Internet Draft
draft-irtf-rrg-ilnp-arch-05.txt
Expires: 29 NOV 2012
Category: Experimental

RJ Atkinson
Consultant
SN Bhatti
U. St Andrews

29 May 2012

ILNP Architectural Description
draft-irtf-rrg-ilnp-arch-05.txt

Status of this Memo

documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This document is not on the IETF standards-track and does not specify any level of standard. This document merely provides information for the Internet community.

This document is part of the ILNP document set, which has had extensive review within the IRTF Routing Research Group. ILNP is one of the recommendations made by the RG Chairs. Separately, various refereed research papers on ILNP have also been published during this decade. So the ideas contained herein have had much broader review than the IRTF Routing RG. The views in this document were considered controversial by the Routing RG, but the RG reached a consensus that the document still should be published. The Routing RG has had remarkably little consensus on anything, so virtually all Routing RG outputs are considered controversial.

Abstract

This document provides an Architectural description and the Concept of Operations for the Identifier-Locator Network Protocol (ILNP), which is an experimental, evolutionary enhancement to IP. This is a product of the IRTF Routing RG.

Table of Contents

1. Introduction .....?
2. Architectural Overview.....?
3. Architectural Changes Introduced by ILNP.....?
4. ILNP Basic Connectivity.....?
5. Multi-Homing & Multi-Path Transport.....?
6. Mobility.....?
7. IP Security with ILNP.....?
8. Backwards Compatibility & Incremental Deployment.....?
9. Security Considerations .....?
10. Privacy Considerations.....?
11. IANA Considerations .....?
12. References .....?

1. INTRODUCTION

At present, the Internet research and development community are exploring various approaches to evolving the Internet Architecture to solve a variety of issues including, but not limited to, scalability of inter-domain routing [RFC4984]. A wide range of other issues (e.g. site multi-homing, node multi-homing, site/subnet mobility, node mobility) are also active concerns at present. Several different classes of evolution are being considered by the Internet research & development community. One class is often called "Map and Encapsulate", where traffic would be mapped and then tunnelled through the inter-domain core of the Internet. Another class being considered is sometimes known as "Identifier/Locator Split". This document relates to a proposal that is in the latter class of evolutionary approaches.

There has been substantial research relating to naming in the Internet through the years [IEN1] [IEN19] [IEN23] [IEN31] [RFC814] [RFC1498] [RFC2956]. Much of that research has indicated that binding end-to-end session state with a specific interface of a node at a specific location is undesirable, for example creating avoidable issues for mobility, multi-homing, end-to-end security. More recently, mindful of that important prior work, and starting well before the Routing RG was re-chartered to focus on inter-domain routing scalability, the authors have been examining enhancements to certain naming aspects of the Internet Architecture.

Our ideas and progress so far are embodied in the on-going definition of an experimental protocol which we call the Identifier Locator Network Protocol (ILNP). Links to relevant material are all available at:

http://ilnp.cs.st-andrews.ac.uk/

At the time of writing, the main body of peer-reviewed research from which the ideas in this and the accompanying documents draw is given in [LABH06], [ABH07a], [ABH07b], [ABH08a], [ABH08b], [ABH09a], [ABH09b], [RAB09], [ABH10], [RB10], [BA11], [BAK11].

In this document, we:

a) describe the architectural concepts behind ILNP and how various ILNP capabilities operate: this document deliberately focuses on describing the key architectural changes that ILNP introduces and defers engineering discussion to separate documents.

Other documents (listed below):

b) show how functions based on ILNP would be realised on today's Internet by proposing an instance of ILNP based on IPv6, which we call ILNPv6 (there is also a document describing ILNPv4, which is how ILNP could be applied to IPv4).

c) discuss salient operational and engineering issues impacting the deployment of ILNPv6 and the impact on the Internet.

d) give architectural descriptions of optional advanced capabilities in advanced deployments based on the ILNP approach.

1.1 Document Roadmap

This document describes the architecture for the Identifier Locator Network Protocol (ILNP). The authors recommend reading and understanding this document as the starting point to understanding ILNP.

However, the ILNP architecture can have more than one engineering instantiation. For example, one can imagine a "clean-slate" engineering design based on the ILNP architecture. In separate documents, we describe two specific engineering instances of ILNP. The term ILNPv6 refers precisely to an instance of ILNP that is based upon, and backwards compatible with, IPv6 [RFC2460]. The term ILNPv4 refers precisely to an instance of ILNP that is based upon, and backwards compatible with, IPv4.

Many engineering aspects common to both ILNPv4 and ILNPv6 are described in [ILNP-ENG]. A full engineering specification for either ILNPv6 or ILNPv4 is beyond the scope of this document.

Readers are referred to other related ILNP documents for details not described here:

a) [ILNP-ENG] describes engineering and implementation considerations that are common to both ILNPv4 and ILNPv6.

b) [ILNP-DNS] defines additional DNS resource records that support ILNP.

b) [ILNP-ICMPv6] defines a new ICMPv6 Locator Update message used by an ILNP node to inform its correspondent nodes of any changes to its set of valid Locators.

c) [ILNP-NONCEv6] defines a new IPv6 Nonce Destination Option used by ILNPv6 nodes (1) to indicate to ILNP correspondent nodes (by inclusion within the initial packets of an ILNP session) that the node is operating in the ILNP mode and (2) to prevent off-path attacks against ILNP ICMP messages. This Nonce is used, for example, with all ILNP ICMPv6 Locator Update messages that are exchanged among ILNP correspondent nodes.

d) [ILNP-ICMPv4] defines a new ICMPv4 Locator Update message used by an ILNP node to inform its correspondent nodes of any changes to its set of valid Locators.

e) [ILNP-V4OPTS] defines a new IPv4 Nonce Option used by ILNPv4 nodes to carry a security nonce to prevent off-path attacks against ILNP ICMP messages and also defines a new IPv4 Identifier Option used by ILNPv4 nodes.

As Nonces are an engineering tool and not part of the ILNP architecture, their use is described in [ILNP-ENG], with definitions in [ILNP-NONCEv6] for ILNPv6 and [ILNP-V4OPTS] for ILNPv4.

1.2 History

In 1977, Internet researchers at University College London wrote the first Internet Experiment Note (IEN), which discussed issues with the interconnection of networks [IEN1]. This identified the inclusion of network-layer addresses in the transport-layer session state (e.g. TCP checksum) as a significant problem for mobile and multi-homed nodes and networks. It also proposed separation of identity from location as a better approach to take when designing the TCP/IP protocol suite. Unfortunately, that separation did not occur, so the deployed IPv4 and IPv6 Internet entangles upper-layer protocols (e.g. TCP, UDP) with network-layer routing and topology information (e.g. IP addresses) [IEN1] [RFC768] [RFC793].

The architectural concept behind ILNP derives from a June 1994 note by Bob Smart to the IETF SIPP WG mailing list [SIPP94]. In January 1995, Dave Clark sent a similar note to the IETF IPng WG mailing list, suggesting that the IPv6 address be split into separate Identifier and Locator fields [IPng95].

Afterwards, Mike O'Dell pursued this concept in Internet-Drafts describing "8+8" or "GSE" [8+8] [GSE]. More recently, the IRTF Namespace Research Group (NSRG) studied this matter around the turn of the century. Unusually for an IRTF RG, the NSRG operated

on the principle that unanimity was required for the NSRG to make a recommendation. Atkinson was a member of the IRTF NSRG. At least one other protocol, the Host Identity Protocol (HIP), also derives in part from the IRTF NSRG studies (and related antecedent work). This current proposal differs from O'Dell's work in various ways, notably in that it does not require deployment or use of Locator rewriting.

The key idea proposed for ILNP is to directly and specifically change the overloaded semantics of the IP address. The Internet community has indicated explicitly, several times, that this use of overloaded semantics is a significant problem with the use of the Internet protocol today [RFC1498] [RFC2101] [RFC2956] [RFC4984].

While the research community has made a number of proposals that could provide solutions, so far there has been little progress on changing the status quo.

1.3 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. ARCHITECTURAL OVERVIEW

ILNP takes a different approach to naming of communication objects within the network stack. Two new data types are introduced which subsume the role of the IP address at the network and transport layers in the current IP architecture.

2.1 Identifiers and Locators

ILNP explicitly replaces the use of IP addresses with two distinct name spaces, each having distinct and different semantics:

a) Identifier: a non-topological name for uniquely identifying a node.

b) Locator: a topologically-bound name for an IP subnetwork.

The use of these two new namespaces in comparison to IP is given in Table 1. The table shows where existing names are used for state information in end-systems or protocols.

| Layer | IP | ILNP |

Application	FQDN or IP address	FQDN
Transport	IP address	Identifier
Network	IP address	Locator
Physical i/f	IP address	MAC address

FQDN = Fully Qualified Domain Name
i/f = interface

Table 1: Use of names for state information in various communication layers for IP and ILNP.

As shown in Table 1, if an application uses a Fully-Qualified Domain Name at the application-layer, rather than an IP Address or other lower-layer identifier, then the application perceives no architectural difference between IP and ILNP. We call such applications "well-behaved" with respect to naming as use of the FQDN at the application-layer is recommended in RFC1958 [RFC1958]. Some other applications also avoid use of IP address information within the application-layer protocol; we also consider these applications to be "well-behaved". Any well-behaved application should be able to operate on ILNP without any changes. Note that application level use of IP addresses includes application-level configuration information, e.g. Apache Web Server (httpd) configuration files make extensive use of IP addresses as a form of identity.

ILNP does not require applications to be rewritten to use a new Networking Application Programming Interface (API). So existing well-behaved IP-based applications should be able to work over ILNP as-is.

In ILNP, transport-layer protocols use only an end-to-end, non-topological node Identifier. It is important to note that the node Identifier names the node, not a specific interface of the node. In this way, it has different semantics and properties than either the IPv4 Address, the IPv6 Address, or the IPv6 Interface Identifier [RFC791] [RFC4219].

The use of the ILNP Identifier value within application-layer protocols is not recommended. Instead, the use of either a Fully Qualified Domain Name (FQDN) or some different topology-independent namespace is recommended.

At the network-layer, Locator values, which have topological significance, are used for routing and forwarding of ILNP packets, but Locators are not used in upper-layer protocols.

As well as the new namespaces, another significant difference in ILNP, as shown in Table 1, is that there is no binding of a routable name to an interface, or Sub-Network Point of Attachment (SNPA), as there is in IP. The existence of such a binding in IP effectively binds transport protocol flows to a specific, single interface on a node. Also, application sessions that use IP addresses effectively bind to a specific, single interface on a node in their application-layer state [RFC2460] [RFC3484].

In ILNP, dynamic bindings exist between Identifier values and associated Locator values, as well as between {Identifier, Locator} pairs and (physical or logical) interfaces on the node.

This change enhances the Internet architecture by adding crisp and clear semantics for the Identifier and for the Locator, removing the overloaded semantics of the IP address [RFC1992] [RFC4984], by updating end system protocols, but without requiring any router or backbone changes. In ILNP, the closest approximation to an IP address is an I-L Vector (I-LV), which is a given binding between an Identifier and Locator pair, written as [I, L]. I-LVs are discussed in more detail below.

Where, today, IP packets have:

- source IP address, destination IP address

instead ILNP packets have:

- source I-LV, destination I-LV

However, it must be emphasised that the I-LV and the IP address are *not* equivalent.

With these naming enhancements, we will improve the Internet architecture by adding explicit harmonised support for many functions, such as multi-homing, mobility and IP Security.

2.2 Deprecating IP Addresses

ILNP places an explicit Locator and Identifier in the IP packet header, replacing the usual IP address. Locators are tied to the topology of the network. They may change frequently, as the node or site changes its network connectivity. The node Identifier is normally much more static, and remains constant throughout the life of a given transport-layer session, and frequently much longer. However, there are various options for Identifier values, as will be discussed later [ILNP-ENG]. The way that I-LVs are encoded into packet headers is different for IPv4 and IPv6, as

explained in [ILNP-ENG].

Identifiers and Locators for hosts are advertised explicitly in DNS, through the use of new Resource Records (RRs). This is a logical and reasonable use of DNS, completely analogous to the capability that DNS provides today. At present, among other current uses, the DNS is used to map from an FQDN to a set of addresses. As ILNP replaces IP addresses with Identifiers and Locators, it is then clearly rational to use the DNS to map an FQDN to a set of Identifiers and a set of Locators for a node.

The presence of ILNP Locators and Identifiers in the DNS for a DNS owner name is an indicator to correspondents that the correspondents can try to establish an ILNP enhanced transport session with that DNS owner name.

Specifically in response to [RFC4984], ILNP improves routing scalability by helping multi-homed sites operate effectively with provider-aggregatable (PA) address prefixes. Many multi-homed sites today request provider-independent (PI) address prefixes so they can provide session survivability despite the failure of one or more access links or Internet Service Providers (ISPs). ILNP provides this session survivability by having a provider-independent node Identifier (I) value that is free of any topological semantics. This NID value can be bound dynamically to a provider-aggregatable Locator (L) value, the latter being a topological name i.e. a PA network prefix. By allowing correspondents to change arbitrarily among multiple PA Locator values, survivability is enabled as changes to the L values need not disrupt transport-layer sessions. In turn, this allows an ILNP multi-homed site to have the full session resilience that is today offered by PI addressing while using the equivalent of PA addressing, and so eliminates the current need to use globally visible PI routing prefixes for each multi-homed site.

2.3 Other Goals

While we seek to make significant enhancements to the current Internet Architecture, we also wish to ensure that instantiations of ILNP are:

a) Backwards compatible: implementations of ILNP should be able to work with existing IPv6 or IPv4 deployments, without requiring application changes.

b) Incrementally deployable: to deploy an implementation of ILNP, changes to the network nodes should only be for those

nodes that choose to use ILNP. The use of ILNP by some nodes does not require other nodes (that do not use ILNP) to be upgraded.

3. ARCHITECTURAL CHANGES INTRODUCED BY ILNP

In this section, we describe the key changes that are made to the current Internet architecture. These key changes impact end systems, rather than routers.

3.1 Identifiers

Identifiers are non-topological values that identify an ILNP node. A node might be a physical node or a virtual node. For example, a single physical device might contain multiple independent virtual nodes. Alternately, a single virtual device might be composed from multiple physical devices. In the case of a Multi-Level Secure (MLS) system, each valid sensitivity label of that system might be a separate virtual node.

A node MAY have multiple Identifier values associated with it, which MAY be used concurrently.

In normal operation when a node is responding to a received ILNP packet that creates a new session, the correct I value to use for that session with that correspondent node will be learned from the received ILNP packet.

In normal operation when a node is initiating communication with a correspondent node, the correct I value to use for that session with that correspondent node will be learned either through the application-layer naming, through DNS name resolution, through some alternative name resolution system, or an application may be able to select different I values directly as Identifiers are visible above the network-layer via the transport protocol.

3.1.1 Identifiers are immutable during a session

Once an Identifier value has been used to establish a session it forms part of the end-to-end (invariant) session state and so must remain fixed for the duration of that session. This means, for example, that throughout the duration of a given TCP session, the source Identifier and destination Identifier values will not change.

In normal operation, a node will not change its set of valid Identifier values frequently. However, a node MAY change its set

of valid Identifier values over time, for example in an effort to provide identity obfuscation, while remaining subject to the architectural rule of the preceding paragraph.

3.1.2 Syntax

ILNP Identifiers have the same syntax as IPv6 Interface Identifiers [RFC4291], based on the EUI-64 format [IEEE-EUI], which helps with backwards compatibility. There is no semantic equivalent to an ILNP Identifier in IPv4 or IPv6 today.

The Modified EUI-64 syntax used by both ILNP Identifiers and IPv6 Interface Identifiers contains a bit indicating whether the value has global-scope or local-scope [IEEE-EUI] [RFC4219]. ILNP Identifiers have either global-scope or local-scope. If they have global scope, they SHOULD be globally unique.

Regardless of whether an Identifier is global-scope or local-scope, an Identifier MUST be unique within the scope of a given Locator value to which it is bound for a given session or packet flow. As an example, with ILNPv6, the ordinary IPv6 Neighbour Discovery (ND) processes ensure that this is true, just as ND ensures that no two IPv6 nodes on the same IPv6 subnetwork have the same IPv6 address at the same time.

Both the IEEE EUI-64 specification and the Modified EUI-64 syntax also has a 'Group' bit [IEEE-EUI][RFC4291] For both ILNP node Identifiers and also IPv6 Interface Identifiers, this Group bit is set to 0.

3.1.3 Semantics

Unicast ILNP Identifier values name the node, rather than naming a specific interface on that node. So ILNP Identifiers have different semantics than IPv6 Interface Identifiers.

3.2 Locators

Locators are topologically-significant names, analogous to (sub)network routing prefixes. The Locator names the IP subnetwork that a node is connected to. ILNP neither prohibits nor mandates in-transit modification of Locator values.

A host MAY have several Locators at the same time, for example if it has a single network interface connected to multiple subnetworks (e.g. VLAN deployments on wired Ethernet), or has

multiple interfaces each on a different subnetwork. Locator values normally have Locator Precedence Indicator (LPI) values associated with them. These LPIs indicate that a specific Locator value has higher or lower precedence for use at a given time. Local LPI values may be changed through local policy or via management interfaces. Remote LPI values are normally learned from the DNS, but the local copy of a remote LPI value might be modified by local policy relating to preferred paths or prefixes.

Locator values are used only at the network-layer. Locators are not used in end-to-end transport state. For example, Locators are not used in transport-layer protocol state or application session state. However, this does not preclude an end-system setting up local dynamic bindings for a single transport flow to multiple Locator values concurrently.

The routing system only uses Locators, not Identifiers. For unicast traffic, ILNP uses longest-prefix match routing, just as the IP Internet does.

Section 4 below describes in more detail how Locators are used by the forwarding and routing packets from a sending node on an origin subnetwork to one or more receiving nodes on one or more destination subnetworks.

A difference from earlier [GSE, 8+8] proposals is that, in normal operation, the originating host supplies both Source Locator and Destination Locator values in the packets it sends out.

Section 4.2 describes packet forwarding in more detail, while Section 4.3 describes packet routing in more detail.

3.2.1 Locator Values are Dynamic

The ILNP architecture recognises that Locator values are topologically significant, so the set of Locator values associated with a node normally will need to change when the node's connectivity to the Internet topology changes. For example, a mobile or multi-homed node is likely to have connectivity changes from time to time, along with the corresponding changes to the set of Locator values.

When a node using a specific set of Locator values changes one or more of those Locator values, then the node (1) needs to update its local knowledge of its own Locator values, (2) needs to inform all active Correspondent Nodes (CNs) of those changes to its set of Locator values so that ILNP session continuity is maintained, and (3) if it expects incoming connections the node

also needs to update its Locator related entries in the Domain Name System. [ILNP-ENG] describes the engineering and implementation details of this process.

3.2.2 Locator Updates

As Locator values can be dynamic, and they could change for a node during a communication session, correspondents need to be notified when a Locator value for a node changes for any communication sessions that are in progress. To enable this, a node that sees its Locator values have changed needs to send a Locator Update (LU) message to its correspondent nodes. (The change in Locator values may also need to be notified to DNS but that is discussed elsewhere.)

3.2.3 Syntax

ILNP Locators have the same syntax as an IP unicast routing prefix.

3.2.4 Semantics

ILNP unicast Locators have the same semantics as an IP unicast routing prefix, since they name a specific subnetwork. ILNP neither prohibits nor requires in-transit modification of Locator values.

3.3 IP Address and Identifier-Locator Vector (I-LV)

Historically, an IP Address has been considered to be an atomic datum, even though it is recognised that an IP address has an internal structure: the network prefix plus either the host ID (IPv4) or the interface identifier (IPv6). However, this internal structure has not been used in end-system protocols: instead all the bits of the IP address are used. (Additionally, in IPv4 the IPv4 sub-net mask uses bits from the host ID, a further confusion of the structure, even thought it is an extremely useful engineering mechanism.)

In ILNP, the IP address is replaced by an "Identifier-Locator Vector" (I-LV). This consists of a pairing of an Identifier value and a Locator value for that packet, written as [I, L]. All ILNP packets have Source Identifier, Source Locator, Destination Identifier, and Destination Locator values. The I value of the

I-LV is used by upper-layer protocols (e.g. TCP, UDP, SCTP), so needs to be immutable. Locators are not used by upper-layer protocols (e.g. TCP, UDP, SCTP). Instead, Locators are similar to IP routing prefixes, and are only used to name a specific subnetwork.

While it is possible to say that an I-LV is an approximation to an IP address of today, it should be understood that an I-LV:

a) is not an atomic datum, being a pairing of two data types, an Identifier and a Locator.

b) has different semantics and properties to an IP address, as is described in this document.

In our discussion, it will be convenient sometimes to refer to an I-LV, but sometimes to refer only to an Identifier value, or only to a Locator value.

ILNP packets always contain a source I-LV and a destination I-LV.

3.4 Notation

In describing how capabilities are implemented in ILNP, we will consider the differences in end-systems state between IP and ILNP in order to highlight the architectural changes.

We define a formal notation to represent the data contained in the communications session state. We define:

A = IP address
I = Identifier
L = Locator
P = Transport-layer port number

To differentiate the local and remote values for the above items, we also use suffixes, for example:

_L = local
_R = remote

With IPv4 and IPv6 today, the invariant state at the transport-layer for TCP can be represented by the tagged tuple:

<TCP: A_L, A_R, P_L, P_R> --- (1)

Tag values that will be used are:

```
IP   Internet Protocol
ILNP Identifier Locator Network Protocol
TCP  Transmission Control Protocol
UDP  User Datagram Protocol
```

So, for example, with IP, a UDP packet would have the tagged tuple:

```
<UDP: A_L, A_R, P_L, P_R>                                  --- (2)
```

A TCP segment carried in an IP packet may be represented by the tagged tuple binding:

```
<TCP: A_L, A_R, P_L, P_R><IP: A_L, A_R>                    --- (3)
```

and a UDP packet would have the tagged tuple binding:

```
<UDP: A_L, A_R, P_L, P_R><IP: A_L, A_R>                    --- (4)
```

In ILNP, the transport-layer state for TCP is:

```
<TCP: I_L, I_R, P_L, P_R>                                  --- (5)
```

The binding for a TCP segment within an ILNP packet:

```
<TCP: I_L, I_R, P_L, P_R><ILNP: L_L, L_R>                  --- (6)
```

When comparing tuple expressions (3) and (6), we see that for IP, any change to network addresses impacts the end-to-end state, but for ILNP, changes to Locator values do not impact end-to-end state, providing end-system session state invariance, a key feature of ILNP compared to IP as it is used in some situations today. ILNP adopts the end-to-end approach for its architecture [SRC84]. As noted previously, nodes MAY have more than one Locator concurrently and nodes MAY change their set of active Locator values as required.

3.5 Transport-layer state and transport pseudo-headers

In ILNP, protocols above the network-layer do not use the Locator values. Thus, the transport-layer uses only the I values for the transport-layer state (e.g. TCP checksum, UDP checksum), as is shown, for example, in expression (6) above.

Additionally, again from a practical perspective, while the I

values are only used in protocols above the network-layer, it is convenient for them to be carried in network packets, so that the namespace for the I values can be used by any transport-layer protocols operating above the common network-layer.

3.6 Rationale for this document

This document provides an architectural description of the core ILNP capabilities and functions. It is based around the use of example scenarios so that practical issues can be highlighted.

In some cases, illustrative suggestions and light discussion are presented with respect to engineering issues, but detailed discussion of engineering issues are deferred to other ILNP documents.

The order of the examples presented below are intended to allow an incremental technical understanding of ILNP to be developed. There is no other reason for the ordering of the examples listed below.

Many of the descriptions are based on the use of an example site network as shown in Figure 2.1.

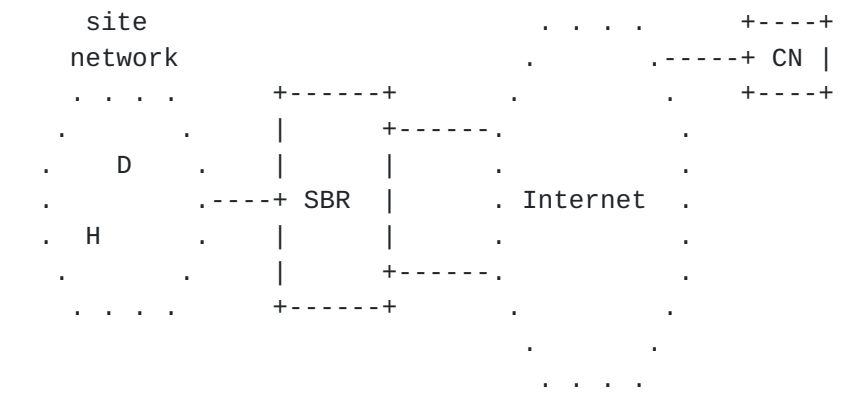


Figure 2.1: A simple site network for ILNP examples.

In some cases, hosts (H) or devices (D) act as end-systems within the site network, and communicate with (one or more) Correspondent Node (CN) instances that are beyond the site.

Note that the Figure is illustrative and presents a logical view. For example, the CN may itself be on a site network, just like H or D.

Also, for formulating examples, we assume ILNPv6 is in use, which has the same packet header format (as viewed by routers) as IPv6, and can be seen as a superset of IPv6 capabilities.

For simplicity, we assume that name resolution is via the deployed DNS which has been updated to store DNS records for ILNP [ILNP-DNS].

Note that, from an engineering viewpoint, this does NOT mean that the DNS also has to be ILNP capable: existing IPv4 or IPv6 infrastructure can be used for DNS transport.

3.7 ILNP Multicasting

Multicast forwarding and routing are unchanged, in order to avoid requiring changes in deployed IP routers and routing protocols. ILNPv4 multicasting is the same as IETF standards-track IPv4 multicasting. ILNPv6 multicasting is the same as IETF standards-track IPv6 multicasting.

4. ILNP BASIC CONNECTIVITY

In this section, we describe basic packet forwarding and routing in ILNP. We highlight areas where it is similar to current IP, and also where it is different from current IP. We use examples in order to illustrate the intent and show the feasibility of the approach.

For this section, in Figure 4.1, H is a fixed host in a simple site network, CN is a remote Correspondent Node outside the site, H and CN are ILNP-capable, while the Site Border Router (SBR) does not need to be ILNP-capable.

CN = Correspondent Node
H = Host
SBR = Site Border Router

Figure 4.1: A simple site network for ILNP examples.

4.1 Basic Local Configuration

This section uses the term "Address management", in recognition of the analogy with capabilities present in IP today. In this document, address management is about enabling hosts to attach to a subnetwork and enabling network-layer communication between and among hosts, also including:

a) enabling identification of a node within a site.
b) allowing basic routing/forwarding from a node acting as an end-system.

If we consider Figure 4.1, imagine that host H has been connected to the site network. Administratively, it needs at least one I value and one L value in order to be able to communicate.

Today, local administrative procedures allocate IP addresses, often using various protocol mechanisms (e.g. NetConf-based router configuration, DHCP for IPv4, DHCP for IPv6, IPv6 Router Advertisements). Similarly, local administrative procedures can allocate I and L values as required, e.g. I_H and L_H. This may be through manual configuration.

Additionally, if it is expected or desired that H might have incoming communication requests, e.g. it is a server, then the values I_H and L_H can be added to the relevant name services (e.g. DNS, NIS/YP), so that FQDN lookups for H resolve to the appropriate DNS resource records (e.g. NID, L32, L64, and LP [ILNP-DNS]) for node H.

From a network operations perspective, this whole process also can be automated. As an example, consider that in Figure 3.1 the Site Border Router (SBR) is an IPv6 capable router and is connected via link1 to an ISP that supports IPv6. SBR will have been allocated one (or more) IPv6 prefixes that it will multicast using IPv6 Routing Advertisements (RAs) into the site network, e.g. say prefix L_1. L_1 is actually a local IPv6 prefix (/64),

which is formed from an address assignment by the upstream ISP, according to [RFC3177] or [RFC6177]. Host H will see these RAs, for example, on its local interface with name eth0, will be able to use that prefix as a Locator value, and will cache that Locator value locally.

Also, node H can use the mechanism documented in either Section 2.5.1 of [RFC4291], in [RFC3972] [RFC4581] [RFC4982], or in [RFC4941] in order to create a default I value, say I_H, just as an IPv6 host can. For DNS, the I_H and L_1 values may be pre-configured in DNS by an administrator who already has knowledge of these, or added to DNS by H using Secure DNS Dynamic Update [RFC3007] to add or update the correct NID and L64 records to DNS for the FQDN for H.

4.2 I-L Communication Cache

For the purposes of explaining the concept of operations, we talk of a local I-L Communication Cache (ILCC). This is an engineering convenience and does not form part of the ILNP architecture, but is used in our examples. More details on the ILCC can be found in [ILNP-ENG]. The ILCC contains information that is required for the operation of ILNP. This will include, amongst other things, the current set of valid Identifier and Locator values in use by a node, the bindings between them and the bindings between Locator values and interfaces.

4.3 Packet Forwarding

When the SBR needs to send a packet to H, it uses local address resolution mechanisms to discover the bindings between interface addresses and currently active I-LVs for H. For our example of Figure 3.1, IPv6 Neighbour Discovery (ND) can be used without modification, as the I-LV for ILNPv6 occupies the same bits as the IPv6 address in the IPv6 header. For packets from H to SBR, the same basic mechanism applies, as long as SBR supports IPv6 and even if it is not ILNPv6-capable, as IPv6 ND is used unmodified for ILNPv6.

For Figure 3.1, assuming:

- SBR advertises prefix L_1 locally, uses I value I_S, and has an Ethernet MAC address M_S on interface with local name sbr0

- H uses I value I_H, and has an ethernet MAC address of M_H on the interface with local name eth0

then H will have in its ILCC:

```
  [I_H, L_1]                                        --- (7a)
  L_1, eth0                                         --- (7b)
```

After the IPv6 RA and ND mechanism has executed, the ILCC at H would contain, as well as (7a) and (7b), the following entry for SBR:

```
  [I_S ,L_1], M_S                                   --- (8)
```

For ILNPv6, it does not matter that the SBR is not ILNPv6 capable, as the I-LV [I_S, L_1] is physically equivalent to the IPv6 address for the internal interface sbr0.

At SBR, which is not ILNP-capable, there would be the following entries in its local cache and configuration:

```
   L_1:I_S                                          --- (9a)
   L_1, sbr0                                        --- (9b)
```

Expression (9a) represents a valid IPv6 ND entry: in this case, the I_S value (which is 64 bits in ILNPv6) and the L_1 values are, effectively, concatenated and treated as if they were a single IPv6 address. Expression (9b) binds transmissions for L_1 to interface sbr0 (again, sbr0 is a local, implementation-specific name, and such a binding is possible with standard tools today, for example ifconfig(8)).

4.4 Packet Routing

If we assume that host H is configured as in the previous section, it is now ready to send and receive ILNP packets.

Let us assume that, for Figure 3.1, it wishes to contact the node CN, which has FQDN cn.example.com and is ILNP-capable. A DNS query by H for cn.example.com will result in NID and L64 records for CN, with values I_CN and L_CN, respectively, being returned to H, and stored in its ILCC:

```
  [I_CN, L_CN]                                     --- (10)
```

This will be considered active, as long as the TTL values for the DNS records are valid. If the TTL for an I or L value is zero, then the value is still useable but becomes stale as soon as it has been used once. However, it is more likely that the TTL value will be greater than zero [BA11] [SBK02].

Once the CN's I value is known, the upper layer protocol, e.g. the transport protocol, can set up suitable session state:

<UDP: I_H, I_CN, P_H, P_CN> --- (11)

For routing of ILNP packets, the destination L value in an ILNPv6 packet header is semantically equivalent to a routing prefix. So, once a packet has been forwarded from a host to its first-hop router, only the destination L value needs to be used for getting the packet to the destination network. Once the packet has arrived at the router for the site network, local mechanisms and packet forwarding mechanism, as described above in Section 4.3, allow the packet to be delivered to the host.

For our example of Figure 4.1, H will send a UDP packet over ILNP as:

<UDP: I_H, I_CN, P_H, P_CN><ILNP: L_1, L_CN> --- (12a)

and CN will send UDP packets to H as:

<UDP: I_CN, I_H, P_CN, P_H><ILNP: L_CN, L_1> --- (12b)

The I value for H used in the transport-layer state (I_H in expression (12a)) selects the correct L value (L_1 in this case) from the bindings in the ILCC (expression (7a)), and that, in turn, selects the correct interface from the ILCC (expression (7b)), as described in Sec 4.2. This gets the packet to the first hop router, and beyond that, the ILNPv6 packet is treated as if it were an IPv6 packet.

5.0 MULTI-HOMING AND MULTI-PATH TRANSPORT

For multi-homing, there are three cases to consider:

a) Host Multi-Homing (H-MH): a single host is, individually, connected to multiple upstream links, via separate routing paths, and those multiple paths are used by that host as it wishes. That is, use of multiple upstream links is managed by the single host itself. For example, the host might have multiple valid Locator values on a single interface, with each Locator value being associated with a different upstream link (provider).

b) Multi-Path Transport (MPT): This is similar to using ILNP's support for host multi-homing (i.e. H-MH), so we describe multi-path transport here. (Indeed,

for ILNP, this can be considered a special case of H-MH.)

c) Site Multi-Homing (S-MH): a site network is connected to multiple upstream links via separate routing paths, and hosts on the site are not necessarily aware of the multiple upstream paths. That is, the multiple upstream paths are managed, typically, through a site-border router, or via the providers.

Essentially, for ILNP, multi-homing is implemented by enabling:

a) multiple Locator values to be used simultaneously by a node

b) dynamic, simultaneous binding between one (or more) Identifier value(s) and multiple Locator values

With respect to the requirements for hosts [RFC1122], the multi-homing function provided by ILNP is very flexible. It is not useful to discuss ILNP multi-homing strictly within the confines of the exposition presented in Section 3.3.4 of [RFC1122], as that text is couched in terms of relationships between IP addresses and interfaces, which can be dynamic in ILNP. The closest relationship between ILNP multi-homing and [RFC1122] would be that certainly ILNP could support the notion of "Multiple Logical Networks", "Multiple Logical Hosts" and "Simple Multihoming".

5.1 Host Multi-Homing (H-MH)

At present, host multi-homing is not common in the deployed Internet. When TCP or UDP are in use for an IP session, host multi-homing cannot provide session resilience, because the transport pseudo-header checksum binds the session to a single address of the multi-homed node, and hence to a single interface. SCTP has a protocol-specific mechanism to support node multi-homing; SCTP can support session resilience both at present and also without change in the proposed approach [RFC5061].

Host multi-homing in ILNP is supported directly in each host by ILNP. The simplest explanation of H-MH for ILNP is that an ILNP-capable host can simultaneously use multiple Locator values, for example by having a binding between an I value and two different L values, e.g. the ILCC may contain the I-LVs:

```
[I_1, L_1]                                    --- (14a)
[I_1, L_2]                                    --- (14b)
```

Additionally, a host may use several I values concurrently,

e.g. the ILCC may contain the I-LVs:

```
[I_1, L_1]                                    --- (15a)
[I_1, L_2]                                    --- (15b)
[I_2, L_2]                                    --- (15c)
[I_3, L_1]                                    --- (15d)
```

Architecturally, ILNP considers these all to be cases of multi-homing: the host is connected to more than one subnetwork, each subnetwork being named by a different Locator value.

In the cases above, the selection of which I-LV to use would be through local policy or through management mechanisms. Additionally, suitably modified transport-layer protocols, such as multi-path transport-layer protocol implementations, may make use of multiple I-LVs. Note that in such a case, the way in which multiple I-LVs are used would be under the control of the higher-layer protocol.

Recall, however, that L values also have precedence - LPI values - and these LPI values can be used at the network-layer, or by a transport-layer protocol implementation, in order make use of L values in a specific manner.

Note that, from a practical perspective, ILNP dynamically binds L values to interfaces on a node to indicate the SNPA for that L value, so the multi-homing is very flexible: a node could have a single interface and have multiple L values bound to that interface. For example, for expressions (14a) and (14b) if the end-system has a single interface with local name eth0, then the entries in the ILCC will be:

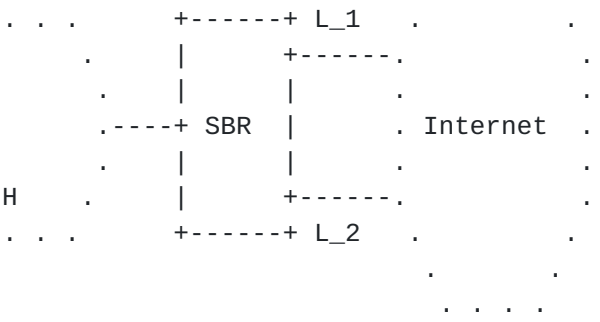
```
L_1, eth0                                     --- (16a)
L_2, eth0                                     --- (16b)
```

and if we assume that for expressions (15a-c), the end-system has two interfaces, eth0 and eth1, then these ILCC entries are possible:

```
L_1, eth0                                     --- (17a)
L_2, eth1                                     --- (17b)
```

Let us consider the network in Figure 5.1.

```
     site                        . . . .
    network                     .       .
```



L_1 = global Locator value 1
L_2 = global Locator value 2
SBR = Site Border Router

Figure 5.1: A simple multi-homing scenario for ILNP.

We assume that H has a single interface, eth0. SBR will advertise L_1 and L_2 internally to the site. Host H will configure these as both reachable via its single interface, eth0, by using ILCC entries as in expressions (16a) and (16b). When packets from H that are to egress the site network reach SBR, it can make appropriate decisions on which link to use based on the source Locator value (which has been inserted by H), or based on other local policy.

If, however, H has two interfaces, eth0 and eth1, then it can use ILCC entries as in expressions (17a) and (17b).

Note that the values L_1 and L_2 do not need to be PI based Locator values, and can be taken from ISP-specific PA routing prefix allocations from the upstream ISPs providing the two links.

Of course, this example is illustrative: many other configurations are also possible, but the fundamental mechanism remains the same, as described above.

If any Locator values change then H will discover this when it sees new Locator values in RAs from SBR, and sees that L values that were previously used are no longer advertised. When this happens, H will:

a) maintain existing active upper layer sessions: based on its current ILCC entries and active sessions, send Locator Update (LU) messages to CNs to notify them of the change of L values. (LU messages are synonymous to Mobile IPv6 Binding Updates.)

b) if required, update its relevant DNS entries with the new L value in the appropriate DNS records, to enable correct resolution for new incoming session requests.

From an engineering view point, H also updates its ILCC data, removing the old L value(s) and replacing with new L value(s) as required.

Depending on the nature of the physical change in connectivity that the L value change represents, this may disrupt upper-level protocols, e.g. a fibre cut. Dealing with such physical-level disruption is beyond the scope of ILNP. However, ILNP supports graceful changes in L values, and this is explained below in Section 6 in the discussion on mobility support.

5.2 Support for Multi-Path Transport Protocols (MPTs)

ILNP supports deployment and use of multi-path transport protocols, such as the Multi-Path extensions to TCP (MP-TCP) being defined by the IETF TCPM Working Group. Specifically, ILNP will support the use of multiple paths as it allows a single I value to be bound to multiple L values - see Sec 5.1 and specifically expressions (15a) and (15b).

Of course, there will be specific mechanisms for:
- congestion control
- signalling for connection/session management
- path discovery and path management
- engineering and implementation issues

These transport-layer mechanisms fall outside the scope of ILNP and would be defined in the multi-path transport protocol specifications.

As far as the ILNP architecture is concerned, the transport protocol connection is simply using multiple I-LVs, but with the same I value in each, and different L values, i.e. a multi-homed host.

5.3 Site multi-homing (S-MH)

At present, site multi-homing is common in the deployed Internet. This is primarily achieved by advertising the site's routing prefix(es) to more than one upstream Internet service provider at a given time. In turn, this requires de-aggregation of routing prefixes within the inter-domain routing system. This increases the entropy of the inter-domain routing system

(e.g. RIB/FIB size increases beyond the minimal RIB/FIB size that would be required to reach all sites).

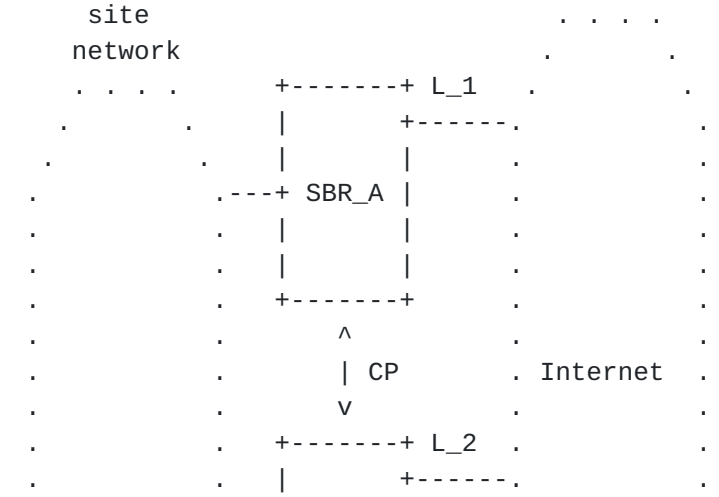
Site multi-homing, in its simplest form in ILNP, is an extension of the H-MH scenario described in Sec 5.1. If we consider Figure 5.1 and assume that there are many hosts in the site network, each can choose to manage its own ILNP connectivity and whether or not multiple Locator values are used. This allows maximal control of connectivity for each host.

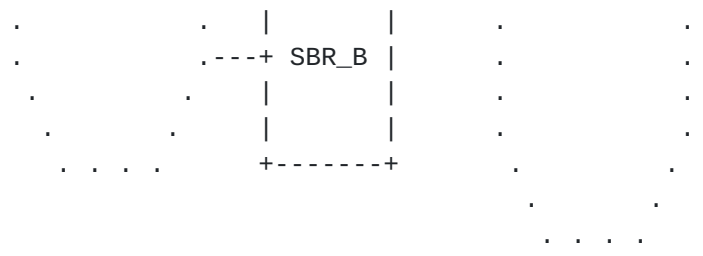
Of course, with ILNPv6, just as any IPv6 router is required to generate IPv6 Router Advertisement messages with the correct routing prefix information for the link the RA is advertised upon, thus also the SBR is required to generate RAs containing the correct Locator value(s) for the link that the RA is advertised upon. The correct values for these RA messages are typically configured by system administration, or might be passed down from the upstream provider.

To avoid a DNS Update burst when a site or (sub)network changes location, a DNS record optimisation is possible by using the new LP record for ILNP. This would change the number of DNS Updates required from Order(Number of nodes within the site/subnetwork that moved) to Order(1) [ILNP-DNS].

5.3.1 A common multi-homing scenario - multiple SBRs

The scenario of Fig 5.1 is an example to illustrate the architectural operation of multi-homing for ILNP. For site multi-homing, a scenario such as the one depicted in Figure 5.2 is also common. Here, there are two SBRs, each with its own global connectivity.





CP = coordination protocol
L_1 = global Locator value 1
L_2 = global Locator value 2
SBR_A = Site Border Router A
SBR_B = Site Border Router P

Figure 5.2: A dual-router multi-homing scenario for ILNP.

The use of two physical routers provides an extra level of resilience compared to the scenario of Fig 5.1. The coordination protocol (CP) between the two routers keeps their actions in synchronisation according to whatever management policy is in place for the site network. Such capabilities are available today in products. Note that, logically, there is little difference between Fig 5.1 and Fig 5.2, but with two distinct routers in Fig 5.2, the interaction using CP is required. Of course, it is also possible to have multiple interfaces in each router and more than two routers.

5.4 Multi-Homing Requirements for Site Border Routers

For multi-homing, the SBR does NOT need to be ILNP-capable for Host Multi-Homing or Site Multi-Homing. This is true provided the multi-homing is left to individual hosts as described above. In this deployment approach, the SBR need only issue Routing Advertisements (RAs) that are correct with respect to its upstream connectivity; that is, the SBR properly advertises routing prefixes (Locator values) to the ILNP hosts.

In such a scenario, when hosts in the site network see new Locator values, and see that a previous Locator value is no longer being advertised, those hosts can update their ILCCs, send Locator Updates to CNs, and change connectivity as required.

6. MOBILITY

ILNP supports mobility directly, rather than relying upon special-purpose mobility extensions as is the case with IPv6

[RFC6275]. There are two different mobility cases to consider:

a) Host Mobility: individual hosts may be mobile, moving across administrative boundaries or topological boundaries within an IP-based network, or across the Internet. Such hosts would need to independently manage their own mobility.

b) Network (Site) Mobility: a whole site, i.e. one (or more) IP subnetwork(s) may be mobile, moving across administrative boundaries or topological boundaries within an IP-based network, or across the Internet. The site as a whole needs to maintain consistency in connectivity.

Essentially, for ILNP, mobility is implemented by enabling:

a) Locator values to be changed dynamically by a node, including for active sessions.

b) use of Locator Updates to allow active sessions to be maintained.

c) for those hosts that expect incoming session requests (such as servers), updates to the relevant DNS entries for those hosts.

It is possible that a device is both a mobile host and part of a mobile network, e.g. a smartphone in a mobile site network. This is supported in ILNP as the mechanism for mobile hosts and mobile networks are very similar and work in harmony.

For mobility, there are two general features that must be supported:

a) Handover (or Hand-off): when a host changes its connectivity (e.g. it has a new SNPA as it moves to a new ILNP subnetwork), any active sessions for that host must be maintained with minimal disruption (i.e. transparently) to the upper layer protocols.

b) Rendezvous: when a host that expects incoming session requests has new connectivity (e.g. it has a new SNPA as it moves to a new ILNP subnetwork), it must update its relevant DNS entries so that name resolution will provide the correct I and L values to remote nodes.

6.1 Mobility/multi-homing duality in ILNP

Mobility and multi-homing present the same set of issues for ILNP. Indeed, mobility and multi-homing form a duality: the set of Locators associated with a node or site changes. The reason for the change might be different for the case of mobility and multi-homing, but the effects on the network session state and on correspondents is identical.

With ILNP, mobility and multi-homing are supported using a common set of mechanisms. In both cases, different Locator values are used to identify different IP subnetworks. Also, ILNP nodes that expect incoming session requests are assumed to have a Fully Qualified Domain Name (FQDN) stored in the Domain Name System (DNS), as is already done within the deployed Internet. ILNP mobility normally relies upon the Secure Dynamic DNS Update standard for mobile nodes to update their location information in the DNS. This approach of using DNS for rendezvous with mobile systems was proposed earlier by others [PHG02].

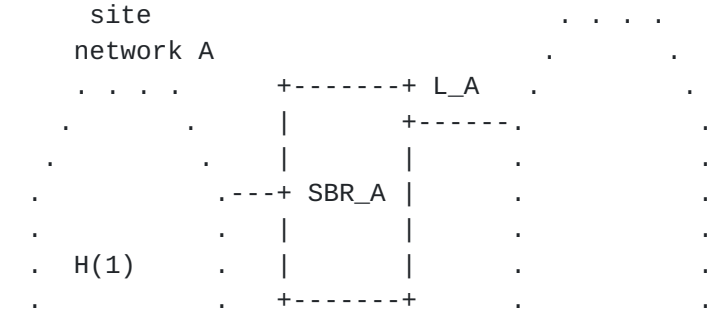
Host Mobility considers individual hosts that are individually mobile, for example a mobile telephone carried by a person walking in a city. Network (Site) Mobility considers a group of hosts within a local topology that move jointly and periodically change their uplinks to the rest of the Internet, for example a ship that has wired connections internally but one or more wireless uplinks to the rest of the Internet.

For ILNP, Host Mobility is analogous to Host Multi-homing (H-MH) and Network Mobility is analogous to Site Multi-homing (S-MH). So, mobility and multi-homing capabilities can be used together, without conflict.

6.2 Host Mobility

With host mobility, each individual end-system manages its own connectivity through the use of Locator values. (This is very similar to the situation described for H-MH in Sec 5.1.)

Let us consider the network in Figure 6.1.



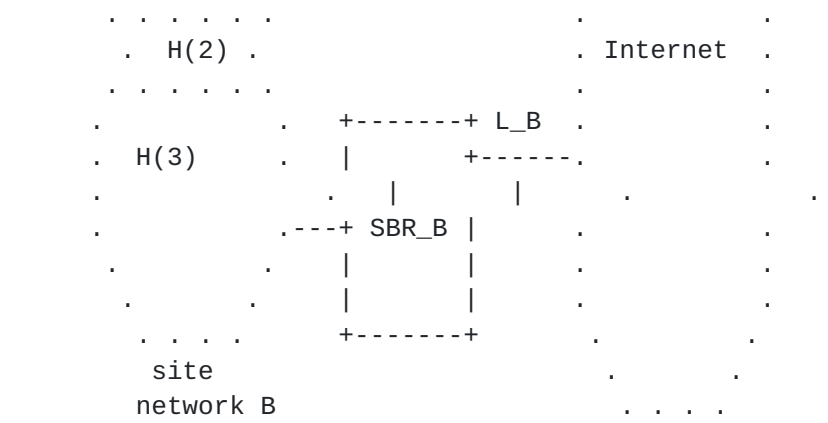


Figure 6.1: A simple mobile host scenario for ILNP.

A host, H is at position (1), hence H(1), in a site network A. This site network might be, for example, a single radio-cell under administrative domain A. We assume that the host will move into site network B, which might be a single radio-cell under administrative domain B. We also assume that the site networks have a region of overlap so that connectivity can be maintained, else, of course, the host will loose connectivity. Also, let us assume that the host already has ILNP connectivity in site network A.

If site network A has connectivity via Locator value L_A, and H uses Identifier value I_H with a single interface ra0, then the host's ILCC will contain:

```
[I_H, L_A]                                          --- (18a)
L_A, ra0                                            --- (18b)
```

Note the equivalence of expressions (18a) and (18b), respectively, with the expressions (15a) and (16a) for host multi-homing.

The host now moves into the overlap region of site networks A and B, and has position (2), H(2) as indicated in Fig 6.1. As this region is now in site network B, as well as site network A, H should see RAs from SBR_B for L_B, as well as the RAs for L_A from SBR_A. The host can now start to use L_B for its connectivity. The host H must now:

a) maintain existing active upper layer sessions: based on its current ILCC entries and active sessions, send Locator Update (LU) messages to CNs to notify them of the change of L values. (LU messages are synonymous to Mobile IPv6 Binding Updates.)

b) if required, update its relevant DNS entries with the new L value in the appropriate DNS records, to enable correct resolution for new incoming session requests.

However, it can opt to do this one of two ways:

1) immediate handover: the host sends Locator Update (LU) messages to CNs, immediately stops using L_A and switches to using L_B only. In this case, its ILCC entries change to:

[I_H, L_B] --- (19a)
L_B, ra0 --- (19b)

There might be packets in flight to H which use L_A and H MAY choose to ignore these on reception.

2) soft handover: the host sends Locator Update (LU) messages to CNS, but it uses both L_A and L_B until (i) it no longer receives incoming packets with destination Locator values set to L_A within a given time period (ii) it no longer sees RAs for L_A (i.e. it has left the overlap region and so has left site network A). In this case, its ILCC entries change to:

[I_H, L_A] --- (20a)
L_A, ra0 --- (20b)
[I_H, L_B] --- (20c)
L_B, ra0 --- (20d)

ILNP does not mandate the use of one handover option over another. Indeed, a host may implement both and decide, through local policy or other mechanisms (e.g. under the control of a particular transport protocol implementation), to use one or other for a specific session, as required.

Note that if using soft handover, when in the overlap region the host is multi-homed. Also, soft handover is likely to provide a less disruptive handover (e.g. lower packet loss) compared to immediate handover, all other things being equal.

There is a case where both the host and its correspondent node

are mobile. In the unlikely event of simultaneous motion which changes both nodes' Locators within a very small time period, there is the possibility that communication may be lost. If the communication between the nodes was direct (i.e. one node initiated communication with another, through a DNS lookup) a node can use the DNS to discover the new Locator value(s) for the other node. If the communication was through some sort of middlebox providing a relay service, then communication is more likely to disrupted only if the middlebox is also mobile.

It is also possible that high packet loss results in Locator Updates being lost, which could disrupt handover. However, this is an engineering issue and does not impact the basic concept of operation: additional discussion on this issue is provided in [ILNP-ENG].

Of course, for any handover, the new end-to-end path through SBR_B might have very different end-to-end path characteristics (e.g. different end-to-end delay, packet-loss, throughput). Also, the physical connectivity on interface ra0 as well as through SBR_B's uplink may be different. Such impact on end-to-end packet transfer are outside the scope of ILNP.

6.3 Network Mobility

For network mobility, a whole site may be mobile, e.g. the SBRs of Figure 6.1 has a radio uplink on a moving vehicle. Within the site, individual hosts may or may not be mobile.

In the simplest case, ILNP deals with mobile networks in the same way as for site multi-homing: the management of mobility is delegated to each host in the site, so it needs to be ILNP-capable. Each host, effectively, behaves as if it was a mobile host, even though it may not actually be mobile. Indeed, in this way, the mechanism is very similar to that for site multi-homing.

Let us consider the mobile network in Figure 6.2.

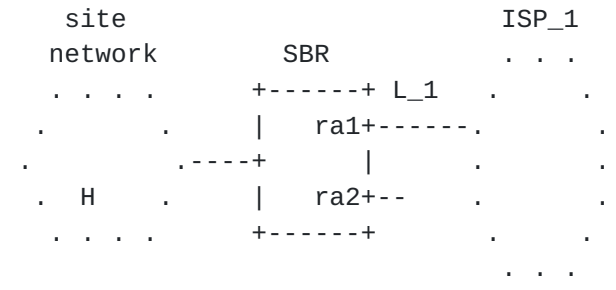


Figure 6.2a: ILNP mobile network before handover.

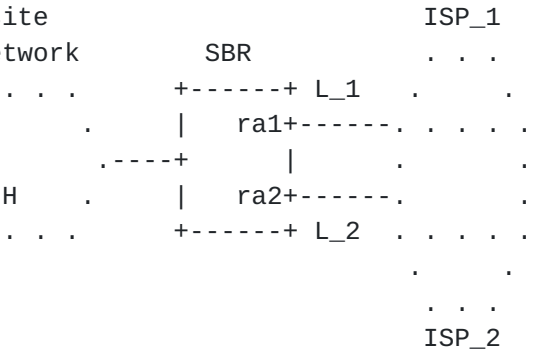


Figure 6.2b: ILNP mobile network during handover.

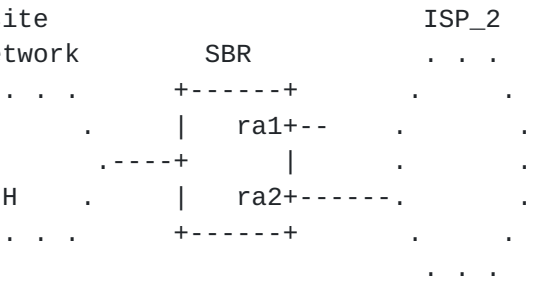


Figure 6.2c: ILNP mobile network after handover.

H = host
L_1 = global Locator value 1
L_2 = global Locator value 2
SBR = Site Border Router

Figure 6.2: A simple mobile network scenario for ILNP.

In Figure 6.2, we assume that the site network is mobile, and the SBR has two radio interfaces ra1 and ra2. However, this particular figure is chosen for simplicity and clarity for our scenario, and other configurations are possible, e.g. a single radio interface which uses separate radio channels (separate carriers, coding channels, etc.) In the figure, ISP_1 and ISP_2 are separate, radio-based service providers, accessible via ra1 and ra2.

In Fig 6.2a, the SBR has connectivity via ISP_1 using Locator value L_1. The host H, with interface ra0 and Identifier I_H, has an established connectivity via the SBR and so has ILCC entries as shown in (21):

[I_H, L_1] --- (21a)

L_1, ra0 --- (21b)

Note the equivalence to expressions (18a) and (18b). As the whole network moves, the SBR detects a new radio provider, ISP_2, and connects to it using ra2, as shown in Figure 6.2b, with the service areas of ISP_1 and ISP_2 overlapping. ISP_2 provides Locator L_2, which SBR advertises into the site network along with L_1. As with the mobile host scenario above, individual hosts may decide to perform immediate handover or soft handover. So, the ILCC state for H will be as for expressions (19a,b) and (20a,b,c,d), but with L_1 in place of L_A and L_2 in place of L_B. Finally, as in Figure 6.2c, the site network moves and is no longer served by ISP_1, and handover is complete. Note that during the handover the site is multi-homed, as in Figure 6.2b.

6.4 Mobility Requirements for Site Border Routers

As for multi-homing, the SBR does NOT need to be ILNP-capable: it simply needs to advertise the available routing prefixes into the site network. The mobility capability is handled completely by the hosts.

6.5 Mobility with multiple SBRs

Just as Section 5.3.1 describes the use of multiple routers for multi-homing, so it is possible to have multiple routers for mobility for ILNP, for both mobile hosts and mobile networks.

7. IP SECURITY FOR ILNP

IP Security for ILNP [ILNP-ENG] becomes simpler, in principle, than IP Security as it is today, based on the use of IP addresses as Identifiers.

An operational issue in the deployed IP Internet is that the IP Security protocols, AH and ESP, have Security Associations (IPsec SAs) that include the IP addresses of the secure session endpoints. This was understood to be a problem when AH and ESP were originally defined. However, the limited set of namespaces in the Internet Architecture did not provide any better choices at that time. ILNP provides more namespaces, thus now enabling better IPsec architecture and engineering.

7.1 Adapting IP security for ILNP

In essence, ILNP provides a very simple architectural change to IP security: in place of IP addresses as used today for SAs, ILNP uses Identifier values instead for SAs. Recall that Identifier values are immutable once in use, so they can be used to maintain end-to-end state for any protocol that requires it. Note from the discussion above that the Identifier values for a host remain unchanged when multi-homing and mobility is in use, so IP security using ILNP can work in harmony with multi-homing and mobility [ABH08b] [ABH09a].

To resolve the issue of IPsec interoperability through a Network Address Translator (NAT) deployment [RFC1631] [RFC3022], UDP encapsulation of IPsec [RFC3948] is commonly used as of the date this document was published. This special-case handling for IPsec traffic traversing a NAT is not needed with ILNP IPsec.

Further, it would obviate the need for specialised IPsec NAT Traversal mechanisms, thus simplifying IPsec implementations while enhancing deployability and interoperability [RFC3948].

This architectural change does not reduce the security provided by the IP Security protocols. In fact, had the Node Identifer namespace existed back in the early 1990s, IP Security would always have bound to that location-independent Node Identifier and would not have bound to IP Addresses.

7.2 Operational use of IP security with ILNP

Operationally, this change in SA bindings to use Identifiers rather than IP addresses causes problems for the use of the IPsec protocols through IP Network Address Translation (NAT) devices, with mobile nodes (because the mobile node's IP address changes at each network-layer handoff), and with multi-homed nodes (because the session is bound to a particular interface of the multi-homed node, rather than being bound to the node itself) [RFC3027] [RFC3715].

8. BACKWARDS COMPATIBILITY & INCREMENTAL DEPLOYMENT

ILNPv6 is fully backwards compatible with existing IPv6. No router software or silicon changes are necessary to support the proposed enhancements. An IPv6 router would be unaware whether the packet being forwarded were classic IPv6 or the proposed enhancement in ILNPv6. IPv6 Neighbour Discovery will work unchanged for ILNPv6. ILNPv6 multicasting is the same as IETF standards-track IPv6 multicasting.

ILNPv4 is backwards compatible with existing IPv4. As the IPv4 address fields are used as 32-bit Locators, using only the address prefix bits of the the 32-bit space, IPv4 routers also would not require changes. An IPv4 router would be unaware whether the packet being forwarded were classic IPv4 or the proposed enhancement in ILNPv4 [ILNP-V4OPTS]. ARP [RFC826] requires enhancements to support ILNPv4 [ILNP-ARP] [ILNP-ENG]. ILNPv4 multicasting is the same as IETF standards-track IPv4 multicasting.

If a node supports ILNP, and intends to receive incoming sessions, the node's Fully-Qualified Domain Name (FQDN) normally will have one or more NID records and one or more Locator (i.e. L32, L64, and/or LP) records associated with the node within the DNS [ILNP-ENG] [ILNP-DNS].

When a host ("initiator") initiates a new IP session with a correspondent ("responder"), it normally will perform a DNS lookup to determine the address(es) of the responder. An ILNP host normally will look for Node Identifier ("NID") and Locator (i.e. L32, L64, and LP) records in any received DNS replies. DNS servers that support NID and Locator (i.e. L32, L64, and LP) records SHOULD include them (when they exist) as additional data in all DNS replies to queries for DNS AAAA records [ILNP-DNS].

If the initiator supports ILNP, and from DNS information learns that the responder also supports ILNP, then the initiator will generate an unpredictable nonce value, cache that value locally as part of the session, and will include the ILNP Nonce value in its initial packet(s) to the responder [ILNP-ENG] [ILNP-NONCEv6] [ILNP-V4OPTS].

If the initiator node does not find any ILNP-specific DNS resource records for the responder node, then the initiator uses classic IP for the new session with the responder, rather than trying to use ILNP for that session. Of course, multiple transport-layer sessions can concurrently share a single network-layer (e.g. IP or ILNP) session.

If the responder node for a new IP session does not support ILNP and the responder node receives initial packet(s) containing the ILNP Nonce, the responder will drop the packet and send an ICMP error message back to the initiator. If the responder node for a new IP session supports ILNP and receives initial packet(s) containing the ILNP Nonce, the responder learns that ILNP is in use for that session (i.e. by the presence of that ILNP Nonce).

If the initiator node using ILNP does not receive a response from

the responder in a timely manner (e.g. within TCP timeout for a TCP session) and also does not receive an ICMP Unreachable error message for that packet, OR if the initiator receives an ICMP Parameter Problem error message for that packet, then the initiator concludes that the responder does not support ILNP. In this case, the initiator node SHOULD try again to create the new session, but this time using IP (and therefore omitting the ILNP Nonce).

Finally, since an ILNP node is also a fully-capable IP node, then the upgraded node can use any standardised IP mechanisms for communicating with a legacy IP-only node. So ILNP will not be worse than existing IP, but when ILNP is used the enhanced capability described in this document will be useable.

9. SECURITY CONSIDERATIONS

This proposal outlines a proposed evolution for the Internet Architecture to provide improved capabilities. This section discusses security considerations for this proposal.

Note that ILNP provides security equivalent to IP for similar threats when similar mitigations (e.g. IPsec or not) are in use. In some cases, but not all, ILNP exceeds that objective and has lower security risk than IP. Additional engineering details for several of these topics can be found in [ILNP-ENG].

9.1 Authentication of Locator Updates

All Locator Update messages are authenticated. ILNP requires use of a session nonce [ILNP-NONCEv6] [ILNP-V4OPTS] to prevent off-path attacks, and also allows use of IPsec cryptography to provide stronger protection where required.

Ordinary IP sessions are vulnerable to on-path attacks unless IP Security is used. So the Nonce Destination Option only seeks to provide protection against off-path attacks on an IP session -- equivalent to ordinary IP sessions when not using IP Security.

It is common to have non-symmetric paths between two nodes on the Internet. To reduce the number of on-path nodes that know the Nonce value for a given session when ILNP is in use, a nonce value is unidirectional, not bidirectional. For example, for a session between nodes A and B, one nonce value is used from A to B and a different nonce value is used from B to A.

ILNP sessions operating in higher risk environments SHOULD also

use the cryptographic authentication provided by IP Security *in addition* to concurrent use of the ILNP Nonce.

It is important to note that at present an IP session is entirely vulnerable to on-path attacks unless IPsec is in use for that particular IP session, so the security properties of the new proposal are never worse than for existing IP.

9.2 Forged Identifier Attacks

In the deployed Internet, active attacks using packets with a forged Source IP Address have been publicly known at least since early 1995 [CA-1995-01]. While these exist in the deployed Internet, they have not been widespread. This is equivalent to the issue of a forged Identifier value and demonstrates that this is not a new threat created by ILNP.

One mitigation for these attacks has been to deploy Source IP Address Filtering [RFC2827] [RFC3704]. Jun Bi at U. Tsinghua cites Arbor Networks as reporting that this mechanism has less than 50% deployment and cites an MIT analysis indicating that at least 25% of the deployed Internet permits forged source IP addresses.

In an other document [ILNP-ENG] there is a discussion of an accidental use of a duplicate Identifier on the Internet. However, this sub-section instead focuses on methods for mitigating attacks based on packets containing deliberately forged Source Identifier values.

Firstly, the recommendations of [RFC2827] & [RFC3704] remain. So any packets that have a forged Locator value can be easily filtered using existing widely available mechanisms.

Secondly, the receiving node does not blindly accept any packet with the proper Source Identifier and proper Destination Identifier as an authentic packet. Instead, each ILNP node maintains an ILNP Communication Cache (ILCC) for each of its correspondents, as described in [ILNP-ENG]. Information in the cache is used in validating received messages and preventing off-path attackers from succeeding. This process is discussed more in [ILNP-ENG]

Thirdly, any node can distinguish different nodes using the same Identifier value by other properties of their sessions. For example, IPv6 Neighbor Discovery prevents more than one node from using the same source I-LV at the same time on the same link [RFC4861]. So cases of different nodes using the same Identifier

value will involve nodes that have different sets of valid Locator values. A node thus can demultiplex based on the combination of Source Locator and Source Identifier if necessary. If IP Security is in use, the combination of the Source Identifier and the SPI value would be sufficient to demux two different sessions.

Fourthly, deployments in high threat environments also SHOULD use IP Security to authenticate control traffic and data traffic. Because IP Security for ILNP binds only to the Identifier values, and never to the Locator values, a mobile or multi-homed node can use IPsec even when its Locator value(s) have just changed.

Lastly, note well that ordinary IPv4, ordinary IPv6, Mobile IPv4, and also Mobile IPv6 already are vulnerable to forged Identifier and/or forged IP address attacks. An attacker on the same link as the intended victim simply forges the victims MAC address and the victim's IP address. With IPv6, when Secure Neighbour Discovery (SEND) and Cryptographically Generated Addresses (CGAs) are in use, the victim node can defend its use of its IPv6 address using SEND. With ILNP, when SEND and CGAs are in use, the victim node also can defend its use of its IPv6 address using SEND. There are no standard mechanisms to authenticate ARP messages, so IPv4 is especially vulnerable to this sort of attack. These attacks also work against Mobile IPv4 and Mobile IPv6. In fact, when either form of Mobile IP is in use, there are additional risks, because the attacks work not only when the attacker has access to the victim's current IP subnetwork but also when the attacker has access to the victim's home IP subnetwork. So the risks of using ILNP are not greater than exist today with IP or Mobile IP.

9.3 IP Security Enhancements

The IP Security standards are enhanced here by binding IPsec Security Associations (SAs) to the Identifiers of the session endpoints, rather than binding IPsec SAs to the IP Addresses as at present. This change enhances the deployability and interoperability of the IP Security standards, but does not decrease the security provided by those protocols. See Section 7 for a more detailed explanation.

9.4 DNS Security

The DNS enhancements proposed here are entirely compatible with, and can be protected using, the existing IETF standards for DNS Security [RFC4033]. The Secure DNS Dynamic Update mechanism used here is also used unchanged [RFC3007]. So ILNP does not change

the security properties of the DNS or of DNS servers.

9.5 Firewall Considerations

In the proposed new scheme, stateful firewalls are able to authenticate ILNP-specific control messages arriving on the external interface. This enables more thoughtful handling of ICMP messages by firewalls than is commonly the case at present. As the firewall is along the path between the communicating nodes, the firewall can snoop on the Session Nonce being carried in the initial packets of an ILNP session. The firewall can verify the correct nonce is present on incoming control packets, dropping any control packets that lack the correct nonce value.

By always including the nonce in ILNP-specific control messages, even when IP Security (IPsec) is also in use, the firewall can filter out off-path attacks against those ILNP messages without needing to perform computationally-expensive IPsec processing. In any event, a forged packet from an on-path attacker will still be detected when the IPsec input processing occurs in the receiving node; this will cause that forged packet to be dropped rather than acted upon.

9.6 Neighbour Discovery Authentication

Nothing in this proposal prevents sites from using the Secure Neighbour Discovery (SEND) proposal for authenticating IPv6 Neighbour Discovery with ILNPv6 [RFC3971].

9.7 Site Topology Obfuscation

A site that wishes to obscure its internal topology information MAY do so by deploying site border routers that rewrite the Locator values for the site as packets enter or leave the site. This operational scenario was presented in [ABH09a] and is discussed in more detail in [ILNP-ADV].

For example, a site might choose to use a ULA prefix internally for this reason [RFC4193] [ID-ULA]. In this case, the site border routers would rewrite the Source Locator of ILNP packets leaving the site to a global-scope Locator associated with the site. Also, those site border routers would rewrite the Destination Locator of packets entering the site from the global-scope Locator to an appropriate interior ULA Locator for the destination node [ABH08b] [ABH09a] [ILNP-ADV].

10. PRIVACY CONSIDERATIONS

ILNP has support for both:

- Location Privacy: to hide a node's topological location by obfuscating the ILNP Locator information. (See also Section 7 of [ILNP-ADV].)

- Identity Privacy: to hide a node's identity by allowing the allowing the use of Node Identifier values that are not tied to the node in some permanent or semi-permanent manner. (See also Section 11 of [ILNP-ENG].)

A more detailed exposition of the possibilities is given in [BAK11].

10.1 Location Privacy

Some users have concerns about the issue of "location privacy", whereby the user's location might be determined by others. The term "location privacy" does not have a crisp definition within the Internet community at present. Some mean the location of a node relative to the Internet's routing topology, while others mean the geographic coordinates of the node (i.e. latitude X, longitude Y). The concern seems to focus on Internet-enabled devices, most commonly handheld devices such as a "smart phone", that might have 1:1 mappings with individual users.

There is a fundamental trade-off here. Quality of a node's Internet connectivity tends to be inversely proportional to the "location privacy" of that node. For example, if a node were to use a router with NAT as a privacy proxy, routing all traffic to and from the Internet via that proxy, then (a) latency will increase as the distance increases between the node seeking privacy and its proxy, and (b) communications with the node seeking privacy will be more vulnerable to communication faults -- both due to the proxy itself (which might fail) and due to the longer path (which has more points of potential failure than a more direct path would have).

Any Internet node that wishes for other Internet nodes to be able to initiate communications sessions with it needs to include associated address (e.g. A, AAAA) or Locator (e.g. L32, L64, LP) records in the publicly accessible Domain Name System (DNS). Information placed in the DNS is publicly accessible. Since the goal of DNS is to distribute information to other Internet nodes, it does not provide mechanisms for selective privacy. Of course, a node that does not wish to be contacted need not be present in the DNS.

In some cases, various parties have attempted to create mappings between IP address blocks and geographic locations. The quality of such mappings appears to vary [GUF07]. Many such mapping efforts are driven themselves by efforts to comply with legal requirements in various legal jurisdictions. For example, some content providers reportedly have licenses authorising distribution of content in one set of locations, but not in a different set of locations.

ILNP does not compromise user location privacy any more than base IPv6. In fact, by its nature ILNP provides additional choices to the user to protect their location privacy.

10.2 Identity Privacy

Both ILNP and IPv6 permit use of identifier values generated using the IPv6 Privacy Address extension [RFC4941]. ILNP and IPv6 also support a node having multiple unicast addresses/locators at the same time, which facilitates changing the node's addresses/locators over time. IPv4 does not have any non-topological identifiers, and many IPv4 nodes only support 1 IPv4 unicast address per interface, so IPv4 is not directly comparable with IPv6 or ILNP.

In normal operation with IPv4, IPv6, or ILNP, a mobile node might intend to be accessible for new connection attempts from the global Internet and also might wish to have both optimal routing and maximal Internet availability, both for sent and received packets. In that case, the node will want to have its addressing or location information kept in the DNS and made available to others.

In some cases, a mobile node might only desire to initiate communications sessions with other Internet nodes, in which case the node need not be present in the DNS. Some potential correspondent nodes might, as a matter of local security policy, decline to communicate with nodes that do not have suitable DNS records present in the DNS. For example, some deployed IPv4-capable mail relays refuse to communicate with an initiating node that lacks an appropriate PTR record in the DNS.

In some cases, for example intermittent electronic mail access or browsing specific web pages, support for long-lived network sessions (i.e. where session lifetime is longer than the time the node remains on the same subnetwork) is not required. In those cases, support for node mobility (i.e. session continuity even when the SNPA changes) is not required and need not be used.

If an ILNP node that is mobile chooses not to use DNS for rendezvous, yet desires to permit any node on the global Internet to initiate communications with that node, then that node can fall back to using Mobile IPv4 or Mobile IPv6 instead.

Many residential broadband Internet users are subject to involuntary renumbering, usually when their ISP's DHCP server(s) deny a DHCP RENEW request and instead issue different IP addressing information to the residential user's device(s). In many cases, such users want their home server(s) or client(s) to be externally reachable. Such users today often use Secure DNS Dynamic Update to update their addressing or location information in the DNS entries, for the devices they wish to make reachable from the global Internet [RFC2136] [RFC3007] [LA2006]. This option exists for those users, whether they use IPv4, IPv6, or ILNP. Users also have the option not to use such mechanisms.

11. IANA CONSIDERATIONS

This document has no IANA considerations.

(Note to RFC Editor; this section can be removed prior to publication as an RFC.)

12. REFERENCES

This section provides normative and informative references relating to this note.

12.1. Normative References

[RFC768] J. Postel, "User Datagram Protocol", RFC768, August 1980.

[RFC791] J. Postel, "Internet Protocol", RFC791, September 1981.

[RFC793] J. Postel, "Transmission Control Protocol", RFC793, September 1981.

[RFC826] D. Plummer, "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware", RFC 826, November 1982.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] S. Deering & R. Hinden, "Internet Protocol Version 6 Specification", RFC2460, December 1998.

[RFC3007] B. Wellington, "Secure Domain Name System Dynamic Update", RFC3007, November 2000.

[RFC3484] R. Draves, "Derfault Address Selection for IPv6", RFC 3484, February 2003.

[RFC4033] R. Arends, et alia, "DNS Security Introduction and Requirements", RFC4033, March 2005.

[RFC4219] R. Hinden & S. Deering, "IP Version 6 Addressing Architecture", RFC4219, February 2006.

[RFC4861] T. Narten, E. Nordmark, W. Simpson, & H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[ILNP-ARP] R.J. Atkinson & S.N. Bhatti, "ARP Extension for ILNPv4", draft-irtf-rrg-ilnp-arp, May 2012.

[ILNP-ENG] R.J. Atkinson & S.N. Bhatti, "ILNP Engineering and Implementation Considerations", draft-irtf-rrg-ilnp-eng, May 2012.

[ILNP-DNS] R.J. Atkinson, S.N. Bhatti, & Rose, "DNS Resource Records for ILNP", draft-irtf-rrg-ilnp-dns, May 2012.

[ILNP-ICMPv4] R.J. Atkinson & S.N. Bhatti, "ICMPv4 Locator Update message" draft-irtf-rrg-ilnp-icmpv4, May 2012.

[ILNP-ICMPv6] R.J. Atkinson & S.N. Bhatti, "ICMPv6 Locator Update message", draft-irtf-rrg-ilnp-icmpv6, May 2012.

[ILNP-NONCEv6] R.J. Atkinson & S.N. Bhatti, "IPv6 Nonce Destination Option for ILNPv6", draft-irtf-rrg-ilnp-noncev6, May 2012.

[ILNP-V4OPTS] R. Atkinson & S. Bhatti, "IPv4 Options for ILNP", draft-irtf-rrg-ilnp-v4opts, May 2012.

12.2. Informative References

[8+8] M. O'Dell, "8+8 - An Alternate Addressing Architecture for IPv6", Internet-Draft, October 1996.

[ABH07a] R. Atkinson, S. Bhatti, & S. Hailes, "Mobility as an Integrated Service Through the Use of Naming", Proceedings of ACM MobiArch 2007, August 2007, Kyoto, Japan.

[ABH07b] R. Atkinson, S. Bhatti, & S. Hailes, "A Proposal for Unifying Mobility with Multi-Homing, NAT, & Security", Proceedings of ACM MobiWAC 2007, Chania, Crete. ACM, October 2007.

[ABH08a] R. Atkinson, S. Bhatti, & S. Hailes, "Mobility Through Naming: Impact on DNS", Proceedings of ACM MobiArch 2008, August 2008, ACM, Seattle, WA, USA.

[ABH08b] R. Atkinson, S. Bhatti, & S. Hailes, "Harmonised Resilience, Security, and Mobility Capability for IP", Proceedings of IEEE Military Communications (MILCOM) Conference, San Diego, CA, USA, November 2008.

[ABH09a] R. Atkinson, S. Bhatti, & S. Hailes, "Site-Controlled Secure Multi-Homing and Traffic Engineering For IP", Proceedings of IEEE Military Communications (MILCOM) Conference, Boston, MA, USA, October 2009.

[ABH09b] R. Atkinson, S. Bhatti, & S. Hailes, "ILNP: Mobility, Multi-Homing, Localised Addressing and Security Through Naming", Telecommunications Systems, Volume 42, Number 3-4, pp 273-291, Springer-Verlag, December 2009, ISSN 1018-4864.

[ABH10] R. Atkinson, S. Bhatti, S. Hailes, "Evolving the Internet Architecture Through Naming", IEEE Journal on Selected Areas in Communication (JSAC), vol. 28, no. 8, pp. 1319-1325, IEEE, Piscataway, NJ, USA, Oct 2010.

[BA11] S. Bhatti & R. Atkinson, "Reducing DNS Caching", Proc. of 14th IEEE Global Internet Symposium (GI2011), Shanghai, China. 15 April 2011.

[BAK11] S. Bhatti, R. Atkinson, & J. Klemets, "Integrating Challenged Networks", Proc. of IEEE Military Communications Conference (MILCOM), Baltimore, USA. 09-12 Nov 2011.

[CA-1995-01] US CERT, "IP Spoofing Attacks and Hijacked Terminal Connections", CERT Advisory 1995-01, Issued 23 JAN 1995, Revised 23 SEP 1997.

[GSE] M. O'Dell, "GSE - An Alternate Addressing Architecture for IPv6", Internet-Draft, February 1997.

[ID-ULA] R. Hinden, G. Huston, & T. Narten, "Centrally Assigned Unique Local IPv6 Unicast Addresses", draft-ietf-ipv6-ula-central-02.txt, 15 June 2007.

[IEEE-EUI] IEEE, "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", http://standards.ieee.org/regauth/oui/tutorials/EUI64.html, IEEE, Piscataway, NJ, USA, March 1997.

[IEN1] C.J. Bennett, S.W. Edge, & A.J. Hinchley, "Issues in the Interconnection of Datagram Networks", Internet Experiment Note (IEN) 1, INDRA Note 637, PSPWN 76, University College London, London, England, UK, WC1E 6BT, 29 July 1977. http://www.postel.org/ien/ien001.pdf

[IEN19] J. F. Shoch, "Inter-Network Naming, Addressing, and Routing", IEN-19, January 1978.

[IEN23] J. F. Shoch, "On Names, Addresses, and Routings", IEN-23, January 1978.

[IEN31] D. Cohen, "On Names, Addresses, and Routings (II)", IEN-31, April 1978.

[ILNP-ADV] R. Atkinson & S. N. Bhatti, "Optional Advanced Deployment Scenarios for ILNP", draft-irtf-rrg-ilnp-adv, January 2012.

[IPng95] D. Clark, "A thought on addressing", electronic mail message to IETF IPng WG, Message-ID: 9501111901.AA28426@caraway.lcs.mit.edu, Laboratory for Computer Science, MIT, Cambridge, MA, USA, 11 January 1995.

[LA2006] C. Liu & P. Albitz, "DNS & Bind", 5th Edition, O'Reilly & Associates, Sebastopol, CA, USA, May 2006. ISBN 0-596-10057-4

[LABH06] M. Lad, R. Atkinson, S. Bhatti, and S. Hailes, "A Proposal for Coalition Networking in Dynamic Operational Environments", Proc. MILCOM2006 - 25th IEEE Military Communications Conference, Washington DC, USA. Nov 2006.

[PHG02] A. Pappas, S. Hailes, & R. Giaffreda, "Mobile Host Location Tracking through DNS", Proceedings of IEEE London Communications Symposium, IEEE, London, England, UK, September 2002.

[RAB09] D. Rehunthan, R. Atkinson, & S. Bhatti, "Enabling Mobile Networks Through Secure Naming", Proc. of IEEE Military Communications Conference (MILCOM), Boston, MA, USA, October 2009.

[RB10] D. Rehunathan and S. Bhatti, "A Comparative Assessment of Routing for Mobile Networks", Proc. WiMob2010 - 6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Niagara Falls, Canada, 11-13 Oct 2010.

[SBK02] Alex C. Snoeren, Hari Balakrishnan, & M. Frans Kaashoek, "Reconsidering Internet Mobility", Proceedings of 8th Workshop on Hot Topics in Operating Systems, 2002.

[SIPP94] Bob Smart, "Re: IPng Directorate meeting in Chicago; possible SIPP changes", electronic mail to the IETF SIPP WG mailing list, Message-ID: 199406020647.AA09887@shark.mel.dit.csiro.au, Commonwealth Scientific & Industrial Research Organisation (CSIRO), Melbourne, VIC, 3001, Australia, 2 June 1994.

[SRC84] J. Saltzer, D. Reed, & D. Clark, "End to End Arguments in System Design", ACM Transactions on Computer Systems, Volume 2, Number 4, ACM, New York, NY, USA, November 1984.

[RFC814] D.D. Clark, "Names, Addresses, Ports, and

Routes", RFC814, July 1982.

[RFC1122] R. Braden, "Requirements for Internet Hosts - Communication Layers", RFC1122, October 1989.

[RFC1498] J.H. Saltzer, "On the Naming and Binding of Network Destinations", RFC1498, August 1993.

[RFC1631] K. Egevang & P. Francis, "The IP Network Address Translator (NAT)", RFC1631, May 1994.

[RFC1958] B. Carpenter (Ed.), "Architectural Principles of the Internet", RFC1958, June 1996.

[RFC1992] I. Castineyra, N. Chiappa, & M. Steenstrup, "The Nimrod Routing Architecture", RFC1992, August 1996.

[RFC2101] B. Carpenter, J. Crowcroft, & Y. Rekhter, "IPv4 Address Behaviour Today", RFC2101, February 1997.

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic Updates in the Domain Name System", RFC2136, April 1997.

[RFC2827] P. Ferguson & D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC2827, May 2000.

[RFC2956] M. Kaat, "Overview of 1999 AB WOrkshop", RFC2956, October 2000.

[RFC3177] IAB and IESG, "IAB/IESG Recommendations on IPv6 Address Allocations to Sites", RFC3177, September 2001.

[RFC3022] P. Srisuresh & K. Egevang, "Traditional IP Network Address Translator", RFC3022, January 2001.

[RFC3027] M. Holdrege and P Srisuresh, "Protocol Complications of the IP Network Address Translator", RFC3027, January 2001.

[RFC3704] F. Baker & P. Savola, "Ingress Filtering for Multihomed Networks, RFC3704, March 2004.

[RFC3715] B. Aboba and W. Dixon, "IPsec-Network Address Translation (NAT) Compatibility Requirements", RFC3715, March 2004.

[RFC6275] C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6", RFC6275, July 2011.

[RFC3948] A. Huttunen, et alia, "UDP Encapsulation of IPsec ESP Packets", RFC3948, January 2005.

[RFC3971] J. Arkko, J. Kempf, B. Zill, & P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC3971 March 2005.

[RFC3972] T. Aura, "Cryptographically Generated Addresses (CGAs)", RFC3972, March 2005.

[RFC4193] R. Hinden & B. Haberman, "Unique Local IPv6 Unicast Addresses, RFC4193, October 2005.

[RFC4291] R. Hinden & S. Deering, "IP version 6 Addressing Architecture", RFC4291, February 2006.

[RFC4581] M. Bagnulo & J. Arkko, "Cryptographically Generated Addresses Extension Field Format", RFC4581, October 2006.

[RFC4941] T. Narten, R. Draves, & S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC4941, September 2007.

[RFC4982] M. Bagnulo & J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses", RFC4982, July 2007.

[RFC4984] D. Meyer, L. Zhang, K. Fall, "Report from the IAB Workshop on Routing and Addressing", RFC4984, September 2007.

[RFC5061] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, & M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC5061, September 2007.

[RFC6177] T. Narten, G. Huston, L. Roberts, "IPv6 Address Assignment to End Sites", RFC6177 (BCP157), March 2011.

[GUF07] B. Gueye, S. Uhlig, & S. Fdida, "Investigating the Imprecision of IP Block-Based Geolocation", Lecture Notes in Computer Science, Volume 4427, pp. 237-240, Springer-Verlag, Heidelberg, Germany, 2007.

ACKNOWLEDGEMENTS

Steve Blake, Stephane Bortzmeyer, Mohamed Boucadair, Noel Chiappa, Wes George, Steve Hailes, Joel Halpern, Mark Handley, Volker Hilt, Paul Jakma, Dae-Young Kim, Tony Li, Yakov Rehkter, Bruce Simpson, Robin Whittle and John Wroclawski (in alphabetical order) provided review and feedback on earlier versions of this document. Steve Blake provided an especially thorough review of an early version of the entire ILNP document set, which was extremely helpful. We also wish to thank the anonymous reviewers of the various ILNP papers for their feedback.

Roy Arends provided expert guidance on technical and procedural aspects of DNS issues.

Noel Chiappa graciously provided the authors with copies of the original email messages cited here as [SIPP94] and [IPng95], which enabled the precise citation of those messages herein.

RFC EDITOR NOTE

This section is to be removed prior to publication.

Please note that this document is written in British English, so British English spelling is used throughout. This is consistent with existing practice in several other RFCs, for example RFC-5887.

This document tries to be very careful with history, in the interest of correctly crediting ideas to their earliest identifiable author(s). So in several places the first published RFC about a topic is cited rather than the most recent published RFC about that topic.

Author's Address

RJ Atkinson
Consultant
San Jose, CA
95125 USA

Email: rja.lists@gmail.com

SN Bhatti
School of Computer Science
University of St Andrews
North Haugh, St Andrews
Fife, Scotland
KY16 9SX, UK

Email: saleem@cs.st-andrews.ac.uk

Expires: 29 NOV 2012