Internet Draft
draft-irtf-rrg-ilnp-arp-01.txt
Expires: 26 OCT 2012
Category: Experimental

RJ Atkinson
Consultant
SN Bhatti
U. St Andrews

March 26, 2012

ARP Extension for ILNPv4
draft-irtf-rrg-ilnp-arp-01.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, 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.....
2. ARP Extension for ILNPv4.....
3. Security Considerations.....
4. IANA Considerations.....
5. References.....

1. INTRODUCTION

The Identifier Locator Network Protocol (ILNP) is an 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

The ILNP Architecture document [ILNP-ARCH] is the best place to start reading about ILNP. ILNP has multiple instantiations. [ILNP-ENG] discusses engineering and implementation aspects common to all instances of ILNP. This document discusses engineering and implementation details that are specific to ILNP for IPv4 (ILNPv4). [ILNP-DNS] describes new Domain Name System (DNS) resource records used with ILNP. [ILNP-ICMPv4] defines the ICMP Locator Update message used with ILNPv4. [ILNP-v4opts] defines new IPv4 options for use with ILNPv4. Other documents describe ILNP for IPv6 (ILNPv6) [ILNP-ICMPv6] [ILNP-NONCE6].

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. [RFC-2119]

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) 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 (Opcode 1) and ARP Reply (Opcode 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 (OP code XXX) is an extended version of the widely deployed ARP Request (Opcode 1). This extension permits the node's Identifier (I) values to be carried in the ARP message, in addition to the node's 32-bit Locator (L32) values [ILNP-DNS].

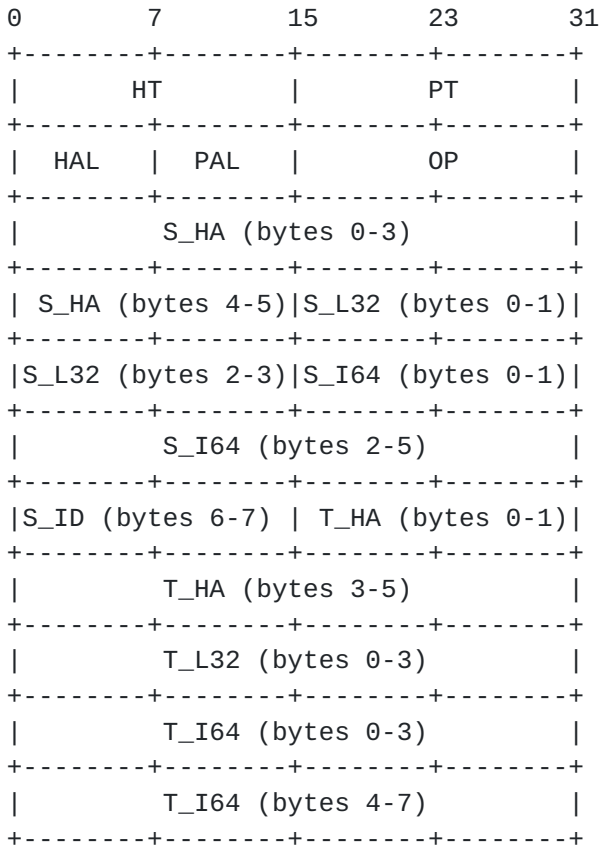


Figure 2.1: ILNPv4 ARP Request packet format

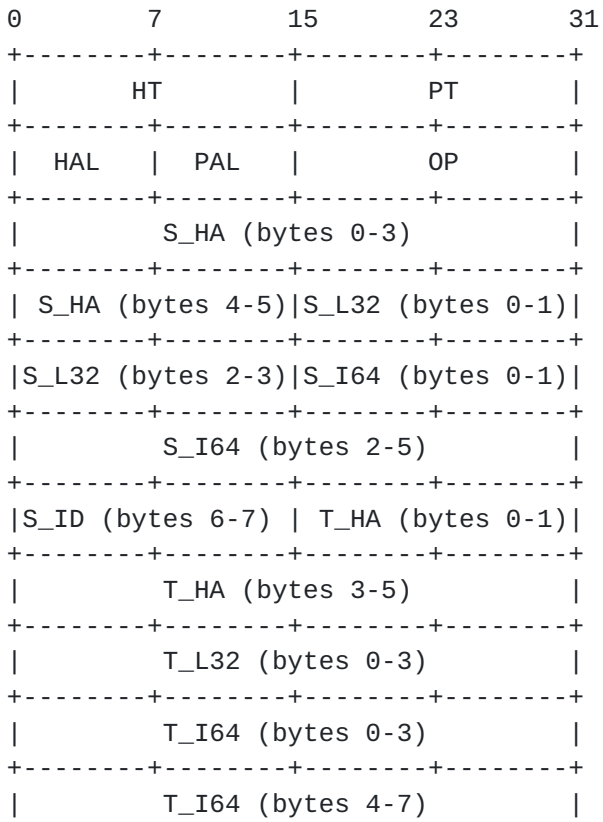
In the diagram of Fig 2.1, the fields are as follows:

HT	Hardware Type (same as for ARP; unchanged)
PT	Protocol Type (same as for ARP; unchanged)
HAL	Hardware Address Length (same as for ARP; unchanged)
PAL	Protocol Address Length (uses new value 12)
OP	Operation Code (uses new value XXX)
S_HA	Sender Hardware Address (same as for ARP; unchanged)
S_L32	Sender L32 (same as Sender IPv4 address for ARP)
S_I64	Sender Identifier (8 bytes)
T_HA	Target Hardware Address (same as for ARP; unchanged)
T_L32	Target L32 (same as Target IPv4 address for ARP)
T_I64	Target 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 (Opcode 2), except that the ILNPv4 ARP Request is sent only by nodes that support ILNPv4.

2.2 ILNPv4 ARP Reply Packet Format

The ILNPv4 ARP Reply (OP code YYY) is an extended version of the widely deployed ARP Reply (OP code 2). This extension permits the node's Identifier (I) values to be carried in the ARP message, in addition to the node's 32-bit Locator (L32) values [ILNP-DNS].



```
    +--------+--------+--------+--------+
```

Figure 2.2: ILNPv4 ARP Reply packet format

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

HT	Hardware Type (same as for ARP; unchanged)
PT	Protocol Type (same as for ARP; unchanged)
HAL	Hardware Address Length (same as for ARP; unchanged)
PAL	Protocol Address Length (uses new value 12)
OP	Operation Code (uses new value YYY)
S_HA	Sender Hardware Address (same as for ARP; unchanged)
S_L32	Sender L32 (same as Sender IPv4 address for ARP)
S_I64	Sender Identifier (8 bytes)
T_HA	Target Hardware Address (same as for ARP; unchanged)
T_L32	Target L32 (same as Target IPv4 address for ARP)
T_I64	Target 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 (Opcode 2), except that the ILNPv4 ARP Reply is sent only by nodes that support ILNPv4.

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 L value (_L32 suffixes in Figs 2.1 & 2.2)
   2. a 64-bit I value (_I64 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 L value (_L32 suffixes in Figs 2.1 & 2.2)
   2. a 64-bit I value (_I64 suffixes in Figs 2.1 & Fig 2.2)

As the OP codes XXX and YYY 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.

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; 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. [RFC-5227] 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.

4. IANA CONSIDERATIONS

In accordance with [RFC-5494], IANA is requested to assign new Operation Codes in the Address Resolution Protocol Parameters registry to the "ILNPv4 ARP Request" message (with value XXX above) and to the "ILNPv4 ARP Reply" message (with value YYY) above.

5. REFERENCES

This document has both Normative and Informational References.

5.1 Normative References

[ILNP-ARCH] R. Atkinson and S. Bhatti, "ILNP Architecture", draft-irtf-rrg-ilnp-arch, March 2012.

[ILNP-ENG] R. Atkinson and S. Bhatti, "ILNP Engineering Considerations", draft-irtf-rrg-ilnp-eng, March 2012.

[ILNP-DNS] R. Atkinson and S. Bhatti, "DNS Resource Records for ILNP", draft-irtf-rrg-ilnp-dns, March 2012.

[ILNP-ICMPv4] R. Atkinson and S. Bhatti, "ICMP Locator Update message for ILNPv4", draft-irtf-rrg-ilnp-icmpv4, March 2012.

[ILNP-v4opts] R. Atkinson and S. Bhatti, "IPv4 Options for ILNPv4", draft-irtf-rrg-ilnp-v4opts, March 2012.

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

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

[RFC-5494] 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.

5.2 Informative References

[ILNP-NONCE6] R. Atkinson and S. Bhatti, "ILNPv6 Nonce Destination Option", draft-irtf-rrg-ilnp-noncev6, March 2012.

[ILNP-ICMPv6] R. Atkinson and S. Bhatti, "ICMPv6 Locator Update Message for ILNPv6", draft-irtf-rrg-ilnp-icmpv6, March 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.

RFC EDITOR NOTE

This section is to be removed prior to publication.

This document is written in English, not American. So English spelling is used throughout, rather than American spelling. 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: 26 OCT 2012