Internet Draft
draft-irtf-rrg-ilnp-icmpv4-01.txt
Expires: 26 OCT 2012
Category: Experimental

RJ Atkinson
Consultant
SN Bhatti
U. St Andrews

March 26, 2012

ICMP Locator Update message for ILNPv4
draft-irtf-rrg-ilnp-icmpv4-01.txt

Status of this Memo

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 note defines an experimental ICMP message type for IPv4 used with the Identifier-Locator Network Protocol (ILNP). The Identifier-Locator Network Protocol (ILNP) is an experimental, evolutionary enhancement to IP. The ICMP message defined herein is used to dynamically update Identifier/Locator bindings for an existing ILNP session. This is a product of the IRTF Routing RG.

Table of Contents

1. INTRODUCTION

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

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. [ILNP-v4OPTS] defines two new IPv4 options used with ILNPv4. This document discusses a new ICMP for IPv4 message. [ILNP-DNS] describes new Domain Name System (DNS) resource records used with ILNP. Other documents describe ILNP for IPv6 (ILNPv6).

1.2 ICMPv4 Locator Update

As described in [ILNP-ARCH] and [ILNP-ENG], an ILNP for IPv4 (ILNPv4) node might need to inform correspondent ILNPv4 nodes of changes to the set of valid Locator values. The new ICMPv4 Locator Update message described in this document enables an ILNP-capable node to update its correspondents about the currently valid set of Locators valid to use in reaching the node sending this message [RFC2460] [RFC4443].

This new ICMPv4 message MUST ONLY be used for ILNPv4 sessions. Authentication is always required, as described in the Security Considerations section later in this note.

Some might consider any and all use of ICMP to be undesirable. In that context, please note that while this specification uses ICMP, on grounds that this is a control message, there is no architectural difference between using ICMP and using some different framing, for example UDP.

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. ICMP Locator Update message for ILNPv4

The ICMP for IPv4 message described in this section has ICMP Type XXX and is used ONLY with a current ILNPv4 session. This message enables an ILNPv4 node to inform ILNPv4 correspondent nodes of changes to the active Locator set for the ILNPv4 node that originates this message. This particular ICMP for IPv4 message MUST ONLY be used with ILNPv4 communications sessions.

ICMP Locator Update message

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Num of Locs  |    RESERVED   |          RESERVED             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                       Locator [1]                             /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Preference [1]         |          Lifetime [1]         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                       Locator [2]                             /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Preference [2]         |          Lifetime [2]         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ICMP Fields:

Type	XXX
Code	0
Checksum	The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the Checksum field is set to 0.
# Locators	The number of 32-bit Locator values that are advertised in this message.
Locator[i],	The 32-bit Locator values currently

i = 1..Num of Locs	valid for the sending ILNPv4 node.
Preference[i], i = 1..Num of Locs	The preferability of each Locator[i], relative to other valid Locator[i] values. The Preference numbers here are identical, both in syntax and semantics, to the Preference values for L32 records that are specified by [ILNP-DNS].
Lifetime[i] i = 1..Num of Locs	The maximum number of seconds that this particular Locator may be considered valid. Normally, this is identical to the DNS lifetime of the corresponding L64 record, if one exists.
RESERVED	A field reserved for possible future use. At present, the sender MUST initialise this field to zero. Receivers should ignore this field at present. The field might be used for some protocol function in future.

All ILNPv4 ICMP Locator Update messages MUST contain a valid ILNPv4 Identifier option and MUST contain an ILNPv4 Nonce Option.

ILNPv4 ICMP Locator Update messages also MAY be protected using IP Security for ILNP [ILNP-ENG] [RFC4301]. Deployments in high-threat environments SHOULD also protect ILNPv4 ICMP Locator Update messages using IP Security. While IPsec ESP can protect a payload, no form of IPsec ESP is able to protect an IPv4 option that appears prior to the ESP header. Note that even when IP Security for ILNP is in use, the ILNPv4 Nonce Option still MUST be present. This simplifies protocol processing, and it also means that a receiver can perform the inexpensive check of the Nonce value before performing any (potentially expensive) cryptographic calculation.

3. Transport Protocol Effects

This message has no impact on any transport protocol.

The message may affect where packets for a given transport session are sent, but an ILNP design objective is to decouple transport-protocols from network-layer changes.

4. Implementation Considerations

Implementers may use any internal implementation they wish, provided that the external appearance is the same as this implementation approach.

To support ILNPv4, and to retain the incremental deployability and backwards compatibility needed, the network layer needs a mode bit in the Transport Control Block (or its equivalent) to track which IP sessions are using the classic IPv4 mode and which IP sessions are using ILNPv4 mode.

Further, when supporting ILNPv4, nodes will need to support a Identifier Locator Communication Cache (ILCC) in the network layer as described in [ILNP-ENG].

A node sending an ICMP Locator Update message MUST include all currently valid Locator values in that message. A node receiving a valid ICMP Locator Update message MUST replace the previously current set of Locator values for that correspondent node in its own ILCC with the newly received set of Locator values.

Every implementation needs to support a large number of Locator values being sent or received in a single ICMP Locator Update message, because a multi-homed node or multi-homed site might have a large number of upstream links to different service providers, each with its own Locator value.

5. Backwards Compatibility

When ILNPv4 is not in use, the receiving IPv4 mode MUST discard the ICMP Locator Update packet without processing the packet.

6. SECURITY CONSIDERATIONS

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

The ICMPv4 Locator Update message MUST ONLY be used for ILNPv4 sessions.

The ILNPv4 Nonce Option [ILNP-v4OPTS] MUST be present in packets containing an ICMPv4 Locator Update message. Further, the

received Nonce Destination Option must contain the correct nonce value for the packet to be accepted by the recipient and then passed to the ICMPv4 protocol for processing. If either of these requirements are not met, the received packet MUST be discarded as not authentic, and a security event SHOULD be logged by the system receiving the non-authentic packet.

Sessions operating in higher risk environments SHOULD use IP Security for ILNP [ILNP-ENG] [RFC4301] *in addition* to the ILNPv4 Nonce Option. Use of IP Security for ILNP to protect a packet does NOT permit the packet to be sent without the Nonce Option.

Implementations need to support the case where a single ICMP Locator Update message contains a large number of Locator and Preference values and ought not develop a security fault (e.g. stack overflow) due to a received message containing more Locator values than expected.

If the ILNP Nonce value is predictable, then an off-path attacker might be able to forge data or control packets. This risk also is mitigated by the existing common practice of IP Source Address filtering [RFC2827] [RFC3704].

7. IANA CONSIDERATIONS

IANA is requested to assign a new ICMP Type number for this ICMP Locator Update message, replacing XXX above, following the procedures in [RFC2780].

The ICMP Locator Update message does not use the ICMP Extension Structure defined in [RFC4884]. At present, the only ICMP Code valid for this ICMP Type is zero (0), which means "No Code".

8. REFERENCES

This document has both Normative and Informational References.

8.1 Normative References

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

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

[ILNP-ENG] R. Atkinson and S. Bhatti, "ILNP Engineering

Considerations", draft-irtf-rrg-ilnp-eng, March 2012.

[ILNP-v4OPTS] R. Atkinson and S. Bhatti, "IPv4 Options for ILNPv4", draft-irtf-rrg-ilnp-v4opts, March 2012.

[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.

[RFC4443] A. Conta, S. Deering, and M. Gupta, "Internet Control Message Protocol Version 6 (ICMPv6) Specification", RFC 4443, March 2006.

[RFC4301] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

8.2 Informative References

[RFC2827] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, May 2000.

[RFC2780] S. Bradner and V. Paxson, "IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers", RFC 2780, March 2000.

[RFC3704] F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks", RFC 3704, March 2004.

[RFC4884] R. Bonica, D. Gan, D. Tappan, C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, April 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.

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