Internet Research Task Force (IRTF)
Request for Comments: 6745
Category: Experimental
ISSN: 2070-1721

RJ Atkinson
Consultant
SN Bhatti
U. St Andrews

November 2012

ICMP Locator Update Message for the Identifier-Locator Network Protocol for IPv4 (ILNPv4)

Abstract

This note defines an experimental ICMP message type for IPv4 used with the Identifier-Locator Network Protocol (ILNP). 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 Research Group.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Research Task Force (IRTF). The IRTF publishes the results of Internet-related research and development activities. These results might not be suitable for deployment. This RFC represents the individual opinion(s) of one or more members of the Routing Research Group of the Internet Research Task Force (IRTF). Documents approved for publication by the IRSG are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6745.

Table of Contents

1. Introduction

This document is part of the ILNP document set, which has had extensive review within the IRTF Routing RG. 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.

At present, the Internet research and development community is 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 multihoming, node multihoming, site/subnet mobility, node mobility) are also active concerns at present. Several different classes of evolution are being considered by the Internet research and 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. Document Roadmap

This document describes 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.

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 is 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 [RFC6741]. 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) [RFC6740] is the main architectural description of ILNP, including the concept of operations.

b) [RFC6741] describes engineering and implementation considerations that are common to both ILNPv4 and ILNPv6.

c) [RFC6742] defines additional DNS resource records that support ILNP.

d) [RFC6743] 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) [RFC6744] 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) [RFC6746] 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 it also defines a new IPv4 Identifier Option used by ILNPv4 nodes.

g) [RFC6747] describes extensions to Address Resolution Protocol (ARP) for use with ILNPv4.

h) [RFC6748] 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. ICMPv4 Locator Update

As described in [RFC6740] and [RFC6741], 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 document.

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

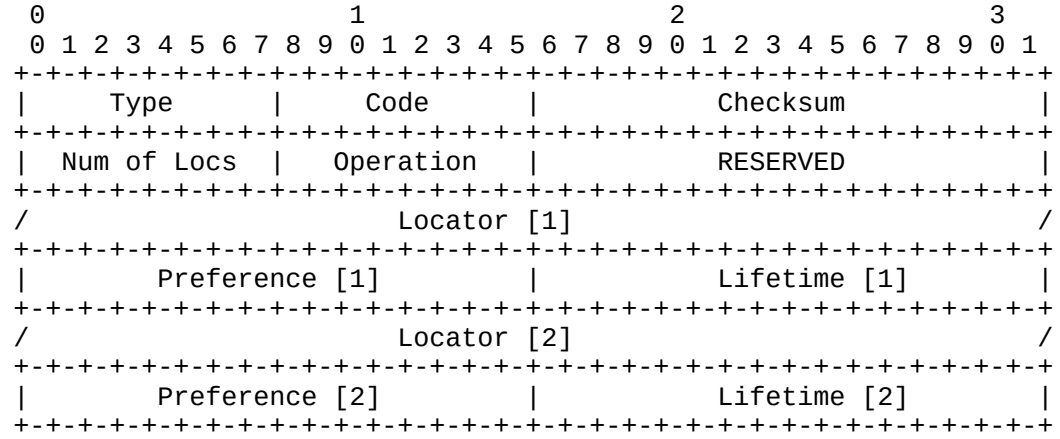
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. ICMP Locator Update Message for ILNPv4

The ICMP for IPv4 message described in this section has ICMP Type 253 (as defined for experimental use in Section 8 of [RFC4727]) and is used ONLY with a current ILNPv4 session. This message enables an ILNPv4 node to advertise changes to the active Locator set for the ILNPv4 node that originates this message to its unicast ILNP correspondent nodes. It also enables those correspondents to acknowledge receipt of the advertisement.

This particular ICMP for IPv4 message MUST ONLY be used with ILNPv4 sessions. The Checksum field for this message is calculated identically as for any other IPv4 ICMP message.

ICMP Locator Update message



ICMP Fields:

Type	253 This type value is taken from Section 8 of [RFC4727] and is allocated for experimental use.
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.
Num of Locs	The number of 32-bit Locator values that are advertised in this message.
Locator[i], i = 1..Num of Locs	The 32-bit Locator values currently 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 [RFC6742].
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 L32 record, if one exists.
Operation	The value in this field indicates whether this is a Locator Update Advertisement (0x01) or a Locator Update Acknowledgement (0x02).
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.

NOTE WELL: The ICMP Type value is allocated for shared experimental use in Section 8 of [RFC4727]. It is not uniquely assigned to ILNPv4. So, implementations need to code particularly defensively as other IPv4 experiments might be using this same ICMP Type value for an entirely different purpose with a different ICMP packet format.

The Operation field has value 1 (hexadecimal 0x01) for a Locator Update Advertisement. The Operation field has value 2 (hexadecimal 0x02) for a Locator Update Acknowledgement. All other values of the Operation field are reserved for future use by future revisions of this specification.

A node whose set of valid Locators has changed MUST send Locator Update Advertisement messages to each correspondent node for each active unicast ILNP session. For unicast ILNP sessions, the receiver of a valid (i.e., authentication checks all passed, advertisement is received from a current correspondent node) Locator Update Advertisement addressed to the receiver MUST send a Locator Update Acknowledgement back to the sender of the Locator Update Advertisement. The Acknowledgement message body is identical to the received Advertisement message body, except for the Operation value.

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 [RFC6741] [RFC4301]. Deployments in high-threat environments SHOULD also protect ILNPv4 ICMP Locator Update messages using IPsec. While IPsec Encapsulating Security Payload (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

The ICMP Locator Update message has no impact on any transport protocol.

The ICMP Locator Update message might affect where packets for a given transport-layer session are sent, but an ILNP design objective is to decouple transport protocols (e.g., TCP, UDP, SCTP) and transport-layer sessions 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 [RFC6741].

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 multihomed node or multihomed site might have a large number of upstream links to different service providers, each with its own Locator value.

It should be noted that as the ICMP Type uses an experimental value from [RFC4727], care should be taken when using with other protocols also using experimental values.

5. Backwards Compatibility

This IPv4 ICMP message uses the same checksum calculations as any other IPv4 ICMP message.

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 [RFC6740]. Additional common security considerations are described in [RFC6741]. 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 [RFC6746] 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 a forgery, and a security event SHOULD be logged by the system receiving the non-authentic packet.

ILNP sessions operating in higher risk environments SHOULD use IP Security for ILNP [RFC6741] [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

This document makes no request of IANA.

If in the future the IETF decided to standardise ILNPv4, then allocation of a unique ICMP Type for the Locator Update as part of the IETF standardisation process would be sensible.

8. References

8.1. Normative References

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

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

[RFC4727] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, January 2006.

[RFC6740] Atkinson, R. and S. Bhatti, "Identifier-Locator Network Protocol (ILNP) Architectural Description", RFC 6740, November 2012.

[RFC6747] Atkinson, R. and S. Bhatti, "Address Resolution Protocol (ARP) Extension for the Identifier-Locator Network Protocol for IPv4 (ILNPv4)", RFC 6747, November 2012.

[RFC6741] Atkinson, R. and S. Bhatti, "Identifier-Locator Network Protocol (ILNP) Engineering and Implementation Considerations", RFC 6741, November 2012.

[RFC6746] Atkinson, R. and S.Bhatti, "IPv4 Options for the Identifier-Locator Network Protocol (ILNP)", RFC 6746, November 2012.

8.2. Informative References

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC4984] Meyer, D., Ed., Zhang, L., Ed., and K. Fall, Ed., "Report from the IAB Workshop on Routing and Addressing", RFC 4984, September 2007.

[RFC6742] Atkinson, R., Bhatti, S. and S. Rose, "DNS Resource Records for the Identifier-Locator Network Protocol (ILNP)", RFC 6742, November 2012.

[RFC6748] Atkinson, R. and S. Bhatti, "Optional Advanced Deployment Scenarios for the Identifier-Locator Network Protocol (ILNP)", RFC 6748, November 2012.

[RFC6743] Atkinson, R. and S. Bhatti, "ICMPv6 Locator Update Message", RFC 6743, November 2012.

[RFC6744] Atkinson, R. and S. Bhatti, "IPv6 Nonce Destination Option for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)", RFC 6744, November 2012.

9. 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.

Authors' Addresses

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 KY16 9SX
Scotland, UK

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