrary, similar to eFIT, Ivip uses a Distributed Mapping System for executing the mapping phase.

5.1.4. Open issues

There are several issues yet unsolved that must be overcome in order to deploy any Map–Encap ILSA scheme in a real network scenario. In particular, we focus on the three main concerns described next:

- **Increased overhead**: This is an undesirable effect produced by the encapsulation phase. As a consequence of the overhead burden, the number of fragmented IP packets in a network may increase, hence driving to an unpleasant situation for network operators, including issues such as slow-path processing in routers and miss-association of fragments of IP packets during reassembly tasks, all of them potentially degrading the communication quality [45].
- **Seamless mobility support**: All Map–Encap ILSA schemes offer support for nomadic mobility. However, the support of seamless mobility for this type of ILSA scheme is yet an open issue. Nomadic mobility stands for the users ability to change their network connection point. Seamless mobility goes one step further. In fact, inherent to nomadic mobility in which there is the need to restart any users established communication, seamless mobility provides to the users with the capacity to change their network connection point while not disrupting their communication sessions. Although several efforts facing seamless mobility in Map–Encap ILSAs have been recently proposed in the literature, such as [46,47] (based on the interaction between LISP and Mobile IP), there are several issues yet hindering their development, mainly related to the process of updating the mapping table and the encapsulation actions.
- **Resilience/survivability**: Several of the current Map–Encap ILSAs overlook potential failures in the network elements part of the ILSA scheme [48]. Therefore, there are no mechanisms for handling any possible failure affecting a border router (ITR, ETR), or a failure in the Mapping System, which may affect the ILSA scheme operations.
- **Security**: There are initiatives for enabling the authentication and authorization of mapping entries requests in a LISP architecture such as LISP-SEC [44]. However, there are several issues that need to be addressed in order to secure the mapping phase, such as authentication of the requester of a mapping entry.

5.2. Address Rewriting schemes

The principal difference between Map–Encap and Address Rewriting schemes is that Map–Encap schemes use tunneling techniques for their operation, while Address Rewriting schemes use Address Rewriting procedures. In fact, Address Rewriting schemes operate in a similar manner as a NAT process does, see Fig. 8. In Address Rewriting schemes, first, the border routers replace the EID of a packet with a RLOC, and afterwards, the packet is forwarded using this RLOC. When the packet reaches the destination domain the inverse process is executed.

The initial concepts for Address Rewriting schemes were originally proposed by Dave Clark and updated later by Mike O'Dell in their GSE 8 + 8 architecture [36]. The

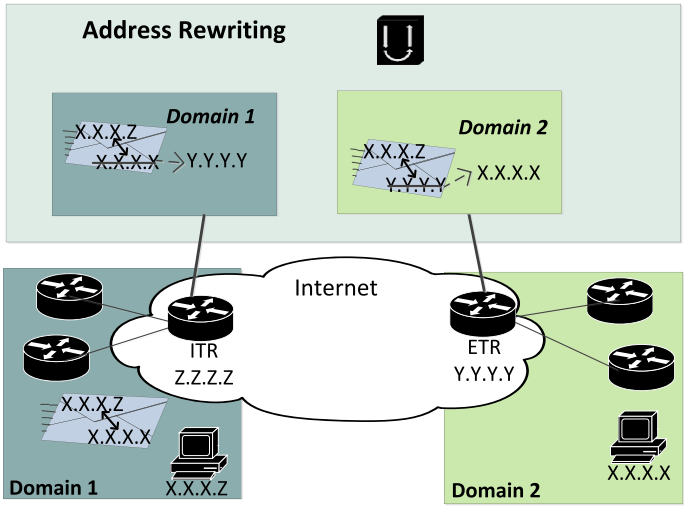


Fig. 8. The operation of Address Rewriting schemes.

foundations for the GSE 8 + 8 architecture boil down to uniformly splitting the 128 bits of an IPv6 address into the routing locator (the top 64 bits, known as routing goop, or GR) and the endpoint identifiers (the lower 64 bits). The GSE 8 + 8 architecture is fueling the development of other Address Rewriting schemes, such as Six/One [35] or NAT66 [49], both briefly introduced next:

5.2.1. Six/One

As any other ILSA scheme, Six/One separates the set of addresses into two blocks, one used for local routing (intra-domain routing) and the other one used for global routing (inter-domain routing), being considered as IDs and locators respectively. Whenever a packet with a destination address belonging to an external domain reaches a border router, the destination address of this packet is translated into a global address and forwarded throughout the transit domains. Afterwards, when the packet reaches the border router of the destination domain, its destination address is once again translated into its original address. This translation feature can be implemented since Six/One adds an extension header into the IP packets including the packet's original source and destination addresses, that is utilized to assist remote Six/One routers (a router with Six/One support) to translate a packet back into its original state. Concerning the Mapping Phase operation, Six/One is compatible with a variety of Mapping Systems. Therefore, no specific Mapping System is proposed in the Six/One architecture.

5.2.2. NAT66

A different Address Rewriting scheme, so-called NAT66, aims at providing address independence at the network edge, standing for the fact that changes in the addresses used for inter-domain routing do not affect the set of addresses used for intra-domain routing. This isolation is definitely aligned to the concept of ID/LOC separation discussed in Section 3, i.e., there is one address set used for hosts identification (ID) and a different address set used for inter-domain routing (locators).

A key element in the operation of NAT66 is the NPTv6 Translator, that is a router featuring the mapping between an IPv6 address prefix to another IPv6 prefix (mapping between IDs and locators). It must be remarked that NAT66 does not use a Mapping System, rather the mechanism employed in the mapping phase is purely algorithmic, i.e., a mapping entry is computed from the information embedded in the network packets.

Unfortunately NPTv6 Translators are exclusively designed for IPv6 addresses operation, which is significantly limiting the NAT66 adaptability to different addressing schemes. For more information regarding NAT66 and its mapping algorithmic the reader is referred to [49].

5.2.3. Open issues

Similarly to Map–Encap schemes, Address Rewriting schemes have several open issues limiting their deployment in real network scenarios such as:

- **Adaptability**: The majority of the Address Rewriting architectures assume IPv6 or IPv4 as the basic addressing scheme, which limits their adaptation.
- **Seamless mobility and renumbering**: The performance of Address Rewriting schemes such as NAT66 may be degraded on mobile scenarios. Also, network features such as address renumbering may be troublesome. However, this is not the case for Six/One, which easily supports address renumbering due to its adaptation to different Mapping Systems.
- **Resilience/survivability**: The reliability of the network elements building the ILSA scheme is a major weakness on Address Rewriting schemes.
- **Security**: Several security issues such as authentication of a mapping entry requester, and validation of a mapping entry, are not covered by most of the Network based ILSA schemes using address rewriting techniques.

Finally, Table 1 shows the performance of both Map–Encap and Address Rewriting schemes regarding several network features.

Table 1
Comparative of Network based schemes.

	Map–Encap	Address Rewriting based
Increased overhead	Med	No affecting
Seamless mobility	Med	Low
Resilience/survivability	High	High
Security	High	Med

6. Host based proposals

Unlike Network based ILSAs, Host based ILSA schemes operate on the user side of the network. As a consequence configurations at the network layer (routers) are not required; rather host's applications and protocols need to be modified. In fact, a middle layer located at hosts acting as a mediator between application/transport layers and network layers is responsible for the mapping between IDs and locators. The middle layer requires that the application layer operates with IDs, while the network layer with locators. In this way there is a perfect separation between IDs and locators, more noticeable in Host based schemes compared to Network based schemes, since the IDs utilized at the application layer are not affected by the locator scheme employed at the network layer. This clear separation inherent to Host based ILSA schemes opens the door to deploy additional network features, such as end-to-end security, resilience/survivability, multihoming, and seamless mobility. However, the modifications required by the end users (the host machines connected to the internet) in order to implement a Host based ILSA scheme may hinder the deployment of such new functionalities, because the modifications needed demand great time effort due to the number of end-users.

6.1. HIP

HIP (Host Identification Protocol) [37], is one of the most relevant Host based ILSA schemes proposed so far. The main objective within HIP is to endow the network with fault tolerant end-to-end communications, end-to-end security, seamless mobility, and multihoming features. As any other Host based ILSA, in HIP the network mechanisms in charge of the location of the hosts employ locators (IP addresses) for their operation, while the network mechanisms responsible for the user identification use identifiers (IDs). The identifiers are 128 bits long, and meet the following two characteristics: are location independent and based on public key cryptography. Therefore, HIP offers support for secure communications and easy address renumbering.

As mentioned above, HIP offer end-to-end communications, which removes several challenges faced by NAT-sensitive applications, such as IP-Security and VoIP [50].

The amendments made to HIP in [51], enable hosts to map a HIP ID to multiple locators. Furthermore, hosts are also able to notify any change regarding their location. As a result, the HIP hosts keep accurate locators information. These last two functionalities provide the hosts with network features such as seamless mobility and multihoming.

Regarding the mapping phase, HIP relies on the DNS system, what facilitates the exploiting of security extensions of the DNS [52] to provide the mapping phase with security features; hence, confirming IDs validation as well as protection against hijacking attacks. Finally, it is worth mentioning that there are many implementations of HIP already developed, such as OpenHIP [53], HIPL [54], infra-HIP [55].

6.2. SHIM6

SHIM6 was mainly designed as a multihoming solution without compromising the scalability of the routing system. To this end, SHIM6 employs a new sublayer, embedded within the IP layer responsible for translating the IP addresses to a constant address, so called the upper layer identifier (ULID), to be used by the upper layers.

But SHIM6 is not just a multihoming solution. SHIM6 also provides security and resilience capabilities. The first, security, relies on cryptographic IDs, that can be categorized as either: Hash-Based Address (HBA) [56] or Cryptographically Generated Address (CGA) [57]. The use of these types of IDs protects the SHIM6 architecture from hijacking attacks. The second, resilience, relies on a protocol named REAP [58] with two clear functions, detecting paths failures in a communication session and determining the new path to be used.

Similarly to HIP, SHIM6 also provides the capacity to endow a single ID with different locators, managed through both the Context Forking and the Context Recovery. A context is defined as the state SHIM6 maintains between identifiers. With Context Forking, a host may fork an existing SHIM6 context into two, what practically means that a network connection can be associated with more than one locator. Thus, whenever a node is unreachable through a determined locator, it may be reached through the other one, hence providing resiliency. Moreover, Context Recovery enables the recovery of a context through any of the two hosts setting the running communication (set in the previous forking step). In other words, Context Recovery enables the recovery of a broken communication by either the server or the client side, what is a helpful feature for servers that are congested by an enormous volume of client connections.

Regarding the mapping phase, the mapping between an ULID and its corresponding locator is performed using a DNS system. This is a major advantage considering the adaptability of SHIM6 in the current Internet architecture, but could also be a drawback considering the shortcomings of a DNS based control plane.

6.3. Other approaches

6.3.1. UIP

UIP (User Identifier Protocol) is a Host based ILSA scheme aiming at facilitating features such as roaming, multihoming and site (address) renumbering [59]. Unlike HIP or SHIM6, the UIP architecture deploys two identifier spaces, a user ID and a device ID. A user ID is a global unique identifier, which identifies the users devices, i.e., the set of devices (computers or mobile nodes), an entity

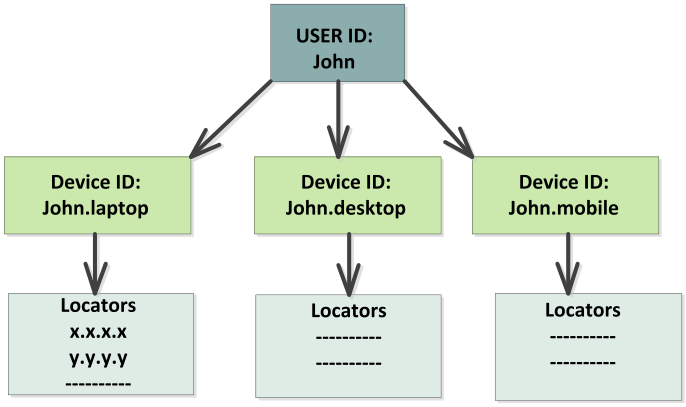


Fig. 9. Identifier and locator space of UIP architecture.

(person or company) can have. Moreover, each device has a device ID for its identification in the network, see Fig. 9. Finally, each device ID can be mapped into several locators (IP addresses) therefore increasing its reachability. These two identifier spaces make the UIP architecture more user-oriented. What does this mean? Generally speaking, a user-oriented communication puts the focus on establishing the connection to the user, regardless the specific device utilized by the user or the explicit user location. That is why UIP uses the concept of user ID.

UIP also extends the locators space, deploying two classes of locators, local and global, the first used to position devices within a domain and the second for inter-domain routing. This extension of the locators address also slows down the exhaustion of IPv4 addresses.

The mapping between IDs and locators is handled by a Distributed Mapping System; hence, not relying on DNS systems as SHIM6 and HIP do.

6.3.2. HRA

HRA (Hierarchical Routing Architecture) was built importing ideas from SHIM6 and HIP [60], but there are some clear differences among them. Unlike HIP, in HRA the IDs and the locators are aggregatable. The use of aggregatable identifiers eases up the process of management and assignment of IDs. The Locators used in HRA, also aggregatable, are 128 bits long, of which 96 bits are used for global routing, and the remaining 32 bits are reserved for local routing. As in UIP, this style of aggregatable locators prolongs the lifetime of IPv4 addresses.

Regarding the mapping phase, HRA relies on a DHT approach. In fact, a hierarchical DHT based Mapping System is applied for solving the mapping between HRA identifiers and locators [61]. Authors in [60] show how the use of a hierarchical DHT jointly with the aggregatable style of HRA identifiers substantially improves the mapping lookup efficiency.

6.3.3. ILNP

ILNP (Identifier-Locator Network Protocol) is a Host based ILSA scheme based in the GSE 8 + 8 architecture. However unlike GSE, ILNP can easily support security functionalities [62]. The main foundation of ILNP assumes IP will remain as the addressing scheme in Internet rather than thinking up novel clean slate approaches. Consequently, there are two versions of ILNP, ILNPv4 and ILNPv6 used for IPv4 and IPv6 addresses respectively. Finally, ILNP relies on a DNS based Mapping System for the mapping phase execution.

6.4. Open issues

The Host based ILSA schemes described in this section[1] have several open issues that hinder their deployment and development. In the following lines we briefly describe these issues.

- **Traffic engineering**: Host based ILSA schemes do not provide support for traffic engineering, as this feature must be managed at the network layer. In light of this, there are ILSA schemes that are hybrid, i.e., Host and Network based ILSAs, e.g., Six/One and HIP [66]. This is a clear example illustrating that Host and Network based ILSA schemes could be complementary with each other.
- **Security**: HIP does not provide security support for network features such as mobility and multihoming.
- **Seamless mobility support**: The seamless mobility support is not covered in SHIM6 and ILNP.
- **Adaptability**: SHIM6 and ILNP can only operate with IP addresses.
- **Other issues**: No performance information can be found for UIP. Moreover in HRA, the hierarchical DHT algorithm is not defined (Chord, Pastry) and no performance evaluation has been conducted proving the efficiency of this hierarchical DHT Mapping System.

7. Mapping System proposals

Any proposed ILSA scheme must accommodate a function termed as mapping phase responsible for the mapping between IDs and locators. Several trends have been already defined to deploy such mapping phase, developed within data and control planes. In fact, several ILSA schemes (e.g., Network based ILSAs) consider that the information

[1] Other proposals of Host based ILSA schemes can be found in [63–65].

concerning the mapping between IDs and locators (mapping entries) is stored locally on the border routers (i.e., the data plane), while others consider an external entity providing a mapping entry upon receiving a query from the ILSA scheme (i.e., the control plane).

Hence, the main task of a Mapping System is to provide a mapping entry, as the outcome of a lookup process on a database containing all mapping information. The overall mapping process relies on the accuracy of the information stored in the database, hence demanding the deployment of a strict updating strategy to accurately draw the real scenario. Unfortunately, this updating process is not that simple since it must guarantee that the deployed updating procedure accurately represents network dynamics, such as topology changes or users changing their ISP or connection point. The remaining part of this section is devoted to introduce a brief discussion on the foundations for each of the 4 flavors coming up after taxonomizing the Mapping Systems according to their technology:

- **DNS based**: Use similar infrastructure to the DNS system.
- **DHT based**: Use same operational concepts of DHT schemes.
- **Distributed Mapping Systems**: Rely on a set of decentralized database servers storing the mapping information.
- **Routing based**: Use routing protocols for their operation.

The following parameters may be used to measure the obtained performance:

- **Query processing time**: Number of queries per unit of time that a Mapping System can handle.
- **Convergence time**: Time required for a Mapping System to collect all the information regarding the mapping entries.
- **Mapping table size**: Stands for the dimension of the mapping table, i.e., the number of mapping entries.
- **Lookup table size**: Stands for the dimension of the lookup table, i.e., the number of nodes that could be queried to get a mapping entry.
- **Mapping resolution time**: The mapping resolution time (T_{map}) is the elapsed-time between submitting a query to the Mapping System and obtaining a response.
- **Hit/miss ratio**: Stands for the ratio between the number of successful query responses, and the total queries submitted to the Mapping System.

Additionally, other network features such as, security and mobility must be also considered when evaluating the performance of different Mapping Systems. In the following paragraphs, a deep description of each technology is introduced along with a descriptive performance evaluation in terms of the parameters previously presented.

7.1. DNS based Mapping Systems

Authors in [67] show the effectiveness of a DNS Mapping System for an ILSA scheme. DNS based Mapping Systems rely on the current DNS architecture for its operation. The main benefit of this approach is that DNS systems are widely deployed and tested in the current Internet. However, there are some issues limiting its deployment as an appealing solution for a Mapping System, all linked to scalability concerns. A significant aspect points to the dimension of the lookup table size on a large-scale scenario (such as the FI). According to [68], there are 142×10^6 domains on the Internet, more than the total entries of the default free zone (DFZ), that is around 400,000 [69]. Since total entries of the default free zone (DFZ) is far less than the total domain on the Internet, it is reasonable to think that the use of DNS systems as Mapping System for an ILSA scheme seems feasible because the burden caused by adding the mapping entries in the DNS system does not represent an important constraint for the DNS.

Another issue concerning DNS based Mapping Systems is the mapping resolution time. In this regard, authors in [70] presented a study assessing that the 30% of the time used to retrieve a web page is spent in the resolution phase (mapping resolution time) and that the resolution time for the 30% of the queries sent to the DNS systems is around 2 s. Despite this, the contribution of the DNS lookup to the resolution time of the current Internet, is far away from being considered as a problem. However, this statement cannot be extended to a FI scenario, mainly due to two key constraints: (i) this level of performance does not meet the QoS requirements demanded by future Internet applications [71], and (ii) Internet grows super-linearly towards the FI what may degrade the performance of a DNS Mapping System. But, where does the delay occur? and who produces it?

The delay in the DNS resolution time is mainly caused by low cache hit rates, which are induced from the heavy-tailed, Zipf-like query distribution in DNS. Past studies on Web caching, demonstrated that a heavy-tailed query distribution severely limits the hit/miss ratio of the DNS. Practically, this effect causes that 23% of the total lookups are never answered and 13% of the lookups does it with errors [72].

DNS per se, is a hierarchical structure. While a hierarchical design assures that the lookup table size will not be drastically impacted [73], this hierarchical nature could also hinder its deployment as a Mapping System for ILSA schemes. This is because high-demand mapping-entries could create "hot spots" in the network, i.e., the nodes (part of the Mapping System) that gather information regarding mapping entries with high-demand queries, could be overloaded.

Finally, accuracy comes up as a severe limitation as well. In fact, while accuracy has been a traditional problem in networking (traffic engineering database, link state information, etc.), the picture posed in ILSA schemes is even more stressful, particularly when dealing with mobility scenarios. This statement is motivated by the capacity users have to move and hence change their locator when migrating to a new ISP provider or due to roaming. The analysis shown in [74,67] evidence an "acceptable" performance of DNS systems in mobile environments. Nevertheless, large scale experiments must be deployed before issuing a final conclusion about performance.

Despite the limitations stated above for deploying a Mapping System DNS based, i.e., lookup table size, delays, hierarchical structure, and accuracy, some control plane schemes relying on DNS have been already proposed. In [75] authors present LISP-Tree as a Mapping System for LISP. Main LISP-Tree characteristic is that it separates the process of storing the mapping entries from the discovery of a new mapping entry.

In the LISP-Tree architecture the border routers store the mapping entries, which may limit the scalability of the ITRs in terms of memory consumption. Moreover, the mapping phase operation is handled by a DNS system, which makes it susceptible to the same limitations of a DNS system (described above).

Another approach for a Mapping System for LISP is proposed in [73]. The proposed approach is a hybrid of DNS based and Distributed Mapping System aiming at minimizing the mapping resolution time. In fact, the main foundation boils down to parallelizing domain and mapping entry lookups, so that $T_{map} + T_{DNS} \approx T_{DNS}$. To this end, an entity named LISP Control Box (LCB) is introduced on each domain storing all mapping entries for the domain. When a node issues a query to its local DNS, the LCB also sets a connection to obtain the ID-LOC mapping, hence parallelizing both domain mapping and ID-LOC mapping.

Therefore, although DNS based solutions suffer from some issues that remain yet unsolved, some key advantages fostering their deployment.

Open issues: As explained above there are aspects related to scalability, lookup table size, DNS hierarchical nature, accuracy and the delays introduced inherent to the mapping resolution time restricting a wide deployment of DNS based Mapping Systems for ILSA schemes.

Advantages: The main advantage of DNS falls in its maturity. DNS is a very well tested and controlled system already deployed in current network infrastructures. Particular extensions have also been proposed to improve DNS performance in concrete scenarios, for example DNS extensions (DNSSEC) endowing the Mapping System with security support.

Conclusions: DNS systems have an "acceptable" performance even in mobile environments, though its effectiveness must be proven in large scale scenarios.

7.2. DHT Mapping Systems

Distributed Hash Table systems (DHTs) such as, Chord [76] and CAN [77], have a solid success trajectory in P2P scenarios. The main reason deals with their good performance and low complexity. For example, Chord exhibits a logarithmic behavior for the lookup table size ($Olog(p)$) and the T_{map}, being p the number of ID/LOC pairs in the overlay network (the topology created by the DHT algorithm). These two characteristics turn DHTs into an appealing solution for a Mapping System. In fact, despite not intended for an ILSA scheme, authors in [78] propose the first approach for a DHT based Mapping System, hence opening the door to deploy DHT in other scenarios requiring mapping capabilities as well.

Thus, several proposals came up in the recent years, using DHT schemes as Mapping Systems for ILSAs. For instance, [79] proposes a DHT Mapping System based on Chord for a LISP environment and [80], proposes an implementation of a DHT Mapping System based on CAN.

Nevertheless, there are several characteristics that may hinder the use of DHTs as Mapping Systems. We put the focus on four main weaknesses. The first weakness deals with the fact that in a DHT network, usually the key-value pairs are randomly distributed in order to avoid hot spots in the network. This means that the node hosting the mapping entry will not be directly queried. In an ILSA context this would mean that each domain will delegate the management of their mapping entries to other domains, what brings significant chances to conflict with the business policies between domains, i.e., a domain might not be interested in delegating their mapping entries to another particular domain that for example, might be a competing company.

The second weakness refers to the lack of geographical proximity [81]. For instance, two nodes that are neighbors in the DHT overlay may be geographically distant in the underlying network. This ignorance may drive to the non desired scenario where a domain in North Korea requests a mapping entry from a domain in USA. Beyond business policies in-place, this unawareness of the underlying network topology could significantly degrade the performance of a DHT Mapping System, hence increasing the T_{map} value.

The third weakness deals with security. The lack of security is also preventing DHT to be a viable solution for a Mapping System. Indeed, the information provided by the Mapping System must be validated to avoid hijacking attacks. Unfortunately native forms of Chord or other DHT schemes do no provide security coverage.

Finally, the fourth weakness deals with failure scenarios. When a node belonging to the DHT overlay fails the key-value pairs need to be redistributed. These changes incur on high churn activity that degrades the DHT performance. In particular, the convergence time and the T_{map} are both increased and the hit/miss ratio may be decreased [82,83]. Another aspect referring to churn activity is the mobility of nodes. In fact, nodes mobility also causes churns in the DHT overlay, which also degrades the performance of DHTs schemes [84].

Recently, several efforts have been deployed to deal with the challenges posed by these four weaknesses. In [85,86] authors propose DHT implementations that consider geographical information when building the DHT topology, hence minimizing resources consumption in the underlying network. Regarding the security issues a collection of DHT security techniques can be found in [87]. Failure scenarios are also analyzed in the ongoing work proposed in [88–90].

The following conclusions can be inferred from the above discussion.

Open issues: Despite several DHT algorithms have already been proposed [91], the need to solve the remaining research challenges yet open, makes impossible to get a wide consensus on the algorithm best suiting the required needs to play the role of a Mapping System in a ILSA scheme. Four research challenges have been clearly illustrated in this section, random

key-values distribution, geographical distribution, security and performance in failure scenarios.

Advantages: The T_{map} and mapping tables size follow a logarithmic behavior. Moreover, a DHT Mapping System can be easily adapted to any addressing scheme (not only to IP, which is usually the case in DNS schemes). These characteristics make DHT a highly scalable and adaptable solution for Mapping Systems in ILSA schemes.

Conclusions: DHT Mapping Systems have a good performance even in large-scale scenarios, even though their effectiveness must be yet proven in mobile environments.

7.3. Distributed Mapping Systems

A Distributed Mapping System bases its operation on (distributed) dedicated nodes serving as databases containing the mapping entries for all Internet users. That said, the reader may confuse Distributed Mapping Systems with DHT Mapping Systems since the latter also distributes the mapping entries among a set of dedicated nodes. The difference falls in the fact that unlike DHT Mapping Systems, the topological organization and the distribution of the mapping entries in a Distributed Mapping System is not done following a DHT algorithm.

Distributed Mapping Systems may be categorized into two approaches: (1) push distribution model, and (2) pull distribution model. In a push distribution model, each domain has a set of network elements that store the mapping entries. These network elements update their mapping entries in a proactive manner at regular time intervals by querying the Distributed Mapping System. In a pull distribution model, a query is sent to the Mapping System whenever a mapping entry is requested.

It must be remarked that at the time of designing a Distributed Mapping System, the distribution of the mapping entries among the nodes building the Mapping System, and the topological organization of these nodes, are a design criteria decoupled from the chosen approach (push or pull).

Depending on some implementation decisions, the final performance could substantially deviate. Thus, metrics such as T_{map} basically depend on the topological organization chosen for the dedicated nodes. But usually, the Distributed based Mapping Systems (as in DNS based Mapping Systems), tend to have low T_{map} values and high query processing time. However, as the number of mapping entries grows, the T_{map} increases, as well as the number of signaling messages generated and the size of the mapping table. At the same time, the computational resources of the nodes building the Mapping System must be higher, what might represent an increase of CapEx and/or Opex that small and medium companies could not afford.

Moreover, issues related to resilience and seamless mobility are not totally addressed. For instance, there are no mechanisms stating any procedure for restoration in case of failures. Specifically, actions to distribute the mapping entries or the redirection of the queries in case of failures must be further defined. There is no either any evaluation analysis showing the performance of a Distributed based Mapping System in a scenario of high churn due to the mobility of users.

On the other hand, security features can be easily supported by Distributed Mapping Systems. In fact, there are well defined protocols, for instance, PKI or IPsec that can be used for providing protection against hijacking attacks as well as for endowing a Distributed Mapping System with validation mechanisms.

Despite the limitations presented above, several Mapping System proposals already adopt a distributed approach, such as, FIRMS [92], and LISP–NERD [93]. FIRMS is a Mapping System (designed for Network based ILSA schemes) which follows a pull distribution model. FIRMS follows a hierarchical design consisting in three layers. The highest layer is formed by regional Internet registries (RIRs): AfriNIC, APNIC, LAC-NIC, ARIN, and RIPE NCC. The middle layer is formed by the local Internet registries (LIRs). A RIR delegates a subset of its mapping entries to a LIR. Every RIR and LIR, exchanges their mapping entries with dedicated nodes, building the Mapping System, so that mapping entries are distributed among these ones. The lower layer is formed by local databases belonging to a particular domain. Regarding the topological design of the Mapping System, it must be noticed that nodes on the same layer are fully meshed. Therefore, a node of a certain layer could query another node for a particular mapping, or could forward this request to its superior layer.

The operation in FIRMS works as follows: When a border router requests a mapping entry, the local database first checks if the mapping entry is on its cache. Otherwise, a request is sent to the Mapping System. Afterwards, the node hosting the requested mapping sends a reply back to the local database. Then, the local database stores the reply on its cache (depending on the cache policies), and forwards it to the border router.

FIRMS promises to make the current Internet architecture more scalable, although additional evaluation tests must be run to check T_{map} behavior to demonstrate its scalability.

Another Distributed Mapping System is LISP–NERD. LISP–NERD uses a central database storing all mapping entries, managed by a central authority. These mapping entries are forwarded to the border routers of each domain following a push distribution model and are updated using HTTP based messaging at regular time intervals.

The following open issues and advantages can be found in a Distributed Mapping System.

Open issues: Scalability issues such as the size of the mapping tables need to be addressed. Also, seamless mobility features are not totally addressed.

Advantages: Distributed Mapping Systems tend to have a low T_{map}. Also, they are easy to implement and deploy.

Conclusions: The low T_{map} of Distributed Mapping Systems makes them an appealing Mapping System solution; however, the scalability of their the mapping tables size hinders their deployment.

7.4. Routing based Mapping Systems

Any ILSA scheme deploying a Routing based Mapping System requires a routing protocol for explicitly supporting the mapping phase. In practice, this means that the distribution and location of mapping entries are both handled by a routing protocol running on the border routers of each domain.

Several advantages are inherent to implementing Routing based Mapping Systems, such as an easy deployment and low CapEx investments. In fact, typical activities such as deployment, management and configuration are easy to handle because of both, a simple upgrade of the operating system on the border routers would be enough, even a small company could run their customized Routing based Mapping System and network administrators are very familiar with using routing protocols.

Nevertheless, despite the easy handling inherent to a routing scheme, there are several issues still hindering a massive adoption of Routing based Mapping Systems. These issues are mainly rooted on the fact that Mapping Systems tend to inherit all flaws of their parent technology. This would mean that whether the chosen routing protocol is unstable against security attacks or does not support traffic engineering techniques, the Routing based Mapping System would also inherit these flaws. Consequently, Routing based Mapping Systems must enhance the routing protocols features, hence adding complexity to the overall design.

LISP–ALT [94] is a proposal for Routing based Mapping System relying on BGP on top of GRE tunnels to propagate ID prefixes. LISP–ALT is designed for operating in a LISP environment, which unfortunately hinders its operation with other ILSA schemes. As mentioned above, LISP–ALT may inherit all BGP flaws, including, the lack of security and traffic engineering support [18,8]. Moreover, the slow convergence of BGP could drive the Mapping System to behave unstable against failures in the network, hence increasing T_{map}, and the hit/miss ratio metrics [95]. However, there are several initiatives such as [96–98,16], that attempt to address the issues regarding security and TE capabilities of BGP.

LISP–EMACS [99] is another Routing based Mapping System, which proposes the use of PIM (Protocol Independent Multicast) as the routing protocol to propagate ID prefixes. However, LISP–EMACS is only compatible for LISP architecture.

The following conclusions can be summarized for Routing based Mapping Systems:

Open issues: Several doubts arise about whether it is feasible to use BGP as the protocol to propagate mapping entries to the Border Routers. For instance, LISP–ALT (which employs BGP) inherits all the flaws of BGP, including slow convergence and security vulnerability. Other routing protocols such as PIM must be endowed with security features.

Advantages: Routing protocols are well proven and exhibit high adaptability with current network technologies.

Conclusions: Routing based Mapping Systems are highly adaptable with the current network technologies, but they are vulnerable to security threats.

7.5. Mapping Systems comparison

Table 2 shows a comparative analysis of the different categories of Mapping Systems regarding different metrics, such as scalability, mobility, security and resilience/survivability performance.

It is important to highlight the scalability problems embedded to Routing based, DNS and Distributed based Mapping Systems. Routing based Mapping Systems assume the linear growth of the size of the mapping tables with the number of users in the network. DNS and Distributed Mapping Systems severely accuse scalability concerns regarding the mapping entries size. Distributed based Mapping Systems must also face the potential overload generated in some nodes receiving a high volume of mapping entries requests due to its hierarchical nature (hot spots).

DHT approaches skip the scalability issues since the mapping table size grows logarithmically. However, similar to Routing based Mapping Systems, DHTs suffer from security concerns more significantly than DNS and Distributed based Mapping Systems.

Nevertheless, considering the resilience/survivability feature, DHTs schemes are more robust compared to the Distributed based Mapping Systems.

8. Conclusions and insights on ILSAs

Several challenging problems are requiring novel ideas from the scientific community to overcome the existing limitations on the current Internet. Unfortunately the nature of these problems is not static, but rather new challenges continuously come up linked to the new technologies offered by the network infrastructure and the continuous birth of applications/services offered to users. Thus, the scientific community should produce solutions devised to face not only the nowadays scenario (and hence its known and well-defined problems) but also to support future expected and non-expected challenges. In this paper, we survey a research line focused on solving well-known routing related issues such as, the depletion of addresses, the increment in the size of the routing tables due to the bad practice of multihoming and traffic engineering, and the limited support for mobility and fault tolerant communications on Internet.

The issue of address depletion has been widely studied and commented by the scientific community. A straightforward solution is to have a bigger address space, as proposed by IPv6 with an address space size of 2^{128}, that seems more than enough to tackle the address depletion problem. However, this is only a workaround that does not solve the main causes of the Internet routing problems.

In fact, the main burden preventing healthy routing procedures refers to the twofold functionality associated to the current addressing scheme, namely identification

Table 2
Comparative of Mapping Systems.

	DNS based	DHT based	Distributed based	Routing based
Scalability	Med	High	Med	Low
Mobility	Med	Low	Low	High
Performance[a]	High	High	High	Med
Security	High	Med	High	Med
Resilience/survivability	Low	High	Low	Med

[a] Performance is an average of the performance metrics described in Section 7: resolution time, hit/miss ratio, etc.

and location of hosts (widely known as semantic overload of addresses). Hence, it seems obvious that decoupling both functionalities might turn into a fast and significant improvement of the routing procedures.

To this end, ID/Locator Split Architectures (ILSAs) are proposed as a straightforward solution. The main advantages of a wide deployment of an ILSA scheme have been deeply detailed in this paper, such as extension of IPv4 lifetime, support in the migration from IPv4 to IPv6, as well as mobility, multihoming and resilience support.

But the ILSA paradigm was tentatively proposed as an architectural framework facing the address semantic overload problem. In other words, ILSA is just a proposal that might not be supported by all the scientific community. Thus, authors in [100] open a discussion about the scalability for ILSA schemes, arguing that ILSA is not the best approach for a scalable routing system. The main arguments to support this statement are: (i) the aggregation imposed by ILSAs is not effective on scale-free networks such as Internet, and (ii) the churn associated to maintain and guarantee updated mapping entries will difficult the scalability of the Mapping System.

We partially agree with the first bullet since theoretically ILSAs cannot improve the routing system scalability. However, an ILSA scheme can enhance several network features, such as multihoming, mobility (at least nomadic), and end-to-end security. Moreover, ILSAs schemes may reduce the routing table size. We also agree on the second bullet stating that the performance of the Mapping System is a critical issue in an ILSA scheme. Nevertheless, we consider that an ILSA scheme employing a Mapping System, which maintains a high performance under several conditions, such as, failures, constant mobility of users, providing protection against security attacks, then this ILSA may address several problems that are affecting the current internet.

On the other hand, there is an open debate in the network research community, concerning the selection of a scalable routing and addressing architecture for the Future Internet (FI). In [11–15,5], proposals for clean slate architectures can be found, all of them imposing a new addressing or routing scheme. Our argument is that the disruptive nature of clean slate architectures hinders their deployment.

Furthermore, new addressing solutions such as IPv6 offer a wide enough address space to support the growing demand of internet users for the coming years. However, in a not distant future, the availability of IPv6 addresses might come to an end, similar to its counterpart (IPv4). On this basis, the idea of adaptation instead of migration is what has to prevail when thinking in the FI.

Our conclusion is that ILSA schemes may be a useful tool for solving the current internet problems, such as the exhaustion of internet address, but they are more suitable to cope with certain concrete use-cases such as:

- Address interoperability (IPv4 and IPv6 coexistence). Therefore, this proves that IPv6 and ILSA schemes are complementary.
- Network mobility, when the network technologies do not support it, this is a handy feature for equipment migration in Data Centers, and for offering roaming capabilities in mobile networks.
- Provide muti-homing and TE capabilities, these network features are not fully supported by the common network technologies, such as BGP. Therefore, network technologies can be enhanced by ILSA schemes.
- Provide resilience capabilities without the use of proprietary protocols. This can be achieved with minimal configurations in the network.

Notice that many network vendors such as Cisco are including ILSA schemes as part of their product catalog, e.g., LISP. As a result, small and large network operators are starting to leverage the advantages provided by ILSAs.

We also conclude that both Network and Host based ILSAs can efficiently address the issues described above. On one hand, Host based schemes offer higher granularity for the identification of entities, i.e., virtual and tangible objects, compared with Network based schemes. On the other hand, Network based ILSAs can be more easily deployed, since modifications are required only on the border routers (Host based ILSAs required modifications on every host machine). In addition, network features such traffic engineering are covered by Host based ILSAs, but they can be easily supported on Network based ILSAs. Nevertheless, as we describe in this article, Network and Host based ILSAs can operate in a combined fashion. To this end, Hybrid based ILSAs have been proposed with the aim of enhancing network features such as traffic engineering.

Moreover, we consider that the Mapping System plays a crucial role on ILSA schemes in order to improve their scalability. The selection of the Mapping System depends on the type of network scenario an ILSA scheme will be deployed in, i.e., network design decision. For large environments, in which scalability is a major concern, DHT Mapping Systems are the best solution. However, for addressing specific issues such as network mobility or address interoperability, routing based Mapping Systems or Distributed Mapping Systems are the best solution respectively, due to the fast convergence of routing based

Mapping Systems compared to DHT schemes, and the low T_{map} offered by distributed based schemes.

Finally, we argue that in the coming years ILSA schemes will start to become a common feature offered by network vendors rather than being a research study. This holds true as long as ILSAs are positioned in small or medium scale scenarios.

Acknowledgments

This work was supported by the Spanish Ministry of Economy under contract TEC2012-34682, and the Catalan Research Council (CIRIT) under contract 2009 SGR1508.

References

[1] L. Cittadini, W. Muhlbauer, S. Uhlig, R. Bush, P. Francois, O. Maennel, Evolution of internet address space deaggregation: myths and reality, IEEE J. Sel. Area. Commun. 28 (8) (2010) 1238–1249, http://dx.doi.org/10.1109/JSAC.2010.101002.
[2] D.W.N. Murphy, The end of eternity part one: IPv4 address exhaustion and consequences, Int. Prot. J. 11, 2011.
[3] T. Hain, A pragmatic report on IPv4 address space consumption, Int. Prot. J. 2008.
[4] G. Huston, IPv4 address depletion, Int. Prot. J. 3, 2003.
[5] h.-. TARIFA.
[6] J.N. Chiappa, Endpoints and endpoint names: a proposed enhancement to the internet architecture, 1999 <http://ana.lcs.mit.edu/simjnc//tech/endpoints.txt>.
[7] http://www.cisco.com/go/lisp.
[8] M. Yannuzzi, X. Masip-Bruin, O. Bonaventure, Open issues in interdomain routing: a survey, IEEE Netw. 19 (6) (2005) 49–56, http://dx.doi.org/10.1109/MNET.2005.1541721.
[9] X. Zhao, D. Pacella, J. Schiller, Routing scalability: an operator's view, IEEE J. Sel. Area. Commun. 28 (8) (2010) 1262–1270, http://dx.doi.org/10.1109/JSAC.2010.101004.
[10] G. Huston, The changing foundation of the internet: confronting IPv4 address exhaustion, Int. Prot. J. 11, 2011.
[11] M. Gritter, D. R. Cheriton, An architecture for content routing support in the internet, in: Proceedings of the 3rd Conference on USENIX Symposium on Internet Technologies and Systems, USITS'01, vol. 3, USENIX Association, Berkeley, CA, USA, 2001, pp. 4–4 <http://dl.acm.org/citation.cfm?id=1251440.1251444>.
[12] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K.H. Kim, S. Shenker, I. Stoica, A data-oriented (and beyond) network architecture, SIGCOMM Comput. Commun. Rev. 37 (4) (2007) 181–192, http://dx.doi.org/10.1145/1282427.1282402.
[13] M. Caesar, T. Condie, J. Kannan, K. Lakshminarayanan, I. Stoica, ROFL: routing on flat labels, SIGCOMM Comput. Commun. Rev. 36 (4) (2006) 363–374, http://dx.doi.org/10.1145/1151659.1159955.
[14] K. Visala, D. Lagutin, S. Tarkoma, LANES: an inter-domain data-oriented routing architecture, in: Proceedings of the 2009 Workshop on Re-Architecting the Internet, ReArch '09, ACM, New York, NY, USA, 2009, pp. 55–60. http://dx.doi.org/10.1145/1658978.1658992.
[15] J. Choi, J. Han, E. Cho, T. Kwon, Y. Choi, A Survey on content-oriented networking for efficient content delivery, IEEE Commun. Mag. 49 (3) (2011) 121–127, http://dx.doi.org/10.1109/MCOM.2011.5723809.
[16] X.M.-B.F.B.R.W.P.M.M. Yannuzzi, R. Serral-Gracia, D. Ward, Path-State Graphs on BGP, Tech. Rep., UPC/CRAAX, 2009.
[17] D. Pei, B. Zhang, D. Massey, L. Zhang, An analysis of convergence delay in path vector routing protocols, Comput. Netw. 50 (3) (2006) 398–421, http://dx.doi.org/10.1016/j.comnet.2005.04.013.
[18] K. Butler, T. Farley, P. McDaniel, J. Rexford, A survey of BGP security issues and solutions, Proc. IEEE 98 (1) (2010) 100–122, http://dx.doi.org/10.1109/JPROC.2009.2034031.
[19] The Internet of Things <http://www.itu.int/internetofthings>.
[20] Y. Huang, G. Li, A semantic analysis for internet of things, in: 2010 International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 1, 2010, pp. 336–339. doi: http://dx.doi.org/10.1109/ICICTA.2010.73.
[21] P. Debaty, D. Caswell, Uniform web presence architecture for people, places, and things, IEEE Pers. Commun. 8 (4) (2001) 46–51, http://dx.doi.org/10.1109/98.944003.
[22] A.M.S. Bradner, The Recommendation for the IP Next Generation Protocol, RFC 1752, 1995.
[23] http://playground.sun.com/ipv6.
[24] K.F.D. Meyer, L. Zhang, Report from the IAB Workshop on Routing and Addressing, Tech. Rep., 2007.
[25] R.H.S. Deering, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, 1998.
[26] D.L.B. Cole, P. Morton, Cisco Hot Standby Router Protocol (HSRP), 1998.
[27] E.D.B.B.V.G.J. Abley, K. Lindqvist, IPv4 Multihoming Practices and Limitations, RFC 4116, 2005.
[28] L.E.C.D. TR. Henderson, A. Gurtov, Dagstuhl Seminar on Naming and Addressing for Next Generation Internetworks, 2007.
[29] J. Saltzer, On the Naming and Binding of Network Destinations, 1993.
[30] R. Ahmed, R. Boutaba, F. Cuervo, Y. Iraqi, T. Li, N. Limam, J. Xiao, J. Ziembicki, Service naming in large-scale and multi-domain networks, IEEE Commun. Surv. Tutor. 7 (3) (2005) 38–54, http://dx.doi.org/10.1109/COMST.2005.1610549.
[31] R.S.P. Leach, M. Mealling, A Universally Unique Identifier (UUID) URN Namespace , RFC 4122, 2005.
[32] M.M.T. Berners-Lee, L. Masinter, Uniform Resource Locators (URL), RFC 1738, 1994.
[33] General requirements for ID/locator separation in NGN.
[34] D.M.D.L.D. Farinacci, V. Fuller, Locator/Id Separation Protocol (LISP), 2012.
[35] C. Vogt, Six/one router: a scalable and backwards compatible solution for provider-independent addressing, in: Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture, MobiArch '08, ACM, New York, NY, USA, 2008, pp. 13–18. http://dx.doi.org/10.1145/1403007.1403011.
[36] M. O'Dell, GSE – An Alternate Addressing Architecture for IPv6.
[37] P.N.R. Moskowitz, Host Identity Protocol (HIP) Architecture, RFC 4423.
[38] M.B.E. Nordmark, Shim6:Level 3 Multihoming Shim Protocol for IPv6, RFC 5533, 2009.
[39] R. Hinden, New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG RFC 1955, 1996.
[40] B.Z.L.D. Massey, L. Wang, A scalable routing system design for future internet, 2007.
[41] F. Templin, The IPvLX Architecture, 2007.
[42] R. Whittle, Ivip (Internet Vastly Improved Plumbing) Architecture, 2010.
[43] X. Zhang, P. Francis, J. Wang, K. Yoshida, Scaling IP routing with the core router-integrated overlay, in: Proceedings of the 2006 IEEE International Conference on Network Protocols, ICNP '06, IEEE Computer Society, Washington, DC, USA, 2006, pp. 147–156. http://dx.doi.org/10.1109/ICNP.2006.320208.
[44] A.C.D.S.O.B.F. Maino, V. Ermagan, LISP-Security (LISP-SEC), draft-ietf-lisp-sec-04, 2012.
[45] P. Savola, MTU and Fragmentation Issues with In-the-Network Tunneling, RFC 4459, 2006.
[46] M. Menth, D. Klein, M. Hartmann, Improvements to LISP Mobile Node, in: Teletraffic Congress (ITC), 2010 22nd International, 2010, pp. 1–8. doi: http://dx.doi.org/10.1109/ITC.2010.5608725.
[47] D.M.D. Farinacci, D. Lewis, LISP Mobile Node.draf-meyer-lisp-mn-08, 2012.
[48] M.G.R.S.-G.M.G.R.S.-G.E.M.-T.M.Y.X.M.-B.A. Martinez, W. Ramirez, An approach to a fault tolerance LISP architecture, in: WWIC, Springer, 2011, pp. 338–349.
[49] F.B.M. Wasserman, IPv6-to-IPv6 Network Address Translation (NAT66), draft-mrw-behave-nat66-02.txt, 2011.
[50] R.M.A. Gurtov, M. Komu, Host Identity Protocol: Identifier/Locator Split for Host Mobility and Multihoming, The Int. Prot. J. 12(1) (2012).
[51] C.V.P. Nikander, T. Henderson, Mobility and Multihoming with the Host Identity Protocol, 2008.
[52] R.G.O. Kolkman, DNSSEC Operational Practices, RFC 4641, 2006.
[53] http://www.openhip.org/.
[54] https://launchpad.net/hipl.
[55] http://infrahip.hiit.fi/.
[56] M. Bagnulo, Hash-Based Addresses (HBA), RFC 5535 (June).
[57] T. Aura, Cryptographically Generated Addresses, (CGA), RFC 3972, 2005.
[58] J. Arkko, I. van Beijnum, Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming, RFC 5534 (June).

[59] H. Li, C. Peng, B. Li, Y. Chen, W. Zhang, J. Wu, H. Huang, User ID routing architecture, IEEE Veh. Technol. Mag. 5 (1) (2010) 62–69, http://dx.doi.org/10.1109/MVT.2009.935541.
[60] X. Xu, D. Guo, Hierarchical Routing Architecture (HRA), in: Next Generation Internet Networks, 2008. NGI 2008, 2008, pp. 92–99. doi: http://dx.doi.org/10.1109/NGI.2008.19.
[61] P.F.K.R.L. Garces-Erice, E. Biesack, G. Urvoy-Keller, Hierarchical Peer-to-peer Systems, in: Euro-Par 2003, 2003.
[62] R. Atkinson, S. Bhatti, S. Hailes, Evolving the internet architecture through naming, IEEE J. Sel. Area. Commun. 28 (8) (2010) 1319–1325, http://dx.doi.org/10.1109/JSAC.2010.101009.
[63] J. Pan, R. Jain, S. Paul, C. So-in, MILSA: a new evolutionary architecture for scalability, mobility, and multihoming in the future internet, IEEE J. Sel. Area. Commun. 28 (8) (2010) 1344–1362, http://dx.doi.org/10.1109/JSAC.2010.101012.
[64] V. Kafle, H. Otsuki, M. Inoue, An ID/locator split architecture for future networks, IEEE Commun. Mag. 48 (2) (2010) 138–144, http://dx.doi.org/10.1109/MCOM.2010.5402677.
[65] W.R.E.M.A. Martinez, X. Masip-Bruin, Toward a New Addressing Scheme for a Service-Centric Internet, ICC, 2012.
[66] http://www.ietf.org/proceedings/70/slides/hip-3.pdf.
[67] S. Yang, H. Luo, Y. Qin, H. Zhang, Design and evaluation of DNS as location manager for HIP, Wireless Pers. Commun. 48 (2009) 605–619, http://dx.doi.org/10.1007/s11277-008-9550-x.
[68] http://www.domaintools.com/internet-statistics/.
[69] http://bgp.potaroo.net/.
[70] C.E. Wills, H. Shang, The Contribution of DNS Lookup Costs to Web Object Retrieval, 2000.
[71] Y. Chen, T. Farley, N. Ye, QoS requirements of network applications on the internet, Inf. Knowl. Syst. Manage. 4 (1) (2004) 55–76.
[72] J. Jung, E. Sit, H. Balakrishnan, R. Morris, DNS performance and the effectiveness of caching, IEEE/ACM Trans. Netw. 10 (5) (2002) 589–603, http://dx.doi.org/10.1109/TNET.2002.803905.
[73] M. Yannuzzi, X. Masip-Bruin, E. Grampín, R. Gagliano, A. Castro, M. Germán, Managing interdomain traffic in Latin America: a new perspective based on LISP, Commun. Mag. 47 (7) (2009) 40–48, http://dx.doi.org/10.1109/MCOM.2009.5183471.
[74] A. Reaz, M. Atiquzzaman, S. Fu, Performance of DNS as location manager for wireless systems in IP networks, in: Global Telecommunications Conference, 2005, GLOBECOM '05, vol. 1, IEEE, 2005, p. 5. doi: 10.1109/GLOCOM.2005.1577649.
[75] L. Jakab, A. Cabellos-Aparicio, F. Coras, D. Saucez, O. Bonaventure, LISP-TREE: a DNS hierarchy to support the lisp mapping system, IEEE J. Sel. Area. Commun. 28 (8) (2010) 1332–1343, http://dx.doi.org/10.1109/JSAC.2010.101011.
[76] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, H. Balakrishnan, Chord: a scalable peer-to-peer lookup protocol for Internet applications, IEEE/ACM Trans. Netw. 11 (1) (2003) 17–32, http://dx.doi.org/10.1109/TNET.2002.808407.
[77] S. Ratnasamy, P. Francis, M. Handley, R. Karp, S. Shenker, A scalable content-addressable network, in: PROC. ACM SIGCOMM 2001, 2001, pp. 161–172.
[78] V. Ramasubramanian, E.G. Sirer, The design and implementation of a next generation name service for the internet, SIGCOMM Comput. Commun. Rev. 34 (4) (2004) 331–342, http://dx.doi.org/10.1145/1030194.1015504.
[79] L. Mathy, L. Iannone, LISP-DHT: towards a DHT to map identifiers onto locators, in: Proceedings of the 2008 ACM CoNEXT Conference, CoNEXT '08, ACM, New York, NY, USA, 2008, pp. 61:1–61:6. doi: http://dx.doi.org/10.1145/1544012.1544073.
[80] H. Luo, Y. Qin, H. Zhang, A DHT-based identifier-to-locator mapping approach for a scalable internet, IEEE Trans. Paral. Distrib. Syst. 20 (12) (2009) 1790–1802, http://dx.doi.org/10.1109/TPDS.2009.30.
[81] J. Dai, F. Liu, B. Li, The disparity between P2P overlays and ISP underlays: issues, existing solutions, and challenges, IEEE Netw. 24 (6) (2010) 36–41, http://dx.doi.org/10.1109/MNET.2010.5634441.
[82] J. Li, J. Stribling, R. Morris, M. Kaashoek, T. Gil, A performance vs. cost framework for evaluating DHT design tradeoffs under churn, in: INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 1, 2005, pp. 225–236. doi: http://dx.doi.org/10.1109/INFCOM.2005.1497894.
[83] K. Gummadi, R. Gummadi, S. Gribble, S. Ratnasamy, S. Shenker, I. Stoica, The impact of DHT routing geometry on resilience and proximity, in: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '03, ACM, New York, NY, USA, 2003, pp. 381–394. doi: http://dx.doi.org/10.1145/863955.863998.
[84] H.-C. Hsiao, C.-T. King, Mobility churn in DHTs, in: 25th IEEE International Conference on Distributed Computing Systems Workshops, 2005, 2005, pp. 799–805. doi: http://dx.doi.org/10.1109/ICDCSW.2005.98.
[85] F. Memon, D. Tiebler, F. Dürr, K. Rothermel, M. Tomsu, P. Domschitz, Scalable spatial information discovery over Distributed Hash Tables, in: Proceedings of the Fourth International ICST Conference on COMmunication System SoftWAre and MiddlewaRE, COMSWARE '09, ACM, New York, NY, USA, 2009, pp. 1:1–1:12. doi: http://dx.doi.org/10.1145/1621890.1621892.
[86] A. Harwood, E. Tanin, Hashing spatial content over peer-to-peer networks, in: Australian Telecommunications, Networks, and Applications Conference – ATNAC, 2003, pp. 1–5.
[87] G. Urdaneta, G. Pierre, M.V. Steen, A survey of DHT security techniques, ACM Comput. Surv. 43 (2) (2011) 8:1–8:49, http://dx.doi.org/10.1145/1883612.1883615.
[88] D. Bin, W. Furong, T. Yun, Improvement of network load and fault-tolerant of P2P DHT systems, in: International Conference on Information Technology: Research and Education, 2006. ITRE '06, 2006, pp. 187–190. doi: http://dx.doi.org/10.1109/ITRE.2006.381561.
[89] Y. Zhai, Y. Wang, I. You, J. Yuan, Y. Ren, X. Shan, A DHT and MDP-based mobility management scheme for large-scale mobile internet, in: 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2011, pp. 379–384. doi: http://dx.doi.org/10.1109/INFCOMW.2011.5928842.
[90] O. Landsiedel, S. Götz, K. Wehrle, A churn and mobility resistant approach for DHTs, in: Proceedings of the 1st International Workshop on Decentralized Resource Sharing in Mobile Computing and Networking, MobiShare '06, ACM, New York, NY, USA, 2006, pp. 42–47. doi: http://dx.doi.org/10.1145/1161252.1161263.
[91] E.K. Lua, J. Crowcroft, M. Pias, R. Sharma, S. Lim, A survey and comparison of peer-to-peer overlay network schemes, IEEE Commun. Surv. Tutor. 7 (2005) 72–93.
[92] M. Menth, M. Hartmann, M. Hofling, FIRMS: a mapping system for future internet routing, IEEE J. Sel. Area. Commun. 28 (8) (2010) 1326–1331, http://dx.doi.org/10.1109/JSAC.2010.101010.
[93] E. Lear, NERD: A Not-so-novel EID to RLOC Database, draft-lear-lisp-nerd-09.txt, 2012.
[94] D.L.V. Fuller, D. Meyer, LISP Alternative Topology (LISP–ALT), draft-fuller-lisp-alt-10.txt, 2011.
[95] R. Oliveira, B. Zhang, D. Pei, L. Zhang, Quantifying path exploration in the internet, IEEE/ACM Trans. Netw. 17 (2) (2009) 445–458, http://dx.doi.org/10.1109/TNET.2009.2016390.
[96] R.B.J. Touch, A. Mankin, The TCP Authentication Option, 5925, 2010.
[97] M. Bagnulo, A. Garcia-Martinez, A. Azcorra, BGP-like TE capabilities for SHIM6, in: 32nd EUROMICRO Conference on Software Engineering and Advanced Applications, 2006. SEAA '06, 2006, pp. 406–413. doi: http://dx.doi.org/10.1109/EUROMICRO.2006.25.
[98] Y.R.H. Ould-Brahim, D. Fedyk, BGP Traffic Engineering Attribute, RFC 5543, 2009.
[99] D.M.J.C.S. Brim, D. Farinacci, EID Mappings Multicast Across Cooperating Systems for LISP, draft-curran-lisp-emacs-00, 2007.
[100] D. Krioukov, k.c. claffy, K. Fall, A. Brady, On compact routing for the internet, SIGCOMM Comput. Commun. Rev. 37 (3) (2007) 41–52, http://dx.doi.org/10.1145/1273445.1273450.

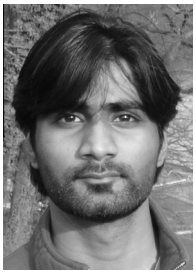
Wilson Ramirez got his Barchelor degree in Electronics and Telecommunications from INTEC University in Santo Domingo, Dominican Republic. He won a scholarship to study in the University Politecnica de Cartagena in Spain and obtained the degree of MSc in Information Technologies and Communications. He is a fellow of the fellowship program FPI of the Ministry of Science and Innovation of Spain for PhD studies, he is currently a PhD student of the program of Computing Architecture Networks and Systems at University of Catalunya, and is actively working on project ONE.

Xavi Masip-Bruin got a MSc and Ph.D. degrees in Telecommunications Engineering both from the Technical University of Catalonia. He is currently an associate professor in the computer science department at the UPC campus in Vilanova i la Geltrú. He is engaged to the Advanced Network Architectures Lab (CRAAX) where he is actively working in the areas of broadband communications, QoS management and provision, traffic engineering and multilayer networks, focusing on both packet and optical networks and lastly in the e-health area. His publications include around 80 papers in national and international refereed journals and conferences. He has also been member of the organizing team of many national and international conferences and also participates in many national and international research projects with public institutions and industries.

Marcelo Yannuzzi received a degree in electrical engineering from the University of the Republic, Uruguay, and the MSc and Ph.D. degrees in Computer Science from the Department of Computer Architecture (DAC), Technical University of Catalonia (UPC), Spain. He is currently an associate professor of computer science at UPC. He held previous positions with the Physics Department of the School of Engineering, University of the Republic, Uruguay, and with the Electrical Engineering Department of the same School between 1997 and 2003. He worked in the industry for ten years at the national Telco in Uruguay from 1993 to 2003. His research interests are in the areas of interdomain routing in IP and optical networks, cross-layer traffic engineering, overlay networks, route control and stability, pervasive and autonomic computing, e-health applications, and the design of novel network paradigms in support of e-health applications.

René Serral-Gracia received a degree, and recently his PhD in Computer Science from the Technical University of Catalunya (UPC) in the Department of Computer Architecture. Currently he is assistant professor in the same University, where his teaching activities are focused in Networking and Operating Systems Administration. From 2003 his research has been focused in topics such as QoS management and provision, traffic engineering, and IP traffic analysis and characterization. More specifically he actively worked in European projects such as Laboratories Over Next Generation Networks (LONG), end-to-end Quality of Service support over heterogeneous networks (EuQoS).

Anny Martinez received the degree of Electronic Engineer in the year 2008 from the Simon Bolivar University (USB) in Caracas, Venezuela. She developed her final career project in the Technical University of Catalonia (UPC), Barcelona, Spain in the optical network field. She served as software engineer in the Development Department of a voting solution oriented enterprise. She is a PhD candidate at the Advanced Network Architectures Lab (CRAAX) at UPC. Her research interests include future Internet architectures, multi-layer networks and ontology-based knowledge management. She is currently active in the European Project ONE: Towards Automated Interactions between the Internet and the Carrier-Grade Management Ecosystems.



Shuaib Siddiqui received his B.Sc in Computer Engineering from King Fahd University of Petroleum & Minerals (KFUPM), Saudi Arabia. He completed his M.Sc in Communication Systems Engineering from École Polytechnique Fédérale de Lausanne (EPFL), Switzerland. He also worked with the R&D department of CURRENT Group based in Switzerland where his study of scaling impact on throughput and latency at any point in the network helped CURRENT's Broadband over PowerLine (BPL) technology to better prepare for mass deployments. He also led the research on capability of BPL technology to stream video services to end-customers which proved fundamental for CURRENT's triple play service roll out. Currently, he is a PhD candidate at the Advanced Network Architectures Lab (CRAAX), where his research interests include Network Security, Inter-Domain Routing Protocols, and Performance Evaluation.