IPv6 versus ILNP: Architectural Harmony and Security

Max Evans

January 26, 2021

Contents

1 Preface

Among the first specifications for the Internet is an RFC specifying the need for an *underlying* Internet protocol, aptly named the Internet protocol. In the introduction to that specification, its scope, or responsibilities, were listed as providing "*the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks*", and nothing more [81]. Needless to say, in the time between the creation of the Internet Protocol and the modern day, the role of network layer protocols has suitably diverged, and so too has the interpretation of an IP address.

As the Internet has evolved, and new technologies and techniques have been adopted, rather than implementing a fundamental, architectural change to the underlying IP infrastructure, these features have instead been facilitated by differing interpretations of the IP address. This is known as **semantic overload**, and results in the so-called *entanglement* of network layer information amongst protocol layers above *and below* the network layer - a common occurrence of this misdeed is amongst transport session state for protocols such as TCP - for IPv6, this involves the misuse of the network prefix bits: the identification of a node amongst a subnet with a port number in mind to satisfy a service's delivery need not concern itself with global routing, but must nonetheless respond appropriately to its whim so as to preserve end-to-end transport session state. For common, modern Internet operations such as node mobility, the dynamism of global routing prefixes is not only likely, but expected, yet, nonetheless, is achieved on the modern internet with layered and complicated standards.

Modern Internet nodes and networks have a new set of requirements from the Internet not supported inherently by the Internet Protocol. These features include, but are not limited to, Network Address Translation (used in the context of network management in this paper, *not* with reference to its address stretching ability proposed as a solution to IPv4 address exhaustion), nodes moving across networks (*mobility*), and nodes or networks maintaining multiple connections to upstream service providers (commonly referred to as *multihoming*). It is possible for individual nodes or networks to implement multiple of these features, however, the modern IP standard requires the discussed *layering* of different protocols in order for them to function. As ubiquitous features themselves, their common layering presents an increasingly complex architecture - this is not helped by the fact that the need for mechanisms that support multihoming, NAT, etc., came at different times in history of the Internet, thus producing protocols not considered to rely on co-dependent operation.

A massively important aspect of networks, perhaps *not* initially considered with modern IP standards, is the privacy and security of the communications that flow through them. Unlike what has been discussed as ubiquitous elements of the Internet that have become increasingly prevalent or necessary (in the case of NAT), there has never been an *increased* need for security and privacy - a guarantee of communication confidentiality, authentic integrity, and non repudiation that seem to be constantly neglected or fell short. This claim will be investigated in this study with reference to the existing and used standard of IPv6, and how privacy can be assured in an implicit, elegant fashion with a more *modern* protocol.

This study discusses the comparison of the modern IPv6 standard with a newer, IETF-assigned *experimental* protocol called the *Identifier Locator Networking Protocol*, or *ILNP*. This protocol looks to support common features of Internet nodes and networks such as multihoming, mobility, and NAT in a *harmonious* fashion, while providing inherent and integral support for private and secure communications. Although ILNP concerns a set of architectural ideas that differ from the IP infrastructure, ILNP aims to be incrementally deployable with the modern Internet - an example of this assurance is with ILNP's ILNPv6-implemented networks, which are backwards-compatible with IPv6 networks.

To better visualise the motivation for this study and its content, it is worth considering the questions that one may ask when comparing both IPv6 and ILNPv6 from an architectural perspective, the specific structure of the paper will then be discussed in order to clarify how the paper will seek to answer these questions:

What are the intrinsic security and privacy features of the protocols? The namesake of the paper, and a key question for the direct comparison. Network layer technologies directly concern themselves with privacy measures, as will be discussed. As for that of security, the judgement will be based on the ease of the protocol's adoption with a modern security standard that IPv6 suggests as a securing protocol in its security considerations (section 10)[DH17].

How compatible is it with the rest of the architecture? This is important as it is vitally important for a system as critical and complex as the Internet to propagate *substitutability* at all costs. This question seeks to acquiesce the protocol, data, and algorithmic dependencies of a protocol, and discern if these overwhelm the rest of the architecture. This will be applied to recognise ILNP's ability to be *integrated* with already existing Internet architecture frameworks such as IPSec.

How many responsibilities will it undertake? This question seeks to discern protocols that do not abide by the *single responsibility principle*, and thus may over-complicate the architecture - this will be applied when discussing the motivation of ILNP in comparison with IP.

What are the intrinsic benefits of its incorporation? This questions discerns the *value* of a protocol, and its ability to outperform what is currently implemented. In the case of this study, the privacy and security of network layer protocols will be examined critically with this question in mind, in other words, **the security and privacy of IPv6 and ILNPv6**.

2 Structure of this Paper

ILNP is a proposed network layer alternative to IP described as an "evolutionary enhancement" to IP itself - the key ideas of the architecture and its components will be discussed in the Introduction. ILNPv6 (an implementation of ILNP that functions over IPv6 networks) contains several purported, intrinsic privacy mechanisms that distinguish it from IPv6. In Objective 1, these claims will be investigated, and, if proven, will explain their importance for the Internet architecture. Objective 2 seeks to evaluate ILNPv6's security, which will be done by evaluating its level of compatibility, or lack thereof, with the IPSec protocol framework. In Objective 3, ILNPv6 will be compared to IPv6 in terms of the approach the protocols both take to achieve several Internet features - multihoming, NAT, and node mobility.

3 Introduction

Circa the RFC that specifies the architectural overview for ILNP, the term "*evolutionary enhancement*" with reference to how it differs from IP is used [AB12b]. As per this claim, it does seem that ILNP seeks to remedy some of the architectural flaws that have been present in IP versions since their inception (as well as issues that predate modern and adopted IP standards), however, this study will focus on the primary architectural differences between ILNP and IPv6, with more technical and specific, architectural criticisms being made on the ILNPv6 implementation of ILNP.

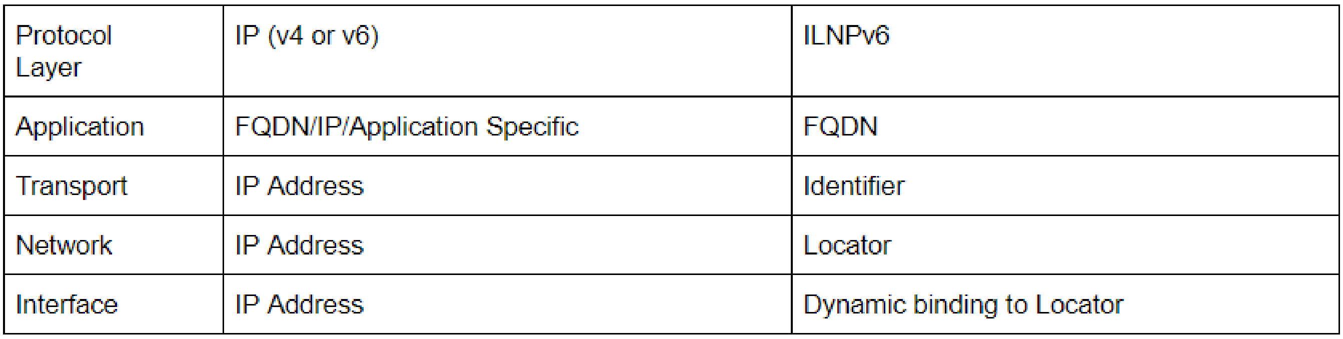
Some of the main motivations discussed concern issues the Internet architecture has in partitioning connection information amongst improper layers - this is referred to as *entanglement* and mostly concerns the usage of network-layer addressing for transport layer protocols such as TCP. This is discussed as the failure to separate routing and topology information (network layer Internet Protocol addresses) from service and delivery control information (transport layer ports etc.). This is discussed from a responsibility perspective, more technically, this kind of entanglement brings about session-critical bindings between improper components.

The paper specifying these issues - which was the first Internet Experiment Note written in 1977 (predating IPv4's official documentation and public adoption [80][81]) - also discusses issues amongst *session state* for this Internet architecture. For example, the altering of network level addresses when nodes move across networks (**node mobility**) interferes with TCP checksums as TCP includes IP addresses, interrupting transport-layer sessions. This same problem affects multihomed nodes [al77].

The motivations discussed as of yet for some new form of an Internet Protocol are valid, however, RFC 6740 makes specific reference to the "overloaded" semantics of the IP address as the "*key idea proposed for ILNP*" - this means that in its current state, the Internet architecture relies on the same piece of information (*an IP address*) to be interpreted differently depending on its context - one RFC identifies several possible interpretations the modern day IPv4 address can be used for, and how they have deviated from their original purpose and responsibility [RCC97]. ILNP looks to solve this by proposing a new architecture for the Internet, one where a single piece of information is not used amongst several layers for seemingly different purposes, but where distinct objects occupy layers in the Internet stack who undertake a single responsibility.

This introduces the key objects of the architecture, and the namesake of the protocol, **Identifier** and **Locator** values together forming a networking vector. The first of these objects, the Identifier, is used at the transport layer, and names the node, virtual or otherwise - **not the interface to the node**. One of the key features of Identifiers is that they are subject to change over time, but never over the same ILNP session. ILNPv6 implements Identifiers via IPv6's interface identifiers. The second of these objects is Locators - exclusively used at the network layer, these objects are used in the naming of subnetworks containing ILNP-compliant nodes and are used for routing. Unlike Identifiers, multiple Locators may exist for a single node, and that set of Locators may change over the course of a single ILNP session if the network topology of the node is altered. ILNPv6 uses the same syntax as IP's unicast routing prefix. Although separate and distinct in terms of their responsibilities (in contrast to the IP address which is referred to as an atomic data type), the Locator and Identifier work in tandem to achieve a dynamic binding, whose features seek to evolve the antiquated IP standard. The combination of the Identifier and the Locator is referred to as a vector, and shall be hereafter shortened to I-LV (as per RFC 6740's syntax [AB12b]). The I-LV used for communication in ILNP has its distinct parts possess **crisp** semantics, as opposed to the overloaded semantics of the atomic IP address.

To better visualise the issue (and how the network stack with an emphasis on naming works with the ILNP architecture), the following table should be illustrative of the over-reliance on the IP address from the perspective of layered responsibilities amongst both of the architectures. This table, or equivalents of it, have been used extensively amongst literature for ILNP because is shows *precisely* what the issue is with naming on the Internet - over-reliance on differing interpretations, with the viewpoint that this reliance, and the IP address in general, is considered *harmful* [YB19].



Protocol Layer	IP (v4 or v6)	ILNPv6
Application	FQDN/IP/Application Specific	FQDN
Transport	IP Address	Identifier
Network	IP Address	Locator
Interface	IP Address	Dynamic binding to Locator

Figure 1: Usage of naming in the IP architecture in comparison to ILNP. FQDN = Fully Qualified Domain Name

Lastly relevant for the purposes of the study is the notion that from an engineering standpoint, ILNP does not seek to be intrusive amongst already existing Internet infrastructure. As such, ILNPv6 networks seek to implement the ILNP architecture onto already existing IPv6 networks such that endpoint hosts are the only machines that will require a change in software. It is important to distinguish ILNP from ILNPv6, where ILNP specifies architecture and associated patterns, ILNPv6 specifies the implementation of the ideas presented with ILNP to already existing IPv6 networks.

4 Objective 1

Privacy concerns the visibility of identity attributes amongst endpoints, and is important for the reason that if not properly considered, can be used to profile the users of networks, an IPv6 problem statement refers to this phenomenon as the "'*profiling' problem*" [Koo07]. Privacy refers to information that endpoints wish to voluntarily communicate just the same as information in transit that is described as involuntary. The use of voluntary and involuntary in this context refers to the planes of communication these endpoints transmit data across: information sent in a context where privacy is concerned sees information voluntarily sent across the data plane, with the management and control planes reserved for involuntary data transit such as protocol header fields and the use of auxiliary protocols. NAT and firewall operations are good examples of the respective invocation of the control and management plane.

This section seeks to first recognise the intrinsic privacy of both ILNPv6 and IPv6, to then examine the compliance, if any, of any mechanisms prepared for these protocols that allows them to achieve privacy. Amongst all privacy and security schemes discussed, there may exist drawbacks, for both ILNP and IP, in respect to network aspects such as logging. For the purposes of this study and its objectives, the examination of this kind of network behaviour and its comparison complicates the discussion of privacy and security.

4.1 Location Privacy Assessed

From a network-layer standpoint, examined first is a node's ability to recognise if a recipient/*correspondent*, or intermediate node may determine their physical location when using a communication scheme for routing and addressing. Beresford and Stajano describe the kind of data that location tracking systems gather to be an "*intrusive catalogue*" of endpoint user activity [BS04].

Location privacy has a much more specific and sinister connotation regarding the recent uptick in use of mobile, Internet-enabled devices: the ability for organisations to track and catalogue the movements of individuals such that the location of their home networks and regular visitation networks (workplaces, schools, etc.) can be identified or inferred [Koo07]. This has implications that vary widely, for instance, it is desirable for the location of military communication network nodes to remain indiscernible.

RFC 4882 identifies the problematic nature of location inference amongst IPv6 network nodes. This RFC presents a situation that mimics the IPv6 system of addressing that reveals how roaming can be inferred: "*unique identifiers with global scope*", where the 128-bit IPv6 address is a uniquely identifiable address for nodes distributed in a global context. "*Roaming*" in the context of this paper, and location privacy in general, is synonymous with the jeopardy of a node's location privacy - the problem statement (RFC 4882) identifies Mobile IP as the IPv6-implementing candidate protocol for roaming concerns. Mobile IP concerns nodes that frequent networks other than their "*Home*" network in order to communicate with correspondent nodes when at "*Visited*" networks, i.e. concerns nodes utilising IPv6 that move around in such a fashion that they connect to other Internet-connected networks before eventually returning to a "*Home*" network - specifically the kind of node behaviour that could be used to discern regular (abundant use of mobile nodes, i.e. IPv6 smartphones) and meaningful (cross network) user movement. Specific terms relating to mobile IP such as "*Home Agent*", and "*Care-of-Address*" can be found in the problem statement [Koo07] or in the standard of Mobile IP itself [JAP11] with the latter being more comprehensive.

One of IPv6's primary address management mechanisms is known as Stateless Address Auto-Configuration (SLAAC). SLAAC utilises a deterministic method of generating Interface Identifiers (IIDs) for addresses via host-specific (and crucially *unique*) MAC addresses. It does this by splitting the host MAC in two and appending the hexadecimal values of FF:FE to the centre and flipping the seventh overall MAC bit, filling the 128-bit requirement of the v6 address.

This results in a system that produces host-unique, auto-configured IPv6 addresses [Wil13]. Although elegant, the means of the determinism involved in this algorithm is the primary concern for both logical (identity privacy jeopardising) and geographical (location privacy jeopardising) tracking. Many of the standards mentioned identify free and online-available tools available for IPv6 geo-tracking such as ping and Traceroute, but fail to elaborate on the methods used in specific and the degree of precision the geo-tracking is rated at.

In reality, geo-tracking over IP can be achieved by multiple means, e.g. heuristic analysis of routes determined via Traceroute (as discussed in length via the documentation for a tool created in 1999 [PN+99]), database lookups amongst already existing geo-tracked IP addresses (although this method is still employable for IPv6, the likelihood of records existing amongst investigated addresses is far lower than that of IPv4 due to the simple abundance of IPv6 addresses) - however, the purported accuracy of these databases has been academically questioned [Poe+11] - and machine learning frameworks utilising ping and known router geo-location [Eri+10] (which boasts a much higher degree of accuracy than "prior methods" which could reference the database lookup scenario discussed).

For common roaming sessions, the correspondent node will be able to infer if the user moves to a different network by the change in address - this address can be referred to as the "*visitation*" or "*foreign*" address and is denoted by the mobile node as the "*Care-of-Address*". An aspect of mobile IPv6 is that the Care-of-Address need not be the destination of packets sent from a correspondent nodes, instead, with the knowledge of a mobile node's Home address (via DNS etc.), packets can be routed to the mobile node's Care-of-Address - this can be achieved via mobile IPv6's bidirectional tunneling mode. For a consistent session amongst a mobile node and a correspondent node (using the syntax from the Mobile IP protocol), the monitored, on-the-wire, Home address of the mobile node can be identified easily by the correspondent node with another mode of operation under Mobile IPv6 - route optimisation (as per RFC4882's conclusion [Koo07]). Correspondent nodes with on the wire network analysis tools such as tcpdump or wireshark will be able to detect roaming as of this change in Care-of-address [Koo07]. As mentioned in the RFC specifying Mobile IP, the method to generate these dynamic address bindings can be via SLAAC - a deterministic address resolution protocol that results in consistent node elements regardless of the network visited. As also mentioned, tools are readily available, and to varying degrees of precision, can be deployed against these kinds of addresses resulting in a system wherein correspondent nodes can a) detect roaming when it occurs, and b) determine the real-world location traversal, or geo-tracking of the mobile node.

It has been revealed through largely normalised IPv6 mechanisms such as Mobile IP and SLAAC that location privacy can be jeopardised. Literature such as RFCs and whitepapers indicate that the ILNP architecture contains methods to ensure location privacy - this paper will examine the approach of Locator Rewriting Relays (LRRs) - a concept borrowed from the Tor project [AB12e].

Tor is public computer network that utilises the Onion model of networking and can function using normal Internet protocols. Tor promises complete endpoint anonymity through its various mechanisms - to illustrate the borrowed concept of Location Relay Rewriting, Tor's "circuit" topology will be explained. Tor endpoints establish "circuits" on the Tor network - these are chains of Tor endpoints who agree to forward traffic for other nodes on the network (all Tor nodes become circuit members upon connection to the Tor network), all the while providing a *layered* encryption scheme (*hence Onion*). Nodes establish key shares exclusively with neighbouring nodes, but are not capable of inferring identity attributes from other nodes in the circuit, *nor* other nodes on the network.

Tor follows a distributed computing model wherein traffic destined for a specific endpoint may have varying routes depending on the state of the circuit formed when the endpoint connects to the network - Tor compatible nodes are not vetted in any way - performance of the Tor network at any one time is nearly purely dependent on the endpoints that agree to use Tor at that time. Internet exchanges via IP that occur between the final node in the circuit (the one that the correspondent node can infer identity attributes from) and the correspondent node are liable to change over time (this could be done by reconnecting to the network or utilising aspects of "*Relay Cells*", a concept discussed alongside other Tor mechanisms, by Dingledine et al [SDM04]), but also do not accurately reflect, in any capacity, the true location of the node that is actually communicating with the correspondent node.

Just as Tor's model utilises other nodes on the network to act as gateways to provide anonymity, so too does ILNP provide an advanced deployment option known as Locator Rewriting Relays to achieve the same thing (bar the cryptographic means). ILNP packets destined for a correspondent node may enter a configured Locator Rewriting Relay "*middlebox*" (node) with Locators for the correspondent node and the host - the Locator rewriting relay acts as a session-exclusive, deterministic translator of these Locator values such that the new Locator assigned is separate and distinct from the host's locator, masking the Locator value that can be geo-tracked [AB12e]. Intermediate LRR nodes should also translate traffic destined for the sender from the correspondent such that the initial Locator is rewritten to the ILNP packet.

It's also worth noting the flexibility of LRR deployments - RFC6748 presents the LRR in the context of the ILNP architecture, not in one specific deployment scenario. This concept allows network designers to include LRRs in various different ways such that the target privacy of the system in place and/or the network infrastructure available (hardware, links) can be optimised for the best approach - Haywood presents several deployment scenarios for the LRR:

- **Scenario 1** - Single Locator Re-write: A Single LRR placed on the gateway to a subnet; LRR provides NAT-like capabilities while masking the locators of nodes within the subnet
- **Scenario 2** - VPN/Service Identifier via Locator prefix: Multiple LRR exit-nodes configured across different physical locations, though, all Internet accessible to nodes associated with a particular service provider - perhaps used such that a locator value can be used to recognise a service provider, while also masking the actual locator of the node, i.e. mobile ILNP networks provided by Vodafone host locator prefixes for their customers when they connect to the Internet using their networks

- **Scenario 3** - Tor-like LRR topology: LRR nodes form circuits with other LRRs as they join the network. Provides Tor-like anonymity capability with less of the overhead normally induced with the setup of a Tor network (layer 3 setup as opposed to network overlay). The procedure of setting up a network of nodes with cryptographic links would require engineering mechanisms not specified amongst any of the official ILNP RFCs [Hay20]
- **Scenario 4** - Policy-based Routing: Upstream nodes infer a node's importance or simple grouping such that the Locator values written in their ILNP packets are re-written appropriately. This has many applications, but could be used for QoS reasons like conditional performance optimisation for businesses, i.e. packets detected as sourced from accounting are assigned a 'faster' Locator than ones detected as packets from sales (proposed in an experimental capacity by Dr. Bhatti) [Bha20]. From a security perspective, selective routing policy (permitted with the right engineering means outside of the scope of ILNP documentation) could allow privileged packets to route through secure zones, as opposed to context-defined 'insecure' ones

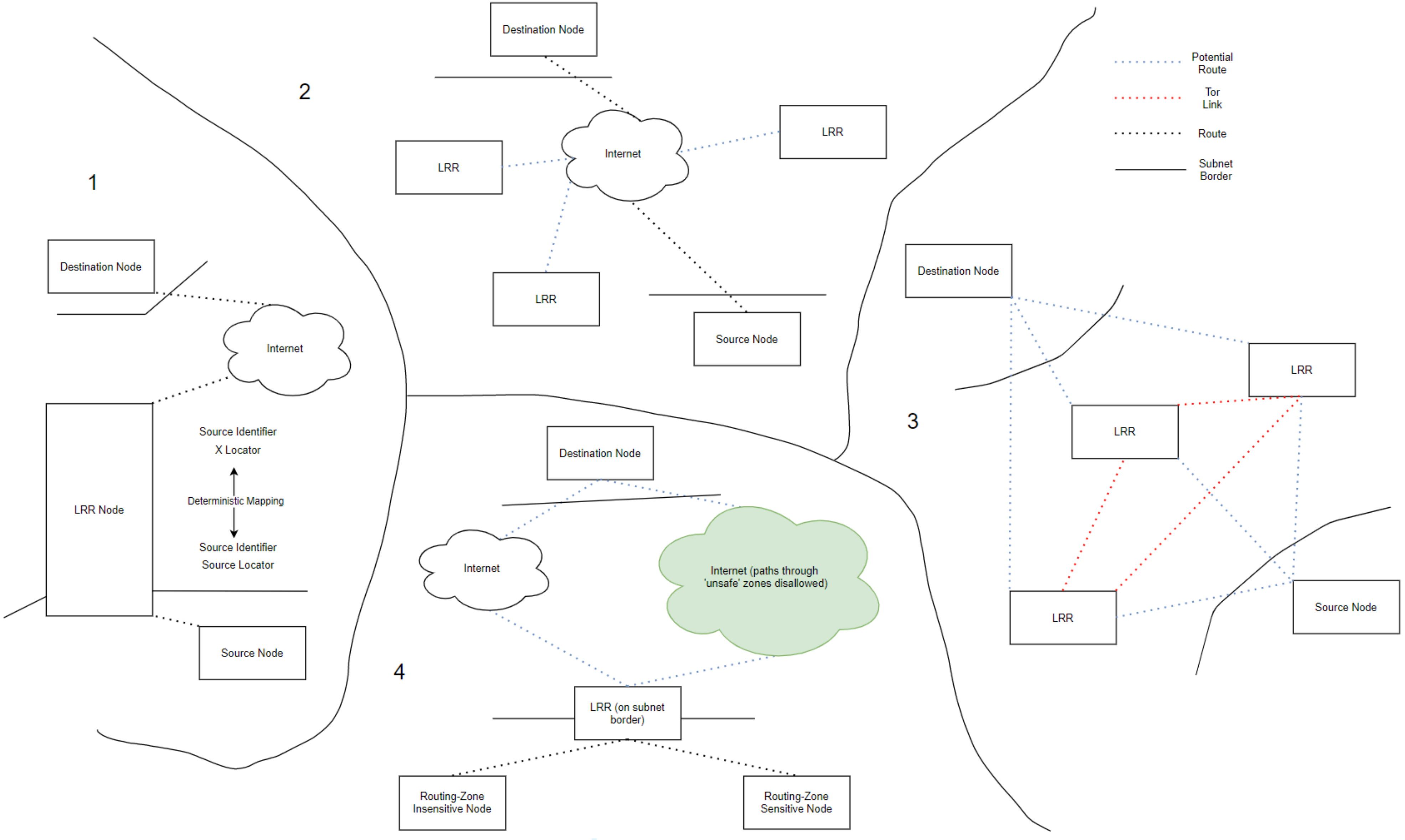


Figure 2: Potential deployment scenarios of the LRR

Despite the criticism made in this section regarding Mobile IPv6's location privacy shortfall (revealing of care-of-address and Home address binding to endpoints amongst direct routing, or revealing the Home address to onlookers on the Home to care-of-address path under bidirectional tunneling), there does exist an official, albeit experimental, RFC specifying how it can be remedied. RFC5726 recommends the use of IPSec encryption upon amongst Home binding signaling messages for the bidirectional tunneling mode of operation, and presents other solutions for location privacy when direct routing is used [QZK10]. Of course, solutions such as VPN and usage of Tor networks can be employed (with the former regularly commercially advertised as being an ideal solution for location "*spoofing*", where location-inferred addresses are used to determine service access). However, the standard discussed and commercial/overlay solutions referenced perfectly describe the architectural issue with IPv6's location privacy: a lack of intrinsic support or thought. ILNP, although not as widely deployed as IPv6 (being experimental), discusses solutions to location privacy alongside the proposal for the full protocol, with literature to suggest ways that these solutions can be used. This was shown with ILNP's Locator Rewriting Relays and their deployment scenarios in Figure 2.

4.2 Identity Privacy Assessed

The IPv6 address management system (SLAAC) has already been proven as a method of unique address formation amongst a subnet, however, node-unique MAC addresses have been identified as a suitable source of uniqueness for the host identifier portion of the IPv6 address. The implication of this tactic is that a single node, when moved across networks, will receive the same host identifier under SLAAC (with the network portion of the address being advertised as the router prefix to the network). In the previous section, location privacy was discussed, and Mobile IPv6's sharing of a node's care-of-address with a correspondent node was revealed as a mechanism that could jeopardise location privacy by implying roaming of the node and providing improved onlooker/correspondent node metrics for Home discovery. To a somewhat lesser, but nonetheless important extent, the inclusion of the MAC address within the v6 address does allow for correspondent nodes to utilise tools such as ping to discover the same node if moved across networks - this has identity privacy implications, which will be discussed later in this section, but can also reveal the physical location of the node using geo-tracking methods already discussed.

Under the IPv6 architecture, the host address is visible to the target endpoint of IPv6 traffic - the deterministic, persistent identifier interface produced via device-centric information such as MAC presents two identity privacy issues: Endpoint activity being tracked across multiple sessions on a single network, and endpoint activity being tracked across multiple sessions across different networks. This can be done by the correspondent node keeping track of endpoint addresses - and their activity, whatever that might be - and persisting it via a DBMS or otherwise. This data can be used to profile individual users, i.e. correlating traffic with users, and thus, breaching identity privacy **regardless** of if their activity was tracked across sessions within the same network, or spanned multiple.

As with the previous entry regarding location privacy, the ILNP architecture provides a mechanism for achieving endpoint identity privacy. To solve the problem sub-types as mentioned, i.e. prevent tracking across sessions within one network as well as across multiple, the use of ephemeral Identifiers is employed. "Ephemeral" refers to the short-lived nature of the ILNP Identifier value being used to identify nodes amongst transport level sessions. RFC7217 specifies a method for the generation of ephemeral IPv6 ephemeral interface identifiers - this exact same technique can be employed for use in the ILNP architecture, as the syntax for ILNP I values is the same as that of IPv6's interface identifiers. RFC7217 specifies the method of generating ephemeral, stable IPv6 interface identifiers via an algorithm that uses random numbers and utilises a mechanism to prevent address duplication (via an address counter) [Gon14].

Assuming the ephemeral, address-producing mechanism discussed does not produce addresses that persist across different networks or sessions for the same node, or addresses that are the same for different nodes under the same network (collision avoidance), the privacy issues identified with SLAAC are solved via ILNP's ephemeral address formation. From a simple, architectural perspective, leaking device-specific information - that most crucially never changes - in the form of an address, is a blatant privacy shortfall for the identification protection of nodes and their behaviour.

Another important aspect of identity privacy not discussed is the topic of identity privacy amongst networks as a whole, as opposed to single nodes. This is important because if it not taken into account, an attacker in the reconnaissance stage of an attack against a network could map information relating to the network, or, more specifically, the site topology of the network (logical representation of the physical network - subnets).

Earlier on in the paper, the subject of how NAT could be achieved via LRRs placed on a subnet border was discussed. However, not discussed was the topic of internal subnets hosting a multitude of individual Locator prefixes for nodes. RFC6748, as per its purpose, presents an option for what *could* be used as a solution for this problem - splitting the Locator value into a global routing prefix and a subnet selector, rather than forcing an SBR to maintain "*flat*" mappings for every subnet (which is purportedly impractical for large sites). The example given in the paper assigns a 45:16 bit split for the global prefix and the subnet selector respectively, allowing the SBR to maintain a smaller list of subnet mappings - an SBR may use the subnet selector from any ingress packets to identify the proper subnet, and perform a basic rewrite of the Locator value accordingly [AB12e]. This does raise the an issue that NAT actually attempts to fix - the irrelevance a Locator should have at a border to a network so as to obfuscate the topology of the network, assigning an *internally* topological significant suffix to Locators that identifies subnets opens the possibility for an attacker to monitor ingress packets on the wire in an attempt to map the organisation of the internal network (or network mapping). With this strategy implemented, non-NAT-ed networks **will still benefit** from the site topology obfuscation NAT would provide. As also stated by RFC6748 in section 2.3, the global part of the Locator proposed as being 45 bits is sufficient for advertisement of the network, therefore the egress Locator may contain zeroed out subnet selectors, effectively obfuscating the interior topology of the network.

IPv6 does present mechanisms that aim to solve its inherent identity privacy problem generated via Stateless Auto-Address Configuration - this solution is given in RFC4941 (as well as RFC7217, as discussed, and 3972), and largely mimics what ILNP seeks to do with its Identifiers inherently: provide *ephemeral* identification of a node under a subnet. Of course, for IPv6, the implementation (amongst all its engineering concerns) for ephemeral interface identifiers (meaning to change over time yet still remain globally unique) is given as another standard to be layered onto IPv6, **and is optional** [NDK07]. In the RFC specifying ILNP's engineering considerations, it actually states that IPv6's privacy extensions could be used for identifier generation, also suggesting that cryptographic techniques may be used (as per RFC3972). It is important to distinguish the roles of ILNP's Locator and Identifier values here: an ILNP Locator is subject to change over an ILNP session (with ILNP session being well-defined as per RFC6740 [AB12b]), the Identifier on the other hand will never change over the course of a single ILNP session. However, the Identifier used between ILNP sessions (described more generally as *over time* amongst ILNP literature) **may be variable**, and may even adopt IPv6's SLAAC method of interface identifier addressing as per Section 3.1 of RFC6741 [AB12c]. This same section also specifies that Identifiers could be semantically opaque or cryptographic in nature (RFC3972 is for the generation of a cryptographically generated entire IPv6 address. The generation of an entirely cryptographic I-L Vector produces an architectural conflict when used in conjunction with RFC3972, therefore it is suggested that only the cryptographically produced Identifier is maintained [Aur05]).

The multiple standards that exist for IPv6 address privacy specified in RFC's 4941, 7217, and 3972 all exist as legitimate, yet **optional** methods of address privacy for ILNP as suggested. Therefore, the purported identity privacy benefits amongst ILNP and IPv6 will only be equivalent if deployed with these standards.

5 Objective 2

Already discussed is the comparison of privacy among IPv6 and ILNP. It was revealed that there are intrinsic mechanisms that exist amongst default options for IPv6 that jeopardise location and identity privacy - the opposite was shown to be true for ILNP. The fact that mechanisms existed at the network level to respectively jeopardise and protect identity attributed of endpoints reveals that privacy considerations are fundamental in the design of network layer protocols, however, what is not intrinsic at the network layer is the concept of packet **security**. Security in this context is discussed as the assurance of confidentiality, authentic integrity, non-repudiation, and anti-replay. Both ILNP and IP, regardless of versions, do not provide defaults in terms of configurations or necessary use of other protocols for achieving packet security. What can be measured, however, as the protocol's ability to be secured is its compatibility with security infrastructure recommended by both protocols. For the sake of network layer analysis, ask not how secure the protocol is intrinsically, ask instead how compatible the protocol is with proven secure protocols and frameworks. One such framework (the recommended one for use with ILNP and IPv6) is the IPSec architecture - one that guarantees data confidentiality, message integrity, origin authentication (non-repudiation), and anti-replay. IPSec operates at the network layer, and *does not* discriminate against transport protocols used inside of IP (or ILNP, as will be discussed) datagrams.

5.1 IPSec

This study seeks to discern the privacy *and* security of both ILNP and IP, therefore, it is vital to evaluate the compliance of each protocol with an industry standard, IPSec. IPSec is a protocol framework, or *architecture*, used for broad security purposes at the network level via end-to-end encryption coupled with various other security mechanisms. It is a largely flexible security framework aiming to secure packets such that they cannot be replayed, tampered with and left undetected, understood to outside parties, or sent from an illegitimate endpoint. IPSec is made up of three abstract parts that translate to additional header information processed at the network layer, the use of various cryptographic algorithms, or the use of management systems such as IKE - these parts are Encryption Security Payload (ESP), Security Associations (SA), and Authentication Header (AH). The complex design of IPSec rooted in its vast range of deployment scenarios and considerations has been criticised in the past [FS99], but is nonetheless respected by some as "*the most extensible and complete network security solution*" [DH03]. IPSec has already been evaluated by other sources to be functional with IPv6, therefore, the extent of adoption that IPSec must undergo to be compliant with ILNP systems will be judged [FK11] in order to determine its effectiveness as a protocol that can be secured.

IPSec uses tunneling in conjunction with the Internet Key Exchange protocol. Tunnels set up using IKE are then used for transmission of packets secured with AH or ESP, the Diffie-Helmann exchange as a part of IKE results in both communicating parties sharing a secret key that is used for subsequent encryption. The scheme grows in complexity as the concept of aggressive and main modes are explained, more so when the difference between tunnel and transport mode are understood.

5.2 Adoption

Recall that ILNP seeks to be non-intrusive with already existing Internet infrastructure, and the case of IPSec is no different. IPSec endpoints use Security Associations that, for a communication session, are uniquely identified with a Security Parameter Index (SPI). Under normal IPSec, the SPI is bound to the endpoint under the network layer (IP), however, as discussed, ILNP separates the responsibilities of the IP address such that its parts are split and are subsequent to change over a single session. Session wise, the architectural change required for IPSec to function with ILNP is as simple as using the *Identifier* portion of ILNP's infrastructure to identify SAs amongst endpoints, as this, *crucially*, will never change over the course of a single ILNP session, as discussed by Bhatti et al. [AB12b]. The architectural change proposed simply changes the binding variables involved in the IPSec process, and doesn't change any of the fundamental security mechanisms.

As per ILNP's architectural goal of harmonised support for Internet features - like the ones discussed later on in this study - the use of an Identifier for a Security Association binding is hugely beneficial. ILNP's Identifier values are immutable over the course of a single connection - for an IPSec connection deployed over a NAT-ed network, the IPv6 architecture requires an additional *NAT traversal* mechanism due to the change in address, and thus, cryptographic binding. For ILNP, this kind of mechanism is not necessary for an identical NAT-ed network because the Identifier is end-to-end preserved over the entire network-layer session. This architectural benefit also extends to if the node discussed in this scenario were to be multihomed, mobile, or both, as will be discussed later. However, the omission of a Locator value present if an SA binding was made to an I-L Vector means that for a single node hosting multiple IPSec connections, there exists the possibility of collisions. Thankfully, ILNP includes a unidirectional nonce value present amongst ILNP sessions, meaning that duplicate ingress packets destined for the same node, but different ILNP IPSec sessions, can be detected from their differing nonce values. RFC6741 suggests that a mapping be made between a host's SAD (Security Associations Database) and its ILCC (Identifier-Locator Communications Cache: a host database containing ILNP communications information including interfaces) - this prevents a host from confusing one IPSec session from another [AB12c].

As mentioned already, it is one of ILNP's key goals to enter the internet architecture ecosystem while remaining as non-intrusive as possible, therefore, IPSec's adoption under RFC6743's security considerations is listed as recommended, but nonetheless optional (this recommendation comes as per the use of "SHOULD" in RFC2119 [Bra97]). Although research can be done into the significant proportions of networks on the internet that would be affected as a result of changes made to facilitate IPSec under ILNP, there will still be networks that will fail if this strategy is implemented. Just as ILNPv6 has this recommendation, so too does IPv6, rendering their adoption of security infrastructure to be equal. In fact, due to ILNP's immutable Identifier bindings, ILNP and IPSec deploying nodes actually simplify the architecture when compared to IPv6 deploying nodes (who must make use of mechanisms like RFC3948 on NAT-ed networks [Vol+05]).

In addition to ILNP's proposed architectural changes to allow IPSec to function on its implemented networks, ILNPv6 proposes an additional option for increased default security, as well as for a mechanism that is used for alerting endpoints that ILNPv6 is to be used instead of IPv6. The ILNPv6 Nonce value is a session-exclusive, "*cryptographically random*" number sent amongst the IPv6 Destination Option header. Use of the nonce value established for an ILNP communication channel prevents off-path attacks such as replay attacks and acts as a way correspondent nodes can be alerted of an endpoint's intended use of ILNPv6 at network-layer session establishment [AB12d].

6 Objective 3

As open sourced systems grow in size, both in terms of users (networks, in the case of the Internet) and features (protocols, typically, again, for the Internet), developers of the system become more frequently familiar with the technologies and algorithms that the system uses to a critical capacity (hereafter referred to simply as infrastructure). With projects that have existed amongst a time frame that spans decades, longstanding infrastructure is increasingly relied on and new infrastructure is expected to be compatible with it. A drawback to this is that the goals of a system change with reference to how the system is being used, but must nonetheless remain compatible with the critical infrastructure present, especially in the context of open-ended systems that have existed for decades.

A system such as the Internet relies upon infrastructure that has largely been unchanged in over 20 years (certainly in the case of layer 3 infrastructure), and certainly exhibits this sort of behaviour. For example, much of the current Internet implements the idea of private networks with their own address space who seek to exist in a topologically significant setting with a single '*public*' IP address - the translation of '*private*' addresses within the subnet are translated from inbound, '*public*' address-assigned packets via a mechanism known as Network Address Translation (NAT) - this architectural segmentation and process is in part to do with a fault of IPv4 addressing known as the address exhaustion problem - it adds complexity to the process of end-to-end routing and takes away from the end-to-end connection paradigm of the initial Internet. The reason this is mentioned is that it exhibits how a system's progression can deviate from its original goals through the necessary adoption of antiquated infrastructure. ILNP exists as a functional, evolutionary progression from IP infrastructure present in the current Internet architecture. ILNP seeks to be an elegant refactor of the antiquated IP standards, whose elegance in presentation is in part attributed to its **harmonious** achievement of Internet features such as NAT and IPSec, as discussed.

This section seeks to reveal the extent that the ILNP architecture goes to in order to adopt infrastructure present as a part of the already existing Internet, and any enhancements ILNP provides with this adoption over that of IPv6. Discussed will be explicit architectural features like NAT and the ability for nodes to be multihomed - also discussed will be a more abstract feature present as a part of the normal Internet - the ability for nodes to move across networks while preserving a connection to an upstream node; mobility.

6.1 NAT

NAT, or Network Address Translation, is a mechanism that allows for the mapping of a single, public node to one or more private nodes that exist behind a subnet border. The deployment of NAT was in part to do with solving the address exhaustion problem inherent with the use of IPv4, which is still a problem at the time of writing. However, with the end-to-end encouraged nodes addressed via IPv6, the issue of address exhaustion has been made practically invalid. However, NAT is still widely used amongst IPv4-deployed Internet nodes, site topology obfuscated networks, and can be deployed easily as a part of network failover mechanisms for ease of translation between a primary and auxiliary NAT-performing node.

ILNP hosts an address space identical to that of IPv6's, therefore, its functionality with NAT, although important for the communication of nodes present on networks implemented with NAT, is not necessary in terms of NAT's ability to prevent address exhaustion. RFC6741 describes the behaviour of NAT-performing nodes when encountering ILNP packets of any sort to be ILNP-*aware*, this is to say that these nodes should pass ILNP traffic through their subnet border without discrimination. This could be done by the recognition of ILNP nodes from the source address of the packet, or by the recognition of the nonce option [AB12c].

Mentioned as an architectural modification to IPSec's adoption was the binding of an SPI to an Identifier as opposed to a full IP address, however, the use of NAT with this in mind raises issues as the true recipient address of IPSec-bond packets will change after a NAT operation. To resolve this for IP traffic, ESP header-ed IPSec traffic can be encapsulated within UDP packets, as specified by RFC3948 [Vol+05]. ILNP nodes make use of Identifier values at the transport layer for their individual identification, as this behaviour is preserved over the course of IPSec sessions, even if an LRR was used in scenario 1 of Fig. 1 from the first objective of this document, the identification of the node would persist, and there would be no need for a mechanism like the one RFC3948 proposes [AB12b].

Not only does this prove that NAT can be made functional with ILNP, it also proves that NAT-deployed networks making use of IPSec at the subnet border can be made functional with ILNP without the need for an additional, layered standard such as RFC3948.

6.2 Multihoming and Mobility

Multihoming is a method for a single host or network to form links with multiple upstream Internet providers. This allows nodes to correspond with others using different technologies as well as different providers, for example, student halls at the University of St. Andrews allow students to connect their devices via Wi-Fi to the well-known Eduroam network, while also allowing students with those same devices connect to a different Internet provider via Ethernet for increased throughput. Exemplified is host multihoming, site multihoming encapsulates the same idea, however: an SBR with access to multiple upstream providers.

Node mobility is a far less abstract concept than multihoming: the action of nodes maintaining connections across different networks as the physical location of the node changes. With the advent of ubiquitous mobile computing, the increased reliance on mobile networks warrants efficient and reliable node mobility, i.e. maintaining transport sessions when a change in network is detected seamlessly. Node mobility is made possible with IPv6 through the implementation of ideas expressed in RFC3775 (although obsoleted by RFC6275, direct routing used to optimise performance is maintained, meaning the security implications are the same for that aspect of the obsoleting) - the privacy implication of mobile IPv6 has already been discussed in context of mobile IPv6 giving up the care-of-address to onlookers and endpoints, however, what was not discussed was how the mobile IPv6 is achieved in the first place. Firstly, the mobile node is said to route through its "*Home*" address to a correspondent using conventional methods, however, when the node connects to a foreign link, it is said to route through a care-of-address with configuration defaults such as SLAAC for address resolution. Direct routing in this scenario performs routing between the node's care-of-address and the correspondent, and is used for performance over the second way the mobile node may route: bidirectional tunneling from their care-of-address through their Home address. Associations between mobile home addresses and care-of-addresses for a single node are known as bindings and come with their own protocol involving updates and acknowledgements. It requires new ICMP messages, modifications to IPv6's address resolution (neighbour discovery), and reverse tunneling [JAP11].

The solution for supporting multihoming and mobility using ILNP is described as a "duality" in RFC6740 [AB12b]. This is to do with the effects or behaviour that is exhibited by ILNP-compliant nodes undergoing multihoming or mobility - changing locator values. Mobility and multihoming both come in the flavours of host and site, and the approaches taken to solve both are overall much more elegant than that of IPv6's.

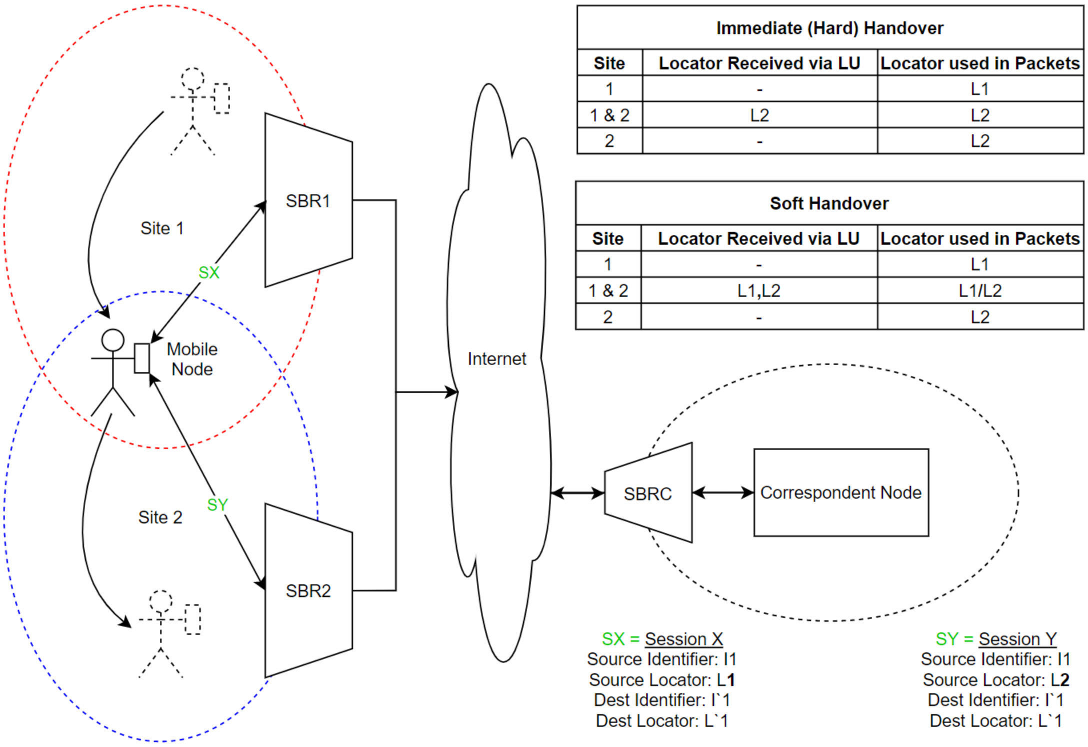
Host Multihoming: Simply speaking, an ILNP-compliant host may occupy multiple *differing* Locator values, facilitating the nodes relevance amongst *differing* network topologies. RFC6740 specifies additional engineering mechanisms that may be needed for transport protocols to function with changing locators in mind, as well as local policy for interface identification. Over a single connection, a foreign node must be informed of multihomed changes to Locator values - this can be done with Locator updates, which match that of mobile IPv6's binding updates discussed previously, and are made up of several new ICMP message types. RFC6743 specifies these message types and how they are to be used in the context of Locator updates [AB12a].

Site Multihoming: This scenario hosts the same architectural change as before, but, again, has effects on the current Internet architecture that need be clarified: Site Border Routers (SBRs) must advertise Locator values to the same capacity as IPv6's network prefix advertisements, however, it is the foreign node's responsibility while on a single connection to update the site node on its changing Locator values, the site node must maintain this for subsequent transmission.

Host Mobility: Each host monitors their own connections, and thus, changing Locator values. Host mobility concerns an individual endpoint device moving from one network to another with the assumption that there is a physical region of overlap wherein both networks may maintain connections. There are two kinds of specified "handovers" for the action of cross-network mobility, *immediate* and *soft*: immediate is where maintained connections are told to direct traffic to a node with the Locator they make them aware of while on the same connection, soft is where the period of overlap is less urgent, and correspondents may use the same Locator they were using before the detected overlap of site networks, at least until they begin receiving packets with the new Locator value, or start receiving Router Advertisements (RAs) for the Locator of the new network.

Site Mobility: Albeit with different semantics, the approach taken for achieving host mobility can be carried over, architecturally, to site mobility. This is to say that as an entire network detects a change in upstream networks due to mobility, there must be a handover process in place for correspondent nodes to recognise the change in networks. Again, the duality present with multihoming and mobility is present here - site mobility shares parallels with multihoming: an entire routing topology having changed from the perspective of the correspondent, while a session state is maintained and a handover process occurs.

As per RFC6748, and comments made regarding the duality present, Locator updates present in the following visualised *mobility* scenario may be reused for a multihoming scenario. There is also the issue of DNS entries for discoverability of the mobile node which is not visualised but is nonetheless relevant. As mentioned throughout this paper for the most part, mobility in IPv6 is achieved by an external standard, RFC6275, that comes with its own problems to do with security. ILNPv6's integral mobility and multihoming solution is much more fundamental to ILNP's harmonised design, not requiring the need for entire external standards that complicate the architecture, instead perhaps requiring engineering considerations expressed in a document like RFC6741.



Immediate (Hard) Handover

Site	Locator Received via LU	Locator used in Packets
1	-	L1
1 & 2	L2	L2
2	-	L2

Soft Handover

Site	Locator Received via LU	Locator used in Packets
1	-	L1
1 & 2	L1,L2	L1/L2
2	-	L2

SX = Session X
Source Identifier: I1
Source Locator: L**1**
Dest Identifier: I`1
Dest Locator: L`1

SY = Session Y
Source Identifier: I1
Source Locator: L**2**
Dest Identifier: I`1
Dest Locator: L`1

Figure 3: ILNP's "handover" process for changing Locator values in a physical mobility setting

7 Evaluation

The topics discussed in this paper are the result of research into already existing literature such as academic publications and RFCs. However, had the Author more available resources in a time when there isn't a pandemic, there could have been an opportunity to investigate ILNP's architectural and security claims. This could have increased the comprehension for the reader surrounding privacy claims and how they are achieved in a practical setting, and how the architecture of ILNP achieves them. For instance, a rudimentary DBMS-implemented back-end could have been implanted onto a honeypot node used to track correspondents moving across networks, and how the ability to do so may change depending on if IPv6 or ILNPv6 is used.

Although architectural in nature, this paper has benefited from work done by others as a result of a protocol's being used in an active, engineered setting. For instance, although obvious from a design perspective, IPv6's SLAAC addressing privacy shortfalls are heavily documented colloquially, and can be assumed to be leveraged on the Internet today. This is mentioned because ILNP and its implementations host extensive academic and architectural insights in the form of literature such as Milcomm papers, and are written mostly by the creators of the protocol itself. This is not a criticism at all, it is a simple observation in that ILNP is technically experimental and doesn't have the same popularity advantage as IPv6. More public scrutiny and colloquial documentation of its ideas could have allowed others to recognise flaws in ILNP's security or privacy that the Author could have benefited from. A prototype Linux implementation of ILNP has been released at the time of writing, but there is still an understandable lack of public scrutiny.

8 Conclusion

ILNP's differing architectural approach to the Internet is in aim to achieve multiple Internet "features" in a harmonious or congruous fashion, while solving the overloaded semantics of the IP address and providing backwards compatibility with the current architecture. In the context of this paper's content, this was discussed in the context of: location and identity **privacy**, **security** via the protocol's adoption (and ease thereof) with the IPSec protocol framework, NAT, multihoming, and mobility. Through the identification of direct shortfalls found amongst the IPv6 architecture (SLAAC addressing), proposed RFC "extension/optional" standards (Privacy Extensions for IPv6), and expected/antiquated behaviour (semantic overload of the IP address), ILNP's architecture was revealed to be superior to that of IPv6's in the scope of what was discussed.

Through Mobile IPv6's Care-of-address revealing, and the ability to geo-locate the standard, unchanging, SLAAC-assigned IPv6 address to varying degrees of accuracy, it was revealed that IPv6 had inherent flaws with its location privacy measures. The use of Mobile IPv6 in this example is critical, as the "profiling" problem discussed has implications that only increase in severity as more of an endpoint's activity can be tracked, with Mobile IPv6, it represents the pathological use-case. IPv6's solution to this could be third party in nature, i.e. VPN or Tor, or make use of a layered standard such as RFC5726. LRR deployment scenarios for ILNP revealed that mobile location privacy could be remedied, for instance, the implementation of scenario 2 visualised in Figure 2. ILNP's recommended ephemeral Locators and Identifier *options* also showed that if properly implemented, ILNP-enabled devices may not be able to be geo-tracked to such a simple extent as IPv6.

Also discussed in the first section was the importance of topology obfuscation, which ILNP considers **even amongst** nodes that aren't a part of a NAT-ed network. In addition to ILNP's harmonised support for IPSec and NAT, ILNP's security measures were also shown to be superior due to the presence of a nonce option amongst sessions and the vanilla topology obfuscation already discussed.

Referring to the last of the aims of this paper: the specific architectural harmony ILNP grants - the topics of NAT, multihoming, and mobility were investigated. Not only was it shown that these features may work in harmony, it also revealed that NAT and IPSec may work in harmony, with a specific standard having to be in place in order for IPv6 to achieve the same result. Mobility and multihoming in ILNP are discussed in this paper, and the literature provided for ILNP, as the same kind of problem under the architecture ILNP provides. This is referred to as a *duality* and concerns the simple change in Locator values amongst a single session for a host or a network.

In conclusion, this study shows that if engineering specifics are to be omitted at the design stage, and elegant architectural forethought is prioritised with security in mind, the protocol produced may contain features and behaviour that outperform a protocol that relies on external mechanisms to achieve what was not achieved architecturally. With the adversarial protocol in mind, ILNPv6's crisp Locator-Identifier semantics, security forethought, and current Internet architecture considerations prove that IPv6 has the ability to be outperformed from a design, complexity, and practicality standpoint.

9 Acknowledgements

The Author would like to thank Professor Saleem Bhatti for his supervision during the period of writing, and for the extremely well written RFCs and white papers him and his colleagues have produced. I would also like to thank Dr. Gregor Haywood for his kind answering of my questions regarding his previous work with ILNP.

References

[al77] C. J. Bennett et al. "Issues in the Interconnection of Datagram Networks". In: (July 1977).

[80] *DoD standard Internet Protocol*. RFC 760. Jan. 1980. DOI: 10.17487/RFC0760. URL: https://rfc-editor.org/rfc/rfc760.txt.

[81] *Internet Protocol*. RFC 791. Sept. 1981. DOI: 10.17487/RFC0791. URL: https://rfc-editor.org/rfc/rfc791.txt.

[Bra97] Scott O. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. RFC 2119. Mar. 1997. DOI: 10.17487/RFC2119. URL: https://rfc-editor.org/rfc/rfc2119.txt.

[RCC97] Yakov Rekhter, Jon Crowcroft, and Brian E. Carpenter. *IPv4 Address Behaviour Today*. RFC 2101. Feb. 1997. DOI: 10.17487/RFC2101. URL: https://rfc-editor.org/rfc/rfc2101.txt.

[FS99] Niels Ferguson and Bruce Schneier. *A cryptographic evaluation of IPsec*. 1999.

[PN+99] Ram Periakaruppan, Evi Nemeth, et al. "GTrace: A Graphical Traceroute Tool." In: *LISA*. Vol. 99. 1999, pp. 69–78.

[DH03] Naganand Doraswamy and Dan Harkins. *IPSec: the new security standard for the Internet, intranets, and virtual private networks*. Prentice Hall Professional, 2003.

[BS04] A. R. Beresford and F. Stajano. "Mix zones: user privacy in location-aware services". In: *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*. 2004, pp. 127–131.

[SDM04] Paul Syverson, Roger Dingledine, and Nick Mathewson. "Tor: The secondgeneration onion router". In: *Usenix Security*. 2004, pp. 303–320.

[Aur05] Tuomas Aura. *Cryptographically Generated Addresses (CGA)*. RFC 3972. Mar. 2005. DOI: 10.17487/RFC3972. URL: https://rfc-editor.org/rfc/rfc3972.txt.

[Vol+05] Victor Volpe et al. *UDP Encapsulation of IPsec ESP Packets*. RFC 3948. Jan. 2005. DOI: 10.17487/RFC3948. URL: https://rfc-editor.org/rfc/rfc3948.txt.

[Koo07] Rajeev Koodli. *IP Address Location Privacy and Mobile IPv6: Problem Statement*. RFC 4882. May 2007. DOI: 10.17487/RFC4882. URL: https://rfc-editor.org/rfc/rfc4882.txt.

[NDK07] Dr. Thomas Narten, Richard P. Draves, and Suresh Krishnan. *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. RFC 4941. Sept. 2007. DOI: 10.17487/RFC4941. URL: https://rfc-editor.org/rfc/rfc4941.txt.

[Eri+10] Brian Eriksson et al. "A Learning-Based Approach for IP Geolocation". In: *Passive and Active Measurement*. Ed. by Arvind Krishnamurthy and Bernhard Plattner. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 171–180. ISBN: 978-3-642-12334-4.

[QZK10] Ying Qiu, Fan Zhao, and Rajeev Koodli. *Mobile IPv6 Location Privacy Solutions*. RFC 5726. Feb. 2010. DOI: 10.17487/RFC5726. URL: https://rfc-editor.org/rfc/rfc5726.txt.

[FK11] Sheila Frankel and Suresh Krishnan. *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*. RFC 6071. Feb. 2011. DOI: 10.17487/RFC6071. URL: https://rfc-editor.org/rfc/rfc6071.txt.

[JAP11] David B. Johnson, Jari Arkko, and Charles E. Perkins. *Mobility Support in IPv6*. RFC 6275. July 2011. DOI: 10.17487/RFC6275. URL: https://rfc-editor.org/rfc/rfc6275.txt.

[Poe+11] Ingmar Poese et al. "IP geolocation databases: Unreliable?" In: *ACM SIGCOMM Computer Communication Review* 41.2 (2011), pp. 53–56.

[AB12a] R. Atkinson and SN Bhatti. *ICMP Locator Update Message for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)*. RFC 6743. Nov. 2012. DOI: 10.17487/RFC6743. URL: https://rfc-editor.org/rfc/rfc6743.txt.

[AB12b] R. Atkinson and SN Bhatti. *Identifier-Locator Network Protocol (ILNP) Architectural Description*. RFC 6740. Nov. 2012. DOI: 10.17487/RFC6740. URL: https://rfc-editor.org/rfc/rfc6740.txt.

[AB12c] R. Atkinson and SN Bhatti. *Identifier-Locator Network Protocol (ILNP) Engineering Considerations*. RFC 6741. Nov. 2012. DOI: 10.17487/RFC6741. URL: https://rfc-editor.org/rfc/rfc6741.txt.

[AB12d] R. Atkinson and SN Bhatti. *IPv6 Nonce Destination Option for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)*. RFC 6744. Nov. 2012. DOI: 10.17487/RFC6744. URL: https://rfc-editor.org/rfc/rfc6744.txt.

[AB12e] R. Atkinson and SN Bhatti. *Optional Advanced Deployment Scenarios for the Identifier-Locator Network Protocol (ILNP)*. RFC 6748. Nov. 2012. DOI: 10.17487/RFC6748. URL: https://rfc-editor.org/rfc/rfc6748.txt.

[Wil13] Sean Wilkins. *Mastering IPv6 SLAAC Concepts and Configuration*. 2013. URL: https://www.ciscopress.com/articles/article.asp?p=2154680.

[Gon14] Fernando Gont. *A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)*. RFC 7217. Apr. 2014. DOI: 10.17487/RFC7217. URL: https://rfc-editor.org/rfc/rfc7217.txt.

[DH17] Dr. Steve E. Deering and Bob Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 8200. July 2017. DOI: 10.17487/RFC8200. URL: https://rfc-editor.org/rfc/rfc8200.txt.

[YB19] Ryo Yanagida and Saleem N. Bhatti. “Seamless Internet Connectivity for Ubiquitous Communication”. In: *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*. UbiComp/ISWC ’19 Adjunct. London, United Kingdom: Association for Computing Machinery, 2019, pp. 1022–1033. ISBN: 9781450368698. DOI: 10.1145/3341162.3349315. URL: https://doi.org/10.1145/3341162.3349315.

[Bha20] Saleem Bhatti. Taken from a conversation in which the author was informed by Bhatti of another possible scenario (experimental, as with the rest) for LRRs to be deployed. July 2020.

[Hay20] Gregor Haywood. Taken from a conversation in which the author proposed several questions to Haywood regarding the work they [Haywood] had done in the past. Taken and re-worded were the scenarios used for LRRs. July 2020.