A survey and taxonomy of ID/Locator Split Architectures.

W. Ramírez, M. Yannuzzi, A. Martínez, X. Masip-Bruin, R. Serral-Gracià, E. Marín-Tordera.

***Abstract*—Addressing in current routing system faces a semantic overload. This semantic overload aggravates problems like the geometrical growth of the routing tables. Furthermore, it also affects traffic engineering and translation from a fixed network to a mobile network in terms of resilience and disruption tolerant communications. The importance of addressing for network operations requires a good understanding of the semantic overload problem and the efforts currently undertaken to counter it. Hence, in this paper we present a survey that introduces the concept of ID/Locator Split Architectures (ILSAs) as well a taxonomy of ILSAs. This taxonomy attempts to formulate a design space for evaluating and designing both existing and future ILSAs. Furthermore we analyze the benefits and weaknesses of existing ILSAs.**

***Index Terms*—ID/LOC separation, Internet addressing, Scalability, Naming, Internet Architecture, Future Networks.**

I. Introduction

IPV4 addressing scheme has almost reached the end of its lifetime and is unable to cope with the unprecedented growth of Internet. IPv6 was proposed to replace IPv4 several years ago but it is still in its early deployment phase. The hindrance in its adaptation is due to the reluctance of network providers to its deployment despite an abundance of research studies dedicated to the address exhaustion problem.

In a future Internet, also named as the Internet of Things (IoT), End to End security, mobility and multi-homing support are obligatory features rather than optional, contrary to the current Internet architecture. A migration is imminent and certain design considerations should be taken into account in the scope of IoT.

In order to migrate to an IoT model, where a plethora of heterogeneous devices will require connectivity, the problem of the semantic overload of addresses needs to be fixed. The current flatness and the semantic load of addresses limits the scalability of internet routing. Several research studies in this field argue that a scalable routing architecture, (defining scalability as a logarithmic growth of routing tables and control messages generated) cannot be accomplished without dealing with these two issues.

In this article we present a surveys that introduces the concept of ID/Locator Split Architectures (ILSAs) and describes a taxonomy, which is built from a collection of ILSAs proposals and earlier articles about this topic. We also illustrate the most prominent ILSA proposals, indicating the strengths and weaknesses of each one, with the aim of providing tools for the evaluation and design of ILSAs, for the purpose of stimulating their use in the Future Internet.

The organization of the papers is as follows. Section II briefly describes related works on ID/LOC Separation. Section III describes the shortcomings of the current addressing scheme. Section IV illustrates the preliminary concepts of ILSAs. Section V gives a taxonomy of ID/LOC proposals. Section VI, VII and VIII describe network based data planes, control planes and host based proposals, respectively. And finally, Section IX offers conclusions on the architectures described above.

II. Related Work

A comparison of ILSAs is presented in [1], but only focuses on network based solutions, and does not cover host based solutions. In [2] the first published survey on ILSAs literature is presented. It covers several ILSAs proposals and gives a taxonomy of each one. However it does not cover Host based proposals and ILSAs proposed recently.

A Review of IPv6 Multihoming solutions can be found in [3]. The authors analyze various architectures that can address multihoming issues concerning an IPv6 network protocol. It does not present an exhaustive classification of existing architectures and the work does not focus on the problems of a current routing system, other than multi-homing.

III. Where are we now ?

Since the early days of Internet, IPv4[4] has been the most widely used address format among others like IPX, and Apple Talk. The predictions about the exhaustion of the IPv4 address scheme are as old as itself [5-6]. Several thorough studies have been made to predict IPv4 address exhaustion, estimating dates ranging from (1990-2030). However, these predictions had scarce attention from the Internet community. In fact the scientific community has traditionally devoted more efforts to deal with interdomain issues [7-8] than to addressing itself, despite both are widely interconnected.

It was Geoff Houston's work [9] that recently showed that the expected depletion time was sooner than many organizations had expected. This concern has now received considerable attention in address-allocation policy circles. As a result of this, several clean slates addressing architectures were designed [10-14], and proposals with security and convergence speed improvements were proposed [15-17] as well.

However the scalability of the Internet is not an easy term to define. The Internet follows the small world pattern [18] and has the scale free properties [19]. These properties

This work was partially funded by the Spanish Ministry of Science and Innovation under contracts TEC2010-12250-E and TEC2009-07041, and the CIRIT (Catalan Research Council) under contract 2009-SGR1508.

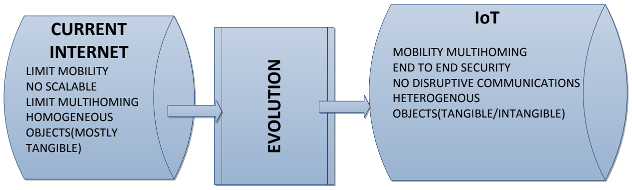


Figure 1. Evolution of the internet.

drive to the fact that the average path length of the Internet grows logarithmically according to the number of nodes in the network, $D = \frac{\ln(n)}{\ln(k)}$, where D is the diameter of the network, and n and k are the total number of vertices (nodes) and edges (links) in the Internet respectively [20]. The communication cost (the number of control messages) has a lower bound of $\Theta(n)$, where n is the size of the network. The upper bounds depends on the stretch factor [21], that is, for a stretch-factor of 3, the scalability of a routing system is $\Omega(\sqrt{n})$. According to [22], the average path length of the inter-domain level and Internet route level is 3.56 and 9.51 hops, respectively. This makes evidence that the Internet is growing super linearly in density but grows much lower in diameter. A recent study has concluded that the routing tables size, (not the convergence time of inter-domain routing system), is the one that needs to be addressed for a migration to an IoT. The main goal is to achieve a routing table growth factor of $\mathcal{O}(\log p)$, where p is the number of entries in the routing table. Hence the inferred conclusion is that a compact routing scheme should be a priority for migration towards IoT.

A. *Expansion of the Internet*

Initially Internet was not planned for large scale commercial use, as it is now, consisting of millions of hosts. Due to the recent technological advances, user-end devices are getting smaller in dimension with increasing demands of mobility and seamless connectivity round the clock.

Due to the exponential growth of possibly identified objects, more addresses have to be allocated to them, evolving the Internet into the IoT [23-26], see figure 1. Unfortunately, 32 bit IPv4 addresses cannot cope with the requirements of IoTs in many aspects, including addressing. Many workarounds and extensions have been proposed and deployed to defer the exhaustion of IPv4 addresses. Techniques like private address blocks, NAT (Network Address Translator), gave a work around to the exhaustion of addresses in IPv4, but in the same way introduced new problems like inability to measure clients, address space hijacking and difficulty in the deployment of NAT sensitive protocols, such as SIP, and IPsec.

More than fifteen years ago, next generation Internet Protocol group (IPng) [27-29] started to develop IPv6 [30]. The proposed 128-bit length IPv6 addresses were planned to provide enough addresses to handle the growing number of hosts. However, there is a reluctance of network operators to adopt IPv6, mainly due to the difficulty of migration tasks.

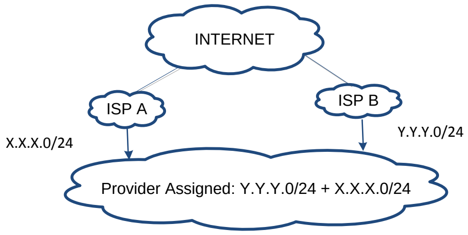


Figure 2. Multihoming scenario.

B. *Multihoming.*

In recent years, routing tables sizes in the Internet have grown super-linearly being multihoming is one of the main reasons. Multihoming has become an essential requirement for users, as it assures a service with fault tolerant capabilities. In fact, the decreased cost of Internet connections has encouraged users to opt for multihoming.

Multihoming is defined as a site having more than one connection to the Internet. Multihoming can be implemented at two different levels: host level and site level. At host level, a host has two or more independent connections to the Internet (see figure 2). At site level, a site has two or more connections to the Internet. In the latter case, hosts are usually unaware of the existence of multiple Internet connections.

To achieve multihoming, a site acquires a provider independent (PI) or provider aggregatable (PA) prefix from its providers. It then announces them through all of its providers. A multihoming site using PI address space, has its prefixes present in the forwarding and routing tables of each of its providers. For PA prefixes, each prefix allocated from each provider address allocation will be aggregatable for that provider but not with other providers. Now for multihoming an ISP has to advertise a site's more specific IP routing prefix to the Internet and rely on the traditional and problematic longest-prefix match route selection algorithm.

De-aggregation of prefixes due to multihoming have contributed to the growth of routing table size[31-32].

C. *Traffic Engineering.*

Traffic engineering (TE) can be defined as the practice of defining how paths should be used or avoided for a certain type of traffic. TE overrides the path selection of routing protocols, hence is used by ISPs for efficient utilization of network resources, and to reduce network operation costs. But unfortunately with the tradeoff of an increase in the DFZ RIB tables in routers.

There are other problems that indirectly affect Internet routing, such as lack of aggregation, hardware constraints (memory of the routers cannot scale faster than the size of the full routing table).

IV. Preliminary concepts of ILSAs.

ID/Locator Split Architecture is not a new topic in network research. This idea has been contemplated for a while as a necessity to face the problems in the routing architecture. The

ID/LOC concept was first introduced by Noel Chiappa [32] to counter the problems in the addressing architecture, described in section III.

Before going into detail about ILSAs, it will be helpful to define related terminologies and concepts.

A. *Terminology and Concepts.*

In this article have been discussed the semantic overloading of IP address, used for both identifiers and locators (addresses). A question to ask is how to define and set the boundary between an identifier and a locator. For this is important to define the following concepts:

Identifier: *A name attached to a network element (tangible or not) that differentiates it from among a collection of entities.*

An identifier (ID) answers the question “who”. Identifiers are used to identify entities in a way that they are independent of the current location of a host (unlike the case in the current routing architecture) [33-34]. An analogy of an identifier can be a person’s name. An ID should be unique. Thorough discussion on the uniqueness of an identifier is done in [35]. Another point to consider is the format of an identifier. A flat identifier (or primitive identifier) has no internal structure and no information can be deduced about the identified object by just looking at its ID. UUIDs described in [36] are an example of primitive IDs. On the other hand, the format of an identifier can be partitioned (or descriptive) [37]. A partitioned identifier has some restrictions over its imposition and hierarchy. Partitioned identifiers have semantic information contrary to flat identifiers. An example of partitioned identifiers are URLs [38].

Identifier Space: *A collection of valid IDs.*

Locator: *The name use to locate the presence of an entity in the network.*

An address or locator answers the question "where". An analogy of a locator can be made with the postal address of a person. A person will always have the same name but can have several addresses over a period of time (for example if he moves).

It is almost a standard model to attach the transport layer to an Identifier and the network layer to a locator (see figure 3). This opens the possibility to support mobility and fault tolerance communications, which will be discussed in a later section.

Locator space: *The collection of valid addresses.*

Mapping System: *The entity who performs the mapping between an identifier and a locator and vice-verse.*

V. Classifying ID/LOC Split Architectures (ILSAs).

ILSAs can be classify in two sets. One set that works in a network based scheme and the other set that works in a host based scheme. Another study describes this approach as a name space, invisible or visible to hosts [39].

Network based scheme architecture works at network level, usually at the customer edge of the network, adding some changes to the network nodes but not to host nodes. Network based schemes can be further divided according to their operation over control plane or data plane. The data plane proposals can be broadly categorized into: map-encap and address rewriting. On these proposals the mapping phase (the action of mapping between identifiers and locators) is done over the data plane. Examples of network based schemes that operate over the data plane are LISP[40-41] and its variants, Six/One [42], etc. Control plane proposals offer a mapping architecture that operates over a control plane, separating in this way the mapping phase from the data plane. This mapping architecture may belong to different *flavors* based on : DNS, DHT, Dedicated/Hierarchical database or Routing protocols(see chapter VII).

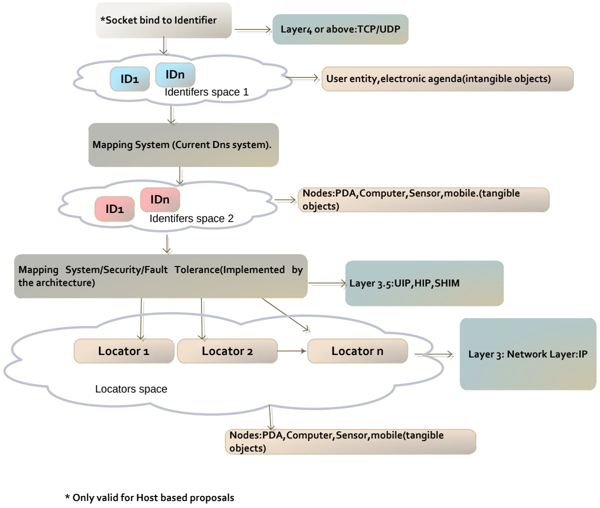
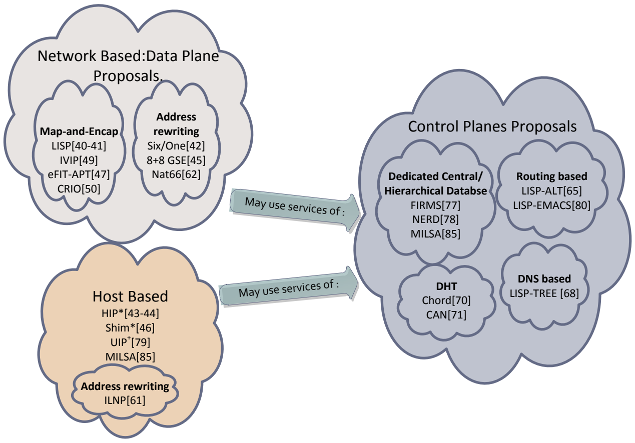

*Socket bind to Identifier
Layer4 or above:TCP/UDP
ID1
IDn
Identifers space 1
User entity,electronic agenda(intangible objects)
Mapping System (Current Dns system).
ID1
IDn
Identifers space 2
Nodes:PDA,Computer,Sensor,mobile.(tangible objects)
Mapping System/Security/Fault Tolerance(Implemented by the architecture)
Layer 3.5:UIP,HIP,SHIM
Locator 1
Locator 2
Locator n
Layer 3: Network Layer:IP
Locators space
Nodes:PDA,Computer,Sensor,mobile(tangible objects)
* Only valid for Host based proposals

Figure 3. Binding of layers after split IDs from LOCs.

Host based schemes require changes at the host node. A new layer is introduced (layer 3.5) between transport layer (layer 4) and network layer (layer 3), see figure 3. Host based proposals may also use map-encap or address writing procedures. Just as well, divide the data plane from the control plane. Another characteristic of host based schemes is that one or more ID spaces could be used. This ID space may have the same syntax of the old ID space. Upper layers are bound with ID spaces and network layers are bound with locators (addresses) Host based schemes offer end-to-end security and multihoming without the network being involved. Examples include HIP[43-44], GSE[45], and SHIM6 [46], see figure 4.

Most Host based ILSAs allow using one or more ID spaces and one or more locator‘s space. In all architectures there is a bidirectional mapping between an ID and a locator ($ID \Leftrightarrow LOC$). Other ILSAs map between ID spaces ($ID_{s1} \Leftrightarrow ID_{s2}$). In conclusion, an ID can be mapped to another ID belonging to a different ID space or it can be mapped to a locator. That is, an ID can have one or more locators or one or more IDs. The Locator’s space is greater than the ID space and, there can be more than one Locator‘s space, e.g. one for global routing and one for local routing.

The concept of separating identifiers from locators, contemplates the ideas of mobility/roaming, renumbering (change of provider). Also an identifier can be assigned to an abstract



* Use a DNS based Control palne.
+Use a Hierarchical Control plane

Figure 4. Taxonomy of ILSAs.

object, an entity that covers all possible tangible objects of a user. The semantic separation in host based ILSAs is not as clean as in network based ILSAs. For network based ILSAs, locators and identifiers have same format, this creates difficulties at the time of separating identifiers from locators. In host based ILSAs identifiers are never used for locating an object, they are used for identification, as discussed in section IV, therefore the concept of splitting the semantic loading of addresses is done successfully.

VI. Network based. Data Plane Proposals.

A. Map-Encap.

Map-encap proposals make use of the tunneling concept. A similar concept is used in locator identifier separation protocol (LISP), eFIT [47], IPvLX [48], Internet Vastly Improved Plumbing (IVIP) [49], and CRIO [50]. All these proposals are map-encap proposals and are inspired by the work described in RFC 1955 [51].

In these schemes, there are two address spaces, one is used for intra-domain routing and other for inter-domain routing. In LISP terminology, they are called EID and RLOC, respectively. Map-encap operates in two phases. In first phase, for a packet destined outside the boundaries of the sender´s domain, the border router, known as the Ingress Tunnel Router (ITR), maps the EID to a RLOC, that corresponds to the border router of the destination domain, called the Egress Tunnel Router (ETR). A router can have a map entry on its own or can obtain it by consulting an external mapping system or by using routing protocols to embed the mapping queries in the routing message(discussed in section VII). The second phase consists of encapsulation of the packet, by adding RLOC as the destination address. The tunneling phase works for any kind of address. In all map-encap proposals, the source address may be treated differently, and may or may not be mapped to an RLOC in the encapsulated packet.

The process at the destination domain is similar. When the packet arrives at the destination domain, the ETR looks up the respective mapping from a destination RLOC to a destination EID and sends the packet to the node that has the destination EID.

It's not necessary that every destination RLOC is a border router in the destination domain, it can be the address of an intermediate router. In that case the intermediate routers change the destination RLOC for a new destination RLOC.

Advantages: map encap proposals offer a good vision when it comes to the scalability of current Internet routing. Among the benefits offered, are the following:

• No changes are required at the hosts
• Minor changes are needed in the routing system
• No need for the renumbering of edge networks
• Transparent interoperation between different addresses formats
• Reduced size of routing tables [52-53]
• Facilitates Traffic Engineering in inter-domain routing

Open Issues:

• No support for end-to-end security
• Increased overhead burden due to encapsulation [54-55]
• Does not scale up for Full Mobility Support
• Fault tolerance

These disadvantages represent a considerable limitation to the implementation of map-encap proposals in the current internet architecture. For example: Fragmentation and reassembly of packets are not feasible in the backbone, Fragmentation raises several problems, such as slow path processing in routers, and missassociation of fragments of multiple IP packets during reassembly tasks.

Also mobility is not well covered. Although efforts have recently emerged to overcome this problem, for example, there are extensions to LISP for Mobility support [56-58]. The central idea is the interaction between LISP and Mobile IP. But keeping the mapping table updated and the required double encapsulation pose cumbersome challenges.

Another limitation is resilience and survivability. The current LISP and other map-encap proposals, do not take failure of network elements into consideration [59].

B. LISP.

LISP[1] (locator identifier separation protocol) is a proposal in development by IETF with substantial support of Cisco, LISP fits in map-encap proposals. Its goal is to address scalability problems in routing system.

LISP only defines the messages to query the Mapping System, leaving the door open for proposals of the Control Plane.

The messaging of LISP is composed of the following:

- Data Probe. A message sent to an ITR for a request a map entry.
- Map-Request. Is a message sent by an ITR to a mapping system to query a map-entry.
- Map-Reply. A message that is sent by an ETR in order to respond to a Data probe or a Map-Request.

[1] not be confused with the programming language lisp

At present LISP can work in a unicast or a multicast scenario, but to implemented LISP in whole internet, cannot be done from scratch, some kind of interworking is needed with the current internet here are two basics Techniques for this purposes, **Lisp network address translator**, and **Proxy Tunnel routers (PTRs)** [60].

Related to security issues, DNSsec and SBGP can be used to overcome weakness of the integrity of a system. In implementations terms, LISP is right on the corner for a future Cisco IOS implementation, so it will not be surprising to see LISP as part of Cisco CLI.

C. Others network based map-encap proposals.

eFIT is another proposal to accomplish scalable Internet routing and addressing. As in LISP, it also utilizes the concepts of tunneling and mapping.

eFIT drastically separates user network from the transit network, in such way that there is no routing protocol operating between the two domains, with each domain having its own address space.

eFIT can be seen as islands of user networks which are connected to each other by highways namely the transit networks. Transit networks only have to learn the addresses of other transit networks. Consequently, making routing tables small, and with this strategy, the routing tables in transit networks are not affected by the user network activities, like multi-homing and traffic engineering.

eFIT uses two approaches to implement the mapping system. One is the use of flooding by transit services providers (border routers), this approach does not scale up due to the number of messages that can be generated. The other approach is the use of distributed servers, like a DNS system, doing a hierarchical implementation, or a more decentralized architecture like DHTs.

CRIO and IPvLX are also network based ILSAs that use map-encap for their operation. They have the same principles as LISP or eFIT. IPvLX is more inclined towards co-existence of IPv6 and IPv4 and it defines a new method of encapsulation. On the other hand, CRIO is more agnostic referring to a locators format and its use of GRE for encapsulation.

D. Address Rewriting.

Address rewriting schemes are based on a similar concept as that of Networks Address Translation (NAT). Instead of using tunneling that adds much overhead to packets, rewrite schemes, as the name suggests, rewrite the address of a packet. Many proposals divide the format of an address into blocks. One block is used for host identifiers, and the other block for locators.

ILNP [61], Six/One [42], and GSE 8+8[45] are address rewriting proposals. All of them are very similar in their operation. A distinction has to be made with ILNP, that it is based on address rewriting but it requires changes on the host layer. So, it is really a host based ILSA. This will be further discussed in section VIII.

The idea behind address rewriting schemes, was originally proposed by Dave Clark and later by Mike O´Dell [45]. The idea was based on taking advantage of 128 bit IPv6 addresses and using the top 64 bits as the routing locator (known as routing goop, or GR) and the lower 64 bits for the endpoint identifier.

SIX/ONE is different in the way that it uses an extension header, including packet's original source and destination addresses, to help remote Six/One routers to translate a packet back into its original state. Six/One is compatible with a variety of mapping systems (see chapter VII for control plane proposals).

Like LISP, Six/One separates address domain into Local addresses and global addresses. Destination addresses of incoming packets are always translated into edge addresses; source addresses of outgoing packets are always translated into transit addresses allocated by the provider via which the packets are sent. To indicate to a remote Six/One router whether and how to translate a packet back into is original, Six/One routers endow outgoing packets with a Six/One extension header including the packet's original source and destination addresses. It is evident that the only difference compared to LISP is that Six/One rewrite addresses and LISP leaves the addresses untouched by using an encapsulation method.

Other architectures like NAT66 [62] employ the rewriting method as well. But there is no implementation of NAT66 available at the moment.

E. Comparisons between Map-encap and Address Rewriting.

Both, map-and encap or address rewriting schemes, achieve splitting locators from identifiers, but each one brings advantages and disadvantages for accomplishing this.

Scalability: For map-encap proposals, the size of the mapping table can pose a burden on the memory of the border routers, this also could affect address rewriting schemes. Control plane proposals may handle this issue but its performance, in terms of the resolution time and required signaling overhead, is unclear. Perhaps DHT mapping systems can obtain better performance due to logarithmic behavior.

Adaptability: Address Rewriting schemes, such as GSE, have limited issues with multicast scenarios. Also the majority of address rewriting architectures, assume IPv6 as the basic format of addressing, which poses limits in terms of adaptation and scalability.

Mobility and Renumbering: Address rewriting schemes, such as NAT66 and GSE, do not support mobility of user nodes. Also renumbering of the nodes without impacting the communication is impossible. However, this is not true for other address rewriting schemes, like Six/One, which supports renumbering due to its adaption of different mapping systems. This also stands true for the tunneling approach.[2]

Fault Tolerance: Reachability and reliability is major weakness on both approaches [58].

Security: Security features are more difficult to implement in address rewriting schemes. In the case of Six/One and LISP, security relies on the mapping system.

[2] In the case of LISP is valid if the is a mapping system implemented.

VII. Control Plane Proposals

ILSAs belonging to this category utilize a control plane for the mapping phase. This also applies to map-encap proposals but not to address rewriting proposals because in such schemes the destination address usually resides in the DNS. A Mapping system, in its basic form, acts as a database where the key is an identifier and the result is a locator.

There are many types of mapping systems:

- **DNS based.** Utilize a similar infrastructure as of DNS system.
- **DHT based.** Utilize basic operational concepts of DHT networks.
- **Dedicate/Hierarchical database.** Centralized or Decentralized database servers gather the mapping entries.
- **Routing based.** An overlay is built on top of a routing protocol for the mapping phase.

Another characteristic that can be used to classify mapping systems is the distribution method (*push or pull*). Push methods are proactive, and in defined periods of time, mapping entries are propagated to ITRs. Pull methods are reactive. A request is made and then the corresponding entry is retrieved. A tradeoff between each model is related to lookup latency, signaling overhead and the amount of states. Push methods offer short lookup latencies and signaling overhead but the number of states grows, limiting the scalability of this approach. There are large mapping databases on the ITRs. Pull methods are the inverse of push. Fewer number of states but higher lookup latencies and signaling overhead. We discuss and present proposals for each category below. Despite different types of mapping systems, the metrics used to evaluate their performance are the same. These metrics are:

- **Query processing time.** Represents the number of queries per unit of time that a Mapping system can handle.
- **Bootstrapping time.** It is the time required for an empty database to reach dynamic equilibrium state.
- **Size of the mapping table.** Represents the dimension of the mapping table, as the numbers of entries saved in the mapping system.
- **Mapping Resolution Time.** Perhaps the most important metric related to performance. The mapping resolution time (T_{map}) can be defined as the elapsed-time between submitting a query to the Mapping System and obtaining its response.
- **Hit miss ratio.** It is a metric related to the accuracy and feasibility of the Mapping System. It represents the number or successful query responses, of the total queries submitted to a Mapping System.

In the following paragraphs, the performance of different types of mapping systems according to the metrics stated above will be discussed

A. DNS based Control Planes.

DNS based control plane proposals follow similar design principles as of DNS systems. These proposals can be considered the most concurrent with the current technologies in terms of deployment, because DNS mapping systems are widely implemented and are pragmatically scalable. According to [63] there are $130\text{x}10^6$ domains on the internet, more than the total entries of the default free zone (DFZ), that is around 400,000 [64]. According to established results about the performance of DNS systems, using them as mapping systems for an ILSA seems feasible, but migration to an IoT should be considered.

Some hurdles are presented when using a DNS architecture as a mapping system. One could be security, but recently there are DNS extensions like DNSSEC that could mitigate security issues. Giving the ITRs the ability to validate and authenticate responses received by the mapping system. Another obstacle of these approaches becomes prominent when resolution time comes into the picture. [65] shows that 30% percent of the time to retrieve a web page is expended in the resolution phase inside the DNS system. [66] shows that resolution time for the 30% of the queries sent to DNS systems is around 2 seconds. The poor performance is mainly due to low cache hit rates, stemming from the heavy-tailed, Zipf-like query distribution in DNS. It is well known from studies on Web caching that a scale-free heavy-tailed query distribution severely limits cache hit rates, that is, 23% of the total of lookups are not answered and 13% of lookups are answered with errors. Also the hierarchical nature of DNS can result in hot spost for popular entries, which is not viable for any domain. Another limitation is the problem for maintaining the mapping entries consistency when the entries are changing. This condition of change will be more drastic in a ID/LOC scenario because nodes are more probable to change their ID due to migration to a new ISP provider or due to roaming.

LISP-Tree [67] is a DNS based mapping systems. They separate the storage of the mappings and the discovery of an entry. XTRs store the entries, which, as mentioned earlier, limits the scalability of the XTRs memory. The discovery mechanism is built on top of DNS systems, which makes it susceptible to the same flaws of a DNS system.

In [68] they propose a DNS based control plane for LISP. Their goal is to prevent the potential dropping of packets at the ITRs, while the EID-to-RLOC mapping resolution is being computed by maintaining the mapping resolution time equal to zero. They try to achieve this by merging the DNS resolution phase and the mapping resolution phase together ($T_{map} + T_{dns} \cong T_{dns}$).

From the discussed above there are some open issues and advantages that can be deduced for a DNS based control plane.

Open Issues: There are doubts as to weather a DNS based proposal can deal with scalability issues and minimize the T_{map} in an IoTs scenario; Others features like mobility seems to be a distant goal for the reach of DNS based control planes.

Advantages: DNS is a well probe system.Which is not prone to configuration errors from spreading and impact outside the boundary of a domain served by a misconfigured name server (contrary to Routing based Control Planes).

B. DHT Control Planes.

Distributed hash table (DHT) systems like Chord [69] and CAN [70] have been successfully implemented and well received for P2P applications. One main reason is their resolution time performance, $\mathcal{O}\log(N)$, where N is the number of nodes in the DHT. Nevertheless there are characteristics that make them unviable to be used as a mapping systems on ILSAs. One of them is that the key value pairs are randomly distributed on DHT. This is done for avoiding hot spot points. But this can be troublesome for a manager of a domain, cause he may wish to control the server that provides the authoritative mappings for the identifiers allocated to its hosts, this is done mainly for traffic engineering purposes. When a node joins the DHT network, the key space is divided and redistributed, which is not suitable for the authorities for reasons described above. Another characteristic is the lack of security in DHT networks that makes them very unattractive for Mapping Systems, mainly because the need for trust on the information provided by the Mapping System to avoid hijacking of the mappings. Another design constraint of DHTs is the lack of geographical proximity. Two nodes which are neighbors in the DHT can be geographically apart in the underlying network. So a domain in Spain can be requesting a locator for an ID from a domain in France. Business and political interest can conflict with this issue. DHT proposals like [71] address the authoritative issues earlier described. In [72] they use Chord for their DHT network and their proposal is not generic, and is based on a LISP environment. [73] also uses DHTs for mapping systems They based their architecture on the CAN algorithm. Systems like [71] implement DHT with notion of space, hence minimizing the expense of resources of the underlying network. Another implementation of DHT as Mapping Systems can be found in [74].

The following conclusions can be deduce of the discussed above.

Open Issues. There are many DHT algorithms available but which one is best for Mapping Systems in ILSAs, remains an open question. Issues like reliability and resilience pose further difficulty. Mobility of the contents represents another obstacle. ID/LOC pairs tend to change because users change providers frequently. Another constraint is the expensive cost of using underlying network resources on DHTs [75].

Advantages. On the other hand, performance of the DHTs is usually around $\log(N)$ and the size of the mapping tables are around $\log(p)$, where p is the number of ID/LOC pairs in the DHT. Also they can be easily adapted to any addressing scheme (not only to IP as it usually happens with DNS). These characteristics also make them attractive in scalability and adaptability terms.

C. Dedicated Central/Hierarchical database.

Dedicated databases require an elevated cost in Opex and Capex for a Network Operator. The use of dedicated nodes as mapping resolvers and as mapping databases, represents the paradigm in this type of control plane. This approach is the simplest of all control plane approaches. FIRMS [76] is one such proposal. But the absence of results, related to T_{map} and scalability makes it unviable.

LISP-NERD [77] is another dedicated database approach. It recommends the existence of a central database managed by a central authority. This database collects all mapping entries. Following a push distribution model, these entries are pushed on to the ITRs of each domain. ITRs update these entries using HTTP based messaging at regular time intervals. The advantages of LISP-NERD are inherited from the push distributed model along with the scalability issues of the central database models (scalability in terms of memory consumption on the ITRs). The time interval required for long bootstrap operation also poses a limit to this approach.

Other proposals like UIP [78] follow a hierarchical approach. A traditional hierarchical database is the legacy telephone system, it uses hierarchical telephone switches (class 5, class 4 and class 3). In the case of UIP each level of the hierarchy maintains the state of their respective entries between the boundaries of their domains. If it requires an entry, which is not found in its domain, it will consult the upper levels to retrieve it.

These open issues and advantages can be deduced for a Dedicated Central/Hierarchical database based control plane.

Open Issues. High cost in Opex and Capex. Also problems to deal with scalability.

Advantages. These systems have a low mapping resolution time.

D. Routing based Control Planes.

Routing based approaches use alternative topologies or overlays for the control plane, as in DHTs, the mapping entries are transported using a routing protocol running on the ITRs of each domain. Contrary to DHTs, the overlay follows a hybrid of push and pull distribution models. That is, IDs are announced to every node on the overlay (push) and when a mapping is required, it is requested to the overlay (pull).

LISP-ALT [79] is a Routing based approach. It uses BGP on top of GRE tunnels to propagate ID prefixes. LISP-ALT, as the name suggests, is only based on LISP and it is not generic to any other architecture. LISP-EMACS [80] is another Routing based approach, it proposes the use of PIM as the routing protocol to propagate ID prefixes.

The following conclusions can be deduce of the discussed about routing based control planes.

Open Issues. Doubts arise about whether it is feasible to use BGP, as the protocol to propagate IDs prefixes to the ITRs. LISP-ALT inherits all the flaws of BGP, like slow convergence and weakness against failures. The Internet has many flaws using LISP-ALT and its alternate topology will cause a parallel internet with the same flaws like the first one.

Advantages. Soft adaptation due to existing technologies.

E. Comparisons about control plane proposals.

In table 1, a comparison of the different categories of control plane proposals is shown. Control overhead, resolution time, scalability, bootstrapping time, security and fault tolerance are the metrics used for the evaluation. It can be observed from table 1 that DHTs offer better results. But the limitations explained in section VII.B, state constraints for their adaptability.

The Control Overhead metric is related to the amount of information generated to obtain a mapping and assuring consistency of the mapping entries and the control plane topology. The DNS and Routing based proposals observed more control overhead information. Assurance for topology consistency and mapping entries can result in a large volume of messages for Routing based proposals. This volume is lower in Central DBs because the information and infrastructure is under administration of a single entity. For DHTs, the need to maintain consistency for control overhead can be high but it is usually lower when a resolution request is made.

Central DBs and Routing based proposals experience more problems with scalability. For Routing based proposals, the size of the routing tables grows linearly with the number of mapping entries and the case is similar with Central DBs. DHTs put an equal and scalable routing burden among routers (ITRs). If the number of mapping entries is p, each router would have $\log(p)$ entries. DNS scalability problems become more drastic with the increasing request for mapping entries. Another limitation of of DNS based control plane proposals is that due to the hierarchical topology of the DNS system, hot spots may exist , which would in turn overload the ITRs that receive a high volume of mapping requests.

In terms of security DHTs and Routing based control planes are the more susceptible, compare to DNS/Hierarchical DB that are more robust. The total opposite occur at time of comparing taking in account the fault tolerance metric, where DHT are the more robust and Central/Hierarchical DB are the more susceptible.

VIII. Host Based Proposals

Host based proposals push all the complexity to the host. There is a middle layer acting as an intermediate between application/transport layers and network layers. Configurations are not needed in the network elements but they are needded in the applications, hosts, services and protocols. As in network based proposals such as LISP, the idea for host bases proposals remains untouched. Host based proposals force the application layer to use a different addressing scheme than network layers use. This feature enables more easily End to End security compared to network based approaches. HIP [43-44], SHIM[46] and UIP [80] are host based proposals. All of them assume than the network address scheme remain the same; They introduce a new upper layer scheme for application use.

As mentioned before host based proposals make communication fault tolerance intrinsically. This is so because transport layers such as TCP and UDP make their socket connection using upper layers identifiers and not IP addresses as traditionally is done in IP layers. Making in this way a resilient communication against lower layer failures. Mutihoming is also support intrinsically and naturally. Since the application layer is agnostic about lower layers interactions.

A. HIP

One of the most supported host based ILSA is **HIP**. As a Host based ILSA, in HIP, the location of the host is bound to IP addresses. The network layer uses the IP addresses for its operation. The higher layers are not bound to the IP addresses. Identifiers of 128 bit length are used for higher layer operation. HIP focus on end-to-end security, mobility and multihoming. The host identifiers have certain characteristics. (1) They are location independent. (2) They are based on public key cryptography. (3) A DNS or DHT is used to obtain the identifier of a host. (4) They can have a length of 128-bit long, if it is used as the medium to authenticate a host. There are many implementations for HIP: OpenHIP, HIP on linux, InfraHIP, pyHIP, HIPL, etc.

Open Issues: No support for traffic engineering.

B. SHIM6

SHIM6 was designed for a multihoming solution. This solution relies on a new sublayer inside the IP layer, the SHIM6 sublayer translates the locator to a constant address used by the upper layers. This constant address is called the upper layer identifier (ULID). Contrary to HIP, ULIDs can be used as locators, i.e. they are routable. The mapping between ULID and the corresponding locator is done using a DNS system. Therefore it inherits all the shortcomings of DNS based control plane, as described in section VII.

In addition to Multihoming, Shim6 also adds security and fault tolerance capabilities. The security relies on the usage of Hash-Based Address (HBA) and/or Cryptographically Generated Address (CGA). The Fault tolerance capabilities rely on a protocol namely REAP [81]. REAP detects path failure in the communication and determines the new path to be used for each unidirectional path. Apart from these features, there are two very important additional features of SHIM6. They are Context forking and Context recovery. Context Forking allows a host to fork an existing SHIM6 context into two; enabling communication resilience. Context recovery allows a context that has been lost in one of the hosts to be recovered. With these last two features the recovery and resilience is left on the client side.

Open Issues: No mobility support yet contemplated on the architecture. Also it is not generic to any network scheme used. Only valid for IPv6 addresses.

C. Others.

UIP (User Identifier Protocol) is a host based proposal with a versatile and natural support for roaming, multi-homing and site renumbering. This architecture defines two identifier spaces: user ID and device ID, and one address space: locators. A user ID is a globally unique identifier, which identifies a user's device. This user ID covers all possible sets of devices, an entity (person, company) can have. Each of these devices, has a device ID that identifies them in the network. Each device ID can have many locators (IP addresses) for making them reachable through the network. The two levels of identifiers make UIP architecture more versatile and user oriented. This fits well in the current Internet where users have more than one device for internet connection. A possible speaker does not care about establishing a communication with a particular device, but just needs to establish a communication with a user without any knowledge of the user´s location or device used. UIP defines two types of locators: Local locators and Global locators. Local locators are used to locate nodes

Table I
COMPARISONS OF CONTROL PLANE PROPOSALS

	DNS	DHT	CENTRAL/ HIERARCHICAL DB	ROUTING BASED
Control Overhead	High	Med	Low	Low
Scalability	Low: N	High: Log N	Low:P	High. N (best), P (worst)
Bootstraping Time	Med	Med	Low	High
Resolution Time	High	Med	Low	High
Security	Med	Low	High	Low
Fault Tolerance	Low	High	Low	Med

inside a domain and global locators are used for interdomain communication. This extends the address space lifetime, e.g IPv4 exhaustion issue can be deferred.

UIP mapping system, contrary to SHIM and HIP, is not based on DNS system. It uses a hierarchical database mapping system, as we explained in section VII.C. This mapping system approach can have issues related to availability and reachability.

Open Issues: In UIP, either the size of the identifiers or locators space is defined. No references, whatsoever, if the identifiers will have semantic information. Also no evaluation information is presented.

Hierarchical Routing (HRA) [82] is another host based ILSA, HRA borrows some ideas from SHIM6 and HIP. Unlike in HIP, identifiers in HRA are aggregable. A portion of the identifier is used to identify the country, another portion identifies the authority and the region of the user. This separation can aim the routing process. Locators are also aggregable, which are 128 bit length, of which 96 bits are used to identify the user domain, and 32 bits are reserved for IPv4 address. HRA uses two approaches for mapping system. A DNS based for mapping of host names to HRA identifiers and a hierarchical DHT based mapping system for the mapping of HRA identifiers to locators. By doing so, HRA is not changing the operation at the application level of the current internet, keeping DNS untouched, and introducing DHTs as the mapping system inside the HRA architecture.

Open Issues: It is not defined which host will participate in the Hierarchical DHT of HRA. Furthermore the hierarchical DHT algorithm is not defined and no performance evaluation has been conducted.

The Internet follows small-world phenomenon and scale-free properties. Hierarchical routing advantages [83] are not effective in the current Internet [21].

ILNP (Identifier-Locator Network Protocol) is a rewriting scheme that has its roots in GSE 8+8. The paradigm of ILNP, as other similar architectures, is that a clean-slate approach is not realistic. ILNP assumes IP address format. There are two flavors of ILNP, ILNPv4 for IPv4 address and ILNPv6 for IPv6 address. For the latter case, the 128-bits of an IPv6 address are divided into two blocks of 64 bits each. One is used as a locator (only routing) and the other as an identifier (node identity). The identifier block is used by upper layers (TCP, UDP). Comparing ILNP vs Six/One, ILNP is more robust in terms of security. This is because the IPSec protocol is supported in ILNP. Another difference is that ILNP encourages the use of FQDN names instead of IP address for future migration plans of the addressing scheme.

Using the classification scheme of host based and network based presented in this article, ILNP can be considered as a host based ILSA as well. No changes at the network level are required. The core remains unaware of the operations running in the background. So ILNP can be considered as a hybrid of both, host based and network based schemes.

Others proposals of host based ILSAs can be found in [84-85].

D. Host based vs network based

As we mentioned on the previous chapter, the main difference between host based and network based ILSAs depend on the implementation. Network based ILSAs require product modifications only on border routers, unlike host based ILSAS which require modifications to he host, applications, service and protocols, depending of the architecture. The functionalities of network-based ILSAs fall more closely to the network layer. Due to this reason network TE actions are easier to implement. In a network scenario using LISP, TE actions are stronger comparing it with BGP. The same case but with HIP or SHIM6 TE actions are even harder to implement.

On the other hand as host based proposals are more far way from the network layer, upper layer functionalities as security are easy to implement.

However is our belief that host based and network based proposals are complementary rather than competing.

IX. CONCLUSIONS

A. Is ID/LOC separation the best solution ?

In this paper, we have provide a taxonomy that attempts to capture a design space of both current and future ID/Locator Split Architectures(ILSAs). In order to provide a formal structure to our discussion and guide the reader through this document, we defined and gave a set of terminology and evaluation criteria that are important to any ILSA. We also brought out the strengths and weakness of each proposal toward the goal of an Internet of Things.

The debate is open for selecting the architecture for an IoT that bring a scalable routing architecture. On [21] discus that (ILSAs) are not the best approach for a scalable routing system. They expose that: The aggregation impose (ILSAs) are not effective on scale-free networks such as internet. They also argue that the task of maintaining updated the mapping entries up-to-date will make the scalability of the system difficult. We disagree on the first point cause it is proven ILSAs cannot improve the uppers bounds of the routing system but can leverage and enhance the routing functions leaving the door open for multi-homing, mobility (at least nomadic), end-to end security, and reducing the routing table´s length. We agree on the second point in the sense that the Mapping Systems are the crucial component of ILSAs. However we think that an ID/LOC separation with a scalable Mapping System are the combination for the evolution to an IoT.

Others like [10,11,13,86,] propose clean slate architectures. They impose a new addressing and routing scheme. We think that the disruption and migration constraints of clean slate architectures makes them unwary at the time of implementation. Adaption and not migration is what has to prevail when thinking in an IoT. However our assessment is that if the locator space can be change, locators with a semantic meaning, e.g: topology aware will guaranty a logarithmic behavior of the entries of a Mapping System.

REFERENCES

[1] H. Naderi,E. Carpenter, “A review of IPv6 Multihoming Solutions”, ICN 2011: The Tenth International Conference On Networks. January 23,2011,145-150

[2] L.Burness, P.Eardley, S.Jiang, X.Xu, "A pragmatic comparison of locator ID split solutions for routing system scalability," Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on , vol., no., pp.1024-1028, 25-27 Aug. 2008.

[3] D.Meyer. “An overview of Current IETF Activity on Routing and addressing models for the Internet”,Cisco Systems,2008.

[4] Internet Protocol, RFC 791, Defense Advanced Research Projects Agency Information Processing Techniques Office,1400 Wilson Boulevard, Arlington, Virginia 22209,1981.

[5] L. Cittadini, W. Muhlbauer, S.Uhlig, R.Bush, P.Francois, O.Maennel, “Evolution of internet address space deaggregation: myths and reality”, IEEE J.Sel. A. Commun. 28, 8 (October 2010), 1238-1249.

[6] Murphy, Niall and Wilson, David, "The End of Eternity Part One: IPv4 Address Exhaustion and Consequences," The Internet Protocol Journal, Volume 11, No. 4, December 2008.

[7] G. Huston, “The Changing Foundation of the Internet: Confronting IPv4 Address Exhaustion”, Internet Protocol Journal, Vol. 11, No. 3, Sept. 2008.

[8] M. Yannuzzi, X. Masip-Bruin, O. Bonaventure, "Open issues in interdomain routing: a survey," Network, IEEE , vol.19, no.6, pp. 49- 56, Nov.-Dec. 2005.

[9] X.Zhao, D.J.Pacella, J.Schiller, "Routing Scalability: An Operator’s View," Selected Areas in Communications, IEEE Journal on , vol.28, no.8, pp.1262-1270, October 2010.

[10] M. Gritter, D.Cheriton. 2001. “An architecture for content routing support in the internet ”, in Proceedings of the 3rd conference on USENIX Symposium on Internet Technologies and Systems - Volume 3 (USITS’01), Vol. 3. USENIX Association, Berkeley, CA, USA, 4-4.

[11] 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 (August 2007), 181-192.

[12] 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, 55-60.

[13] M. Caesar, T. Condie, J. Kannan, K. Lakshminarayanan, I. Stoica, ”ROFL: routing on flat labels ”, SIGCOMM Comput. Commun. Rev. 36, 4 (August 2006), 363-374.

[14] J.Choi, J. Han; E. Cho, T. Kwon, Y. Choi, "A Survey on content-oriented networking for efficient content delivery," Communications Magazine, IEEE , vol.49, no.3, pp.121-127, March 2011.

[15] M. Yannuzzi, R. Serral-Gracia, X. Masip-Bruin, F. Baker, R. White, P. Monclus, and D. Ward, ”Path-State Graphs on BGP,” Technical Report UPC/CRAAX TR0109, Advanced Network Architectures Lab (CRAAX), Technical University of Catalonia, Barcelona, Spain, November 2009.

[16] D. Pei, B. Zhang, D. Massey, L. Zhang, “An analysis of convergence delay in path vector routing protocols. Comput. Netw. 50, 3 (February 2006), 398-421.

[17] K. Butler, T.R. Farley, P. McDaniel, J. Rexford, J, "A Survey of BGP Security Issues and Solutions," Proceedings of the IEEE , vol.98, no.1, pp.100-122, Jan. 2010.

[18] A.L. Barab,A. Rka, “Emergence of scaling in random networks”, In Science, (286) 5439: 509, American Association for the Advancement of Science, Year 1999.

[19] G. Caldarelli,” Scale-Free Networks”, Oxford Universiy Press.2005.

[20] D. J. Watts, S. H. Strogatz, "Collective dynamics of ’small-world’ networks", Nature, vol.393, pp. 440-442, 1998.

[21] M.Thorup, U. Zwick. “Compact routing schemes”, In Proceedings of the thirteenth annual ACM symposium on Parallel algorithms and architectures (SPAA ’01). ACM, New York, NY, USA, 1-10.

[22] A.Vazquez, R. Pastor-Satorras, A.Vespignan, “Internet topology at the router and autonomous system level” , arXiv: cond-mat/0206084,June 2002.

[23] K.Ashton,” That ’Internet of Things’ Thing”, In: RFID Journal, 22. Juli 2009. Abgerufen am 8. April 2011.

[24] P. Debaty, D. Caswell, "Uniform Web presence architecture for people, places, and things ," Personal Communications, IEEE , vol.8, no.4, pp.46-51, Aug 2001.

[25] H. Yinghui, L. Guanyu, “A Semantic Analysis for Internet of Things,” Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on , vol.1, no., pp.336-339, 11-12 May 2010.

[26] The Internet of Things.www.itu.int/internetofthings

[27] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden (December 1998).

[28] http://playground.sun.com/ipv6.

[29] D. Meyer,L. Zhang, K.Fal, “Report from the IAB Workshop on routing and Addressing”,September 2007.

[30] S. Bradner, A. Mankin, The Recommendation for the IP Next Generation Protocol,RFC 1752, January 1995.

[31] J. Abley, K. Lindqvist,E. Davies,B. Black,V. Gill.IPv4 Multihoming Practices and Limitations.RFC 4116,July 2005.

[32] J.Noel Chiappa. Endpoints and Endpoint Names: A proposed enhancement to the internet Architecture,1999.http://ana.lcs.mit.edu/~jnc//tech/endpoints.txt.

[33] M. B. Hauzeur, “A model for naming, addressing and routing”, ACM Trans. Inf. Syst. 4, 4 (December 1986), 293-311.

[34] J. Saltzer, “On the naming and Binding of Network destinations”, RFC 1498.August 1993.

[35] TR. Henderson, A. Gurtov, L. Eggert, C. Dannewitz, ”Dagstuhl Seminar on Naming and Addressing for Next Generation Internetworks ”,2007.

[36] P. Leach, M. Mealling, R. Salz, “A Universally Unique Identifier (UUID) URN Namespace “, RFC 4122,July 2005.

[37] 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,” Communications Surveys & Tutorials, IEEE , vol.7, no.3, pp. 38- 54, Third Quarter 2005.

[38] T. Berber-Lee,L. Masinter,M. McCahill,”Uniform Rource Locators (URL) ” ,RFC 1738,December 1994.

[39] V. Steen, M. Hauck, F.J. Homburg, P. Tanenbaum, "Locating objects in wide-area systems," Communications Magazine, IEEE , vol.36, no.1, pp.104-109, Jan 1998..

[40] D. Farinacci,V. Fuller, D. Meyer, D. Lewis.Locator/Id Separation Protocol (LISP), draft-farinacci-list-12,March 2,2009.

[41] D. Meyer “The Locator Identifier Separation Protocol (LISP),” The Internet Protocol Journal, Volume 11, No. 1, March,2008.

[42] 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, 13-18.

[43] R. Moskowitz, P. Nikander, P.Jokela, Host Identity Protocol,RFC 5201,April 2008.

[44] A. Gurtov, M. Komu, R. Moskowitz, Host Identity Protocol: Identifier/Locator Split for Host Mobility and Multihoming,”The Internet Protocol Journal, Volume 12, No. 1, March,2009.

[45] Mike O´Dell, “GSE-An alternate Addressing Architecture for IPv6,”, draft-ietf-ipngwg-gseaddr-00.

[46] E. Nordmark, M. Bagnulo, Shim6:Level 3 Multihoming Shim Protocol for IPv6.RFC 5533.June 2009.

[47] D. Massey , L. Wang, B. Zhang,, L.Zhang, “A scalable routing system design for future internet”,SIGCOMM, August 2007.

[48] F. Templin, “The IPvLX Architecture”,draft-templin-ipvlx-0.8.May ,2007.

[49] R. Whittle, “Ivip(Internet Vastly Improved Plumbing)Architecture”,draft-whittle-ivip-arch-04.March 07,2010.

[50] X. Zhang, P. Francis, J. Wang, K. Yoshida, “Scaling IP Routing with the Core Router-Integrated Overlay”, in Proceedings of the Proceedings of the 2006 IEEE International Conference on Network Protocols (ICNP ’06). IEEE Computer Society, Washington, DC, USA, 147-156.

[51] R. Hinden, “New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG”, RFC 1955.June,1996.

[52] B. Quoitin, L. Iannone, C. Launois, O. Bonaventure, “Evaluating the benefits of the locator/identifier separation”, in Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture (MobiArch ’07). ACM, New York, NY, USA, , Article 5 , 6 pages.

[53] P. Dong, H. Wang, Y. Qin, H. Zhang; S.Y. Kuo, "Evaluation of Scalable Routing Architecture Based on Locator/Identifier Separation," GLOBECOM Workshops, 2009 IEEE , vol., no., pp.1-6, Nov. 30 2009-Dec. 4 2009.

[54] F. Templin, “Subnetwork Encapsulation and Adaptation Layer (SEAL) draft-templin-seal-23.August 19,2008.

[55] P. Savola, “MTU and Fragmentation Issues with In-the-Network Tunneling”, RFC 4459.April 2006.

[56] D. Frainacci, D. Lewis,D. Meyer, “LISP Mobile Node.draf-meyer-lisp-mn-05”, May 2,2011.

[57] P. Dong, H. Zhang, "MobileID: Universal-ID Based Mobility in Locator/ID Separation Networks", Communications and Mobile Computing (CMC), 2010 International Conference on , vol.1, no., pp.473-477, 12-14 April 2010.

[58] M. Menth, D. Klein, M. Hartmann, "Improvements to LISP Mobile Node", teletraffic Congress (ITC), 2010 22nd International , vol., no., pp.1-8, 7-9 Sept. 2010.

[59] A. Martínez W. Ramírez,M. German R. Serral-Gracià E. Marín-Tordera, Ma.Yannuzzi, X.Masip-Bruin: An Approach to a Fault Tolerance LISP Architecture. WWIC 2011: 338-349.

[60] D. Farinacci, D. Lewis,D. Meyer.V. Fuller, “Interworking LISP with IPv4 and IPv6 draft-lewis-lisp-interworking-02”, January 27,2009

[61] R. Atkinson, S. Bhatti, S. Hailes, "Evolving the Internet Architecture Through Naming", Selected Areas in Communications, IEEE Journal on , vol.28, no.8, pp.1319-1325, October 2010.

[62] M. Wasserman, F. Baker, “IPv6-to-IPv6 Network Address Translation (NAT66)”,draft-mrw-behave-nat66-02.txtNovember,2008.

[63] http://www.domaintools.com/internet-statistics/

[64] http://bgp.potaroo.net/

[65] J. Jung, E. Sit, H. Balakrishnan, R. Morris, "DNS performance and the effectiveness of caching," Networking, IEEE/ACM Transactions on , vol.10, no.5, pp. 589- 603, Oct 2002.

[66] C. Wills, H. Shang, “The contribution of DNS lookup costs to web object retrieval”, Worcester Polytehcnic INst.,Worcester,MA.[Online] Tech. REp TR-00-12.Available: http://www.cs.wpi.edu/cew/papers/tr00-12.ps.gz.

[67] L. Jakab, A.C.Aparicio, F. Coras, D. Saucez, O. Bonaventure,“LISP-TREE: a DNS hierarchy to support the LISP mapping system”, IEEE J.Sel. A. Commun. 28, 8 (October 2010), 1332-1343.

[68] M. Yannuzzi, X. Masip-Bruin, E. Grampin, R. Gagliano, A. Castro, M. German, “Managing interdomain traffic in Latin America: a new perspective based on LISP”, Communications Magazine, IEEE , vol.47, no.7, pp.40-48, July 2009

[69] I. Stoica, R. Morris, D. Karger, M. Frans Kaashoek, H.Balakrishnan, “Chord: A scalable peer-to-peer lookup service for internet applications. SIGCOMM Comput. Commun. Rev. 31, 4 (August 2001), 149-160.

[70] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, and Scott Shenker. 2001. A scalable content-addressable network. SIGCOMM Comput. Commun. Rev. 31, 4 (August 2001), 161-172.

[71] F. Memon, D. Tiebler, 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, , Article 1 , 12 pages.

[72] 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, , Article 61 , 6 pages.

[73] H. Luo, Y. Qin, H. Zhang., “A DHT-Based Identifier-to-Locator Mapping Approach for a Scalable Internet”, IEEE Trans. Parallel Distrib. Syst. 20, 12 (December 2009), 1790-1802.

[74] V. Ramasubramanian, E. Sirer, “The design and implementation of a next generation name service for the internet. In Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM ’04). ACM, New York, NY, USA, 331-342.

[75] J. Dai, F. Liu, Bo Li, “The disparity between P2P overlays and ISP underlays: issues, existing solutions, and challenges”, Netwrk. Mag. of Global Internetwkg. 24, 6 (November 2010), 36-41.

[76] M. Menth, M. Hartmann, M. Hofling. 2010. FIRMS: a mapping system for future internet routing. IEEE J.Sel. A. Commun. 28, 8 (October 2010), 1326-1331.

[77] E. Lear, “NERD: A Not-so-novel EID to RLOC Database”, draft-lear-lisp-nerd-08.txt.March 6,2010.

[78] H. Li, C. Peng, B. Li, Y. Chen, W. Zhang, J. Wu; H. Huang, "User ID Routing Architecture," Vehicular Technology Magazine, IEEE , vol.5, no.1, pp.62-69, March 2010

[79] V. Fuller, D. Meyer, D. Lewis , “LISP Alternative Topology (LISP-ALT),” Internet Draft, Work in Progress, draft-fuller-lisp-alt-06.txt.

[80] S. Brim, D. Farinacci, D. Meyer, and J. Curran, “EID.Mappings Multicast Across Cooperating Systems for LISP,”http://tools.ietf.org/html/draft-curran-lisp-emacs-00, Nov. 2007.

[81] J. Arkko, I.van Beijnum, “Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming”; RFC 5534.June,2009.

[82] X. Xu, D. Guo; , "Hierarchical Routing Architecture (HRA)," Next Generation Internet Networks, 2008. NGI 2008 , vol., no., pp.92-99, 28-30 April 2008

[83] L. Kleinrock and F. Kamoun. Hierarchical routing forlarge networks: Performance evaluation andoptimization. Computer Networks, 1:155-174, 1977.

[84] V.P, Kafle, H. Otsuki, M. Inoue, "An ID/locator split architecture for future networks," Communications Magazine, IEEE , vol.48, no.2, pp.138-144, February 2010.

[85] J. Pan, R. Jain, S. Paul, C. So-in; , "MILSA: A New Evolutionary Architecture for Scalability, Mobility, and Multihoming in the Future Internet," Selected Areas in Communications, IEEE Journal on , vol.28, no.8, pp.1344-1362, October 2010

[86] TARIFA, http://www.i2cat.net/en/projecte/tarifa-1