RJ Atkinson
Consultant
SN Bhatti
U. St Andrews

10 JUL 2012

ARP Extension for ILNPv4
draft-irtf-rrg-ilnp-arp-07.txt

Status of this Memo

Distribution of this memo is unlimited.

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other 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, and 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 defines an Address Resolution Protocol (ARP) extension to support ILNP for IPv4 (ILNPv4). ILNP is is an experimental, evolutionary enhancement to IP. This document is a product of the IRTF Routing RG.

Table of Contents

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.

The Identifier Locator Network Protocol (ILNP) is a proposal for evolving the Internet Architecture. It differs from the current Internet Architecture primarily by deprecating the concept of an IP Address, and instead defining two new objects, each having crisp syntax and semantics. The first new object is the Locator, a topology-dependent name for a subnetwork. The other new object is the Identifier, which provides a topology-independent name for a node.

1.1 ILNP Document Roadmap

This document describes describes extensions to ARP for use with ILNPv4.

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. 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-ARCH] is the main architectural description of ILNP, including the concept of operations.

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

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

d) [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.

e) [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.

f) [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.

g) [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.

h) [ILNP-ADV] describes optional engineering and deployment functions for ILNP. These are not required for the operation or use of ILNP and are provided as additional options.

1.2 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. ARP Extensions for ILNPv4

ILNP for IPv4 (ILNPv4) is merely a different instantiation of the ILNP architecture, so it retains the crisp distinction between the Locator and the Identifier. As with ILNPv6, only the Locator values are used for routing and forwarding ILNPv4 packets [ILNP-ARCH]. As with ILNP for IPv6 (ILNPv6), when ILNPv4 is used for a network-layer session, the upper-layer protocols (e.g. TCP/UDP pseudo-header checksum, IPsec Security Association) bind only to the Identifiers, never to the Locators [ILNP-ENG].

However, just as the packet format for IPv4 is different to IPv6, so the engineering details for ILNPv4 are different also. While ILNPv6 is carefully engineered to be fully backwards-compatible

with IPv6 Neighbor Discovery, ILNPv4 relies upon an extended version of the Address Resolution Protocol (ARP) [RFC826] which is defined here. While ILNPv4 could have been engineered to avoid changes in ARP, that would have required that the ILNPv4 Locator (i.e. L32) have slightly different semantics, which was architecturally undesirable.

The packet formats used are direct extensions of the existing widely deployed ARP Request (OP code 1) and ARP Reply (OP code 2) packet formats. This design was chosen for practical engineering reasons (i.e. to maximise code reuse), rather than for maximum protocol design purity.

We anticipate that ILNPv6 is much more likely to be widely implemented and deployed than ILNPv4. However, having a clear definition of ILNPv4 helps demonstrate the difference between architecture and engineering, and also demonstrates that the common ILNP architecture can be instantiated in different ways with different existing network-layer protocols.

2.1 ILNPv4 ARP Request Packet Format

The ILNPv4 ARP Request is an extended version of the widely deployed ARP Request (OP code 1). For experimentation purposes, the ILNPv4 ARP Request OP code uses decimal value 24. It is important to note that decimal value 24 is a pre-defined, shared-use experimental OP code for ARP [RFC5494], and is not uniquely assigned to ILNPv4 ARP Requests. The ILNPv4 ARP Request extension permits the Node's Identifier (NID) values to be carried in the ARP message, in addition to the node's 32-bit Locator (L32) values [ILNP-DNS].

```
        0        7        15       23       31
        +--------+--------+--------+--------+
        |       HT        |        PT       |
        +--------+--------+--------+--------+
        |  HAL   |  PAL   |        OP       |
        +--------+--------+--------+--------+
        |         S_HA (bytes 0-3)          |
        +--------+--------+--------+--------+
        | S_HA (bytes 4-5)|S_L32 (bytes 0-1)|
        +--------+--------+--------+--------+
        |S_L32 (bytes 2-3)|S_NID (bytes 0-1)|
        +--------+--------+--------+--------+
        |         S_NID (bytes 2-5)         |
        +--------+--------+--------+--------+
        |S_ID (bytes 6-7) | T_HA (bytes 0-1)|
```

```
        +--------+--------+--------+--------+
        |         T_HA (bytes 3-5)          |
        +--------+--------+--------+--------+
        |         T_L32 (bytes 0-3)         |
        +--------+--------+--------+--------+
        |         T_NID (bytes 0-3)         |
        +--------+--------+--------+--------+
        |         T_NID (bytes 4-7)         |
        +--------+--------+--------+--------+
```

Figure 2.1: ILNPv4 ARP Request packet format

In the diagram of Fig 2.1, the fields are as follows:

HT	Hardware Type (*)
PT	Protocol Type (*)
HAL	Hardware Address Length (*)
PAL	Protocol Address Length (uses new value 12)
OP	Operation Code (uses experimental value OP_EXP1=24)
S_HA	Sender Hardware Address (*)
S_L32	Sender L32 (* same as Sender IPv4 address for ARP)
S_NID	Sender Node Identifier (8 bytes)
T_HA	Target Hardware Address (*)
T_L32	Target L32 (* same as Target IPv4 address for ARP)
T_NID	Target Node Identifier (8 bytes)

The changed OP code indicates that this is ILNPv4 and not IPv4. The semantics and usage of the ILNPv4 ARP Request are identical to the existing ARP Request (OP code 2), except that the ILNPv4 ARP Request is sent only by nodes that support ILNPv4.

The field descriptions marked with "*" should have the same values as for ARP as used for IPv4.

2.2 ILNPv4 ARP Reply Packet Format

The ILNPv4 ARP Reply is an extended version of the widely deployed ARP Reply (OP code 2). For experimentation purposes, the ILNPv4 ARP Request OP code uses decimal value 25. It is important to note that decimal value 25 is a pre-defined, shared-use experimental OP code for ARP [RFC5494], and is not uniquely assigned to ILNPv4 ARP Requests. Th ILNPv4 ARP Reply extension permits the Node's Identifier (NID) values to be carried in the ARP message, in addition to the node's 32-bit Locator (L32) values [ILNP-DNS].

```
        0        7        15       23       31
```

```
+--------+--------+--------+--------+
|       HT        |        PT       |
+--------+--------+--------+--------+
|  HAL   |  PAL   |        OP       |
+--------+--------+--------+--------+
|         S_HA (bytes 0-3)          |
+--------+--------+--------+--------+
| S_HA (bytes 4-5)|S_L32 (bytes 0-1)|
+--------+--------+--------+--------+
|S_L32 (bytes 2-3)|S_NID (bytes 0-1)|
+--------+--------+--------+--------+
|         S_NID (bytes 2-5)         |
+--------+--------+--------+--------+
|S_ID (bytes 6-7) | T_HA (bytes 0-1)|
+--------+--------+--------+--------+
|         T_HA (bytes 3-5)          |
+--------+--------+--------+--------+
|         T_L32 (bytes 0-3)         |
+--------+--------+--------+--------+
|         T_NID (bytes 0-3)         |
+--------+--------+--------+--------+
|         T_NID (bytes 4-7)         |
+--------+--------+--------+--------+
```

Figure 2.2: ILNPv4 ARP Reply packet format

In the diagram of Fig 2.2, the fields are as follows:

HT	Hardware Type (*)
PT	Protocol Type (*)
HAL	Hardware Address Length (*)
PAL	Protocol Address Length (uses new value 12)
OP	Operation Code (uses experimental value OP_EXP2=25)
S_HA	Sender Hardware Address (*)
S_L32	Sender L32 (* same as Sender IPv4 address for ARP)
S_NID	Sender Node Identifier (8 bytes)
T_HA	Target Hardware Address (*)
T_L32	Target L32 (* same as Target IPv4 address for ARP)
T_NID	Target Node Identifier (8 bytes)

The changed OP code indicates that this is ILNPv4 and not IPv4. The semantics and usage of the ILNPv4 ARP Reply are identical to the existing ARP Reply (OP code 2), except that the ILNPv4 ARP Reply is sent only by nodes that support ILNPv4.

The field descriptions marked with "*" should have the same values as for ARP as used for IPv4.

2.3 Operation and Implementation of ARP for ILNPv4

The operation of ARP for ILNPv4 is almost identical to that for IPv4. Essentially, the key difference is:

a) where an IPv4 ARP Request would use IPv4 addresses, an ILNPv4 ARP Request MUST use:
   1. a 32-bit L32 value (_L32 suffixes in Figs 2.1 & 2.2)
   2. a 64-bit NID value (_NID suffixes in Figs 2.1 & Fig 2.2)

b) where an IPv4 ARP Reply would use IPv4 addresses, an ILNPv4 ARP Reply MUST use:
   1. a 32-bit L32 value (_L32 suffixes in Figs 2.1 & 2.2)
   2. a 64-bit NID value (_NID suffixes in Figs 2.1 & Fig 2.2)

As the OP codes 24 and 25 are distinct from ARP for IPv4, but the packet formats are Figs 2.1 and 2.2 are, effectively, extended versions of the corresponding ARP packets, it should be possible to implement this extension of ARP by extending existing ARP implementations rather than having to write an entirely new implementation for ILNPv4. It should be emphasised, however, that OP codes 24 and 25 are for experimental use as defined in [RFC5494], and so it is possible that other experimental protocols could be using these OP codes concurrently.

3. SECURITY CONSIDERATIONS

Security considerations for the overall ILNP Architecture are described in [ILNP-ARCH]. Additional common security considerations applicable to ILNP are described in [ILNP-ENG]. This section describes security considerations specific to the specific ILNPv4 topics discussed in this document.

The existing widely deployed Address Resolution Protocol (ARP) for IP version 4 (IPv4) is a link-layer protocol, so it is not vulnerable to off-link attackers. In this way, it is a bit different than IPv6 Neighbor Discovery (ND); IPv6 ND is a subset of the Internet Control Message Protocol (ICMP), which runs over the Internet Protocol version 6 (IPv6).

However, ARP does not include any form of authentication, so current ARP deployments are vulnerable to a range of attacks from on-link nodes. For example, it is possible for one node on a link to forge an ARP packet claiming to be from another node, thereby "stealing" the other node's IPv4 address. [RFC5227] both describes several of these risks and also describes some measures that an ARP implementation can use to reduce the chance of

accidental IPv4 address misconfiguration and also to detect such misconfiguration if it should occur.

This extension does not change the security risks that are inherent in using ARP.

In situations where additional protection against on-link attackers is needed, for example within high-risk operational environments, the IEEE standards for link-layer security [IEEE-802.1-AE] SHOULD be implemented and deployed.

Implementers of this specification need to understand that the 2 OP code values used for these 2 extensions are not uniquely assigned to ILNPv4. Other experimenters might be using the same 2 OP code values at the same time for different ARP-related experiments. Absent prior coordination among all users of a particular IP subnetwork, different experiments might be occurring on the same IP subnetwork. So implementations of these 2 ARP extensions ought to be especially defensively coded.

4. IANA CONSIDERATIONS

This document makes no request of IANA.

If in future the IETF decided to standardise ILNPv4, then allocation of unique ARP OP codes for the two extensions above as part of the IETF standardisation process would be sensible.

5. REFERENCES

This document has both Normative and Informational References.

5.1 Normative References

[RFC826]   D. Plummer, "An Ethernet Address Resolution Protocol", RFC-826, Nov 1982.

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

[RFC5227]   S. Cheshire, "IPv4 Address Conflict Detection", RFC-5227, July 2008.

[RFC5494]   J. Arkko & C. Pignataro, "IANA Allocation Guidelines for the Address Resolution Protocol", RFC-5494, April 2009.

[IEEE-802.1-AE] IEEE, "Media Access Control (MAC) Security",
IEEE Standard 802.1 AE, 18 August 2006, IEEE,
New York, NY, 10016, USA.

[ILNP-ARCH] R.J. Atkinson & S.N. Bhatti,
"ILNP Architectural Description",
draft-irtf-rrg-ilnp-arch, 10 July 2012.

[ILNP-DNS] R.J. Atkinson, S.N. Bhatti, & S Rose,
"DNS Resource Records for ILNP",
draft-irtf-rrg-ilnp-dns, 10 July 2012.

[ILNP-ENG] R.J. Atkinson & S.N. Bhatti,
"ILNP Engineering and Implementation Considerations",
draft-irtf-rrg-ilnp-eng, 10 July 2012.

[ILNP-ICMPv4] R.J. Atkinson & S.N. Bhatti,
"ICMPv4 Locator Update message"
draft-irtf-rrg-ilnp-icmpv4, 10 July 2012.

[ILNP-v4OPTS] R.J. Atkinson & S.N. Bhatti,
"IPv4 Options for ILNP",
draft-irtf-rrg-ilnp-v4opts, 10 July 2012.

5.2 Informative References

[ILNP-ICMPv6] R.J. Atkinson & S.N. Bhatti,
"ICMPv6 Locator Update message"
draft-irtf-rrg-ilnp-icmpv6, 10 July 2012.

[ILNP-NONCEv6] R.J. Atkinson & S.N. Bhatti,
"IPv6 Nonce Destination Option for ILNPv6",
draft-irtf-rrg-ilnp-noncev6, 10 July 2012.

[ILNP-ADV] R.J. Atkinson & S.N. Bhatti,
"Optional Advanced Deployment Scenarios for ILNP",
draft-irtf-rrg-ilnp-adv, 10 July 2012.

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.

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: 10 JAN 2013