

Internet Draft  
[draft-irtf-rrg-ilnp-v4opts-06.txt](#)  
Expires: 10 JAN 2013  
Category: Experimental

RJ Atkinson  
Consultant  
SN Bhatti  
U. St Andrews  
10 July 2012

**IPv4 Options for ILNPv4**  
**[draft-irtf-rrg-ilnp-v4opts-06.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 two new IPv4 options that are used only with ILNP for IPv4 (ILNPv4). ILNP is an experimental, evolutionary enhancement to IP. This document is a product of the IRTF Routing RG.

Table of Contents - ### to be updated

<a href="#">1. Introduction.....</a>	<a href="#">2</a>
<a href="#">2. IPv4 Options for ILNPv4.....</a>	<a href="#">3</a>
<a href="#">3. Security Considerations.....</a>	<a href="#">7</a>
<a href="#">4. IANA Considerations.....</a>	<a href="#">7</a>
<a href="#">5. References.....</a>	<a href="#">8</a>

## [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 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 Document Roadmap**

This document describes 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.

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-ARP](#)] describes extensions to ARP for use with ILNPv4.
- 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 [RFC2119](#). [[RFC2119](#)]

## **2. IPv4 Options 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 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. As with ILNPv6, only the Locator values are used for routing and forwarding ILNPv4 packets.

However, just as the packet format for IPv4 is different to IPv6, so the engineering details for ILNPv4 are different also. Just as



ILNPv6 is carefully engineered to be backwards-compatible with IPv6, ILNPv4 is carefully engineered to be backwards-compatible with IPv4.

Each of these options MUST be copied upon fragmentation. Each of these options is used for control, so uses Option Class 0.

Originally, these two options were specified to use separate IP option numbers. However, only 1 IP option (decimal 158) has been defined for experimental use with properties of MUST COPY and CONTROL.[\[RFC4727\]](#) So these two options have been re-worked to share that same IP option number (158). To distinguish between the two actual options, the unsigned 8-bit field ILNPv4\_OPT inside this option is examined.

It is important for implementers to understand that IP Option 158 is not uniquely allocated to ILNPv4. Other IPv4-related experiments might be using that IP option value for different IP options having different IP option formats.

## **2.1 ILNPv4 Packet Format**

The Source IP Address in the IPv4 header becomes the Source ILNPv4 Locator value, while the Destination IP Address of the IPv4 header becomes the Destination ILNPv4 Locator value. Of course, backwards compatibility requirements mean that ILNPv4 Locators use the same number space as IPv4 routing prefixes.

ILNPv4 uses the same 64-bit Identifier, with the same modified EUI-64 syntax, as ILNPv6. Because the IPv4 address fields are much smaller than the IPv6 address fields, ILNPv4 cannot carry the Identifier values in the fixed portion of the IPv4 header. The obvious two ways to carry the ILNP Identifier with ILNPv4 are either as an IPv4 Option or as an IPv6-style Extension Header placed after the IPv4 header and before the upper-layer protocol (e.g. OSPF, TCP, UDP, SCTP).

Currently deployed IPv4 routers from multiple router vendors use packet forwarding silicon that is able to parse past IPv4 options to examine the upper-layer protocol header at wire-speed on reasonably fast (e.g. 1 Gbps or better) network interfaces. By contrast, no existing IPv4-capable packet forwarding silicon is able to parse past a new Extension Header for IPv4. Hence, for engineering reasons, ILNPv4 uses a new IPv4 Option to carry the Identifier values. Another new IPv4 option also carries a nonce value, performing the same function for ILNPv4 as the IPv6 Nonce Destination Option [ILNP-NONCE6] performs for ILNPv6.





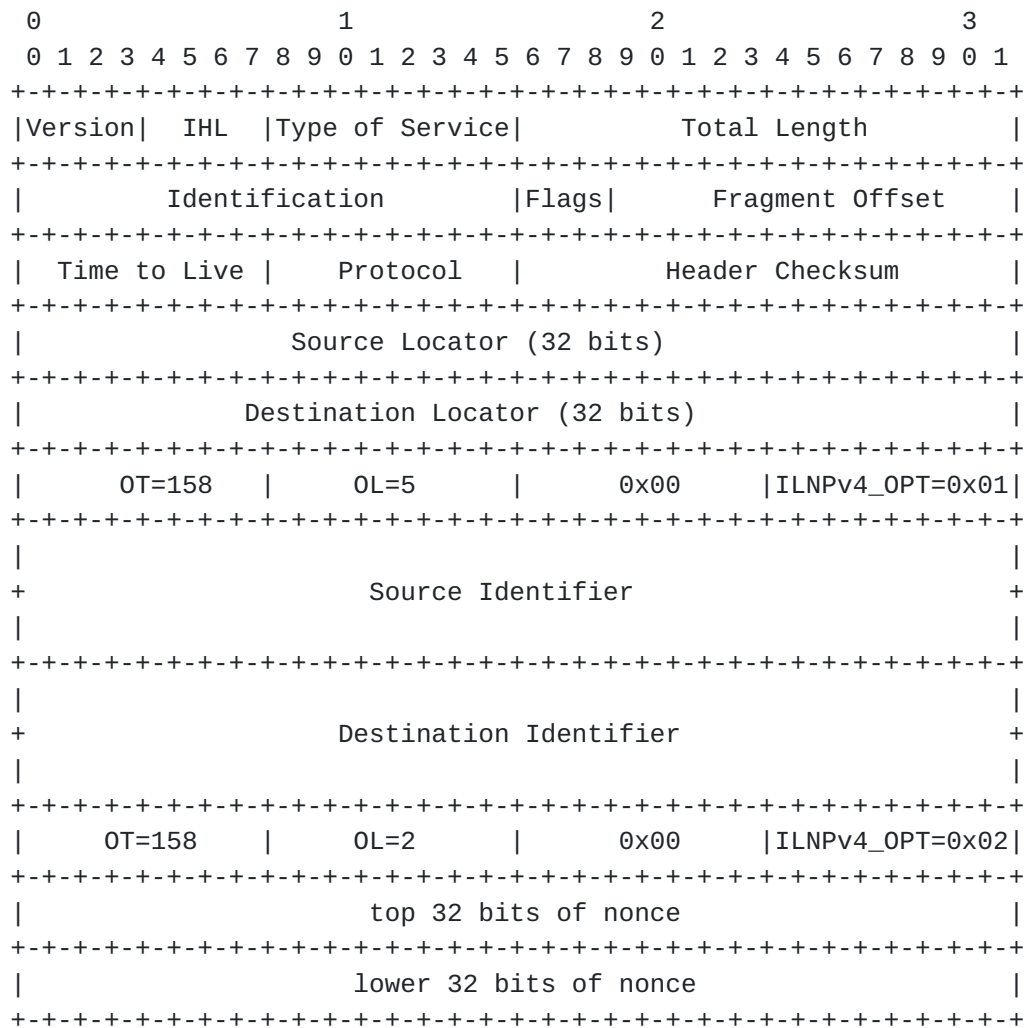


Figure 1: ILNPv4 header with ILNP ID option and ILNP Nonce option.

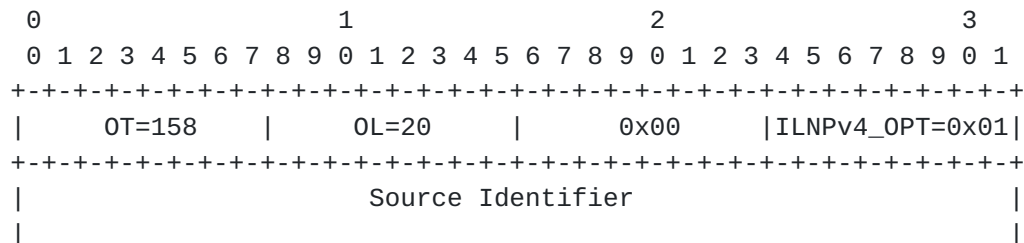
Notation for Figure 1:

IHL: Internet Header Length

OT: Option Type

OL: Option Length

## 2.2 ILNP Identifier Option for IPv4



Atkinson & Bhatti Expires in 6 months

[Page 6]

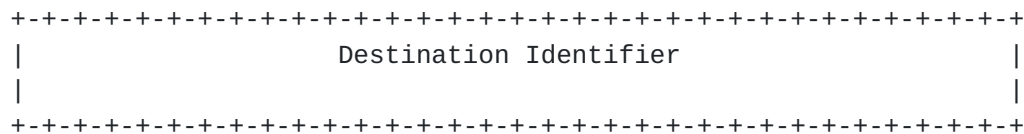


Figure 2: ILNP Identifier Option for IPv4

Notation for Figure 2:

OT:    Option Type  
OL:    Option Length

[RFC-791](#), Page 15 specifies that the Option Length is measured in words and includes the Option Type octet, the Option Length octet, and the option data octets.

The Source Identifier and Destination Identifier are unsigned 64-bit integers. [\[ILNP-ENG\]](#) specifies the syntax, semantics, and generation of ILNP Identifier values. Using the same syntax and semantics for all instantiations of ILNP Identifiers simplifies specification and implementation, while also facilitating translation or transition between ILNPv4 and ILNPv6 should that be desirable in future.

This IP option MUST NOT be present in an IPv4 packet unless the packet is part of an ILNPv4 session. ILNPv4 sessions MUST include this option in the first few packets of each ILNPv4 session, and MAY include this option in all packets of the ILNPv4 session. It is RECOMMENDED to include this option in all packets of the ILNPv4 session if packet loss is higher than normal.

### 2.3 ILNP Nonce Option for IPv4

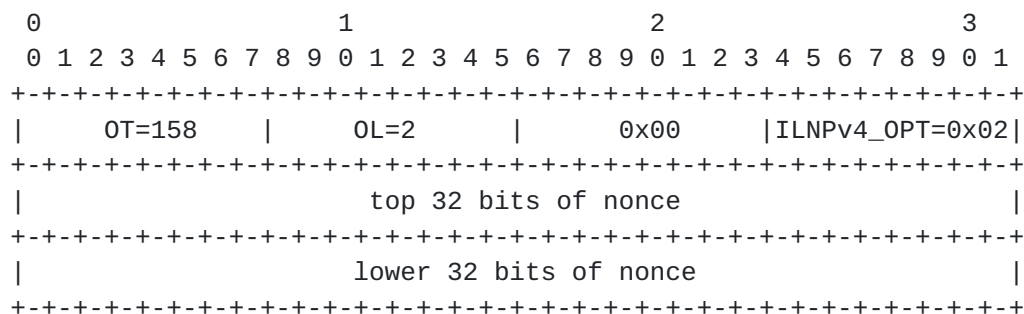


Figure 3: ILNP Nonce Option for IPv4

Notation for Figure 3:

OT:    Option Type  
OL:    Option Length



This option contains a 64-bit ILNP Nonce. As noted in [ILNP-ARCH] and [ILNP-ENG], all ILNP Nonce values are unidirectional. This means, for example, that when TCP is in use the underlying ILNPv4 session will have two different NONCE values: one from Initiator to Responder and another from Responder to Initiator. The ILNP Nonce is used to provide non-cryptographic protection against off-path attacks (e.g. forged ICMP messages from the remote end of a TCP session).

Each NONCE value MUST be unpredictable (i.e. cryptographically random). Guidance to implementers on generating cryptographically random values is provided in [RFC4086].

This IP option MUST NOT be present in an IPv4 packet unless the packet is part of an ILNPv4 session. ILNPv4 nodes MUST include this option in the first few packets of each ILNP session, MUST include this option in all ICMP messages generated by endpoints participating in an ILNP session, and MAY include this option in all packets of an ILNPv4 session.

### **3. 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.

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].

IP Security for ILNP [ILNP-ENG] [RFC4301] provides cryptographic protection for ILNP data and control packets. The ILNP Nonce option is required in the circumstances described in [Section 3](#), even if IP Security is also in use. Deployments of ILNPv4 in high-threat environments SHOULD use IP Security for additional risk reduction.

This option is intended to be used primarily end-to-end between a source node and a destination node. However, unlike IPv6, IPv4 does not specify a method to distinguish between options with hop-by-hop behaviour versus end-to-end behaviour.

[ID-IPv4-OPT-FILTERING] provides general discussion of potential operational issues with IPv4 options, along with specific advice



for handling several specific IPv4 options. Further, many deployed modern IP routers (both IPv4 and IPv6) have been explicitly configured to ignore all IP options, even including the "Router Alert" option, when forwarding packets not addressed to the router itself. Reports indicate this has been done to preclude use of IP options as a (Distributed) Denial-of-Service (D)DoS attack vector on backbone routers.

#### **4. IANA CONSIDERATIONS**

This document makes no request of IANA.

If in future the IETF decided to standardise ILNPv4, then allocation of two unique Header Option values to ILNPv4, one for the Identifier option and one for the Nonce option, would be sensible.

#### **5. REFERENCES**

This document has both Normative and Informational References.

##### **5.1 Normative References**

- [ILNP-ARCH] R.J. Atkinson & S.N. Bhatti, "ILNP Architecture", [draft-irtf-rrg-ilnp-arch](#), May 2012.
- [ILNP-ENG] R.J. Atkinson & S.N. Bhatti, "ILNP Engineering Considerations", [draft-irtf-rrg-ilnp-eng](#), May 2012.
- [ILNP-DNS] R.J. Atkinson & S.N. Bhatti, "DNS Resource Records for ILNP", [draft-irtf-rrg-ilnp-dns](#), May 2012.
- [ILNP-ICMPv4] R.J. Atkinson & S.N. Bhatti, "ICMP Locator Update message for ILNPv4", [draft-irtf-rrg-ilnp-icmpv4](#), May 2012.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4301] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", [RFC-4301](#), December 2005.
- [RFC4727] B. Fenner, "Experimental Values in IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", [RFC 4727](#), Nov 2006.





- [ILNP-ARCH]      R.J. Atkinson & S.N. Bhatti,  
"ILNP Architectural Description",  
[draft-irtf-rrg-ilnp-arch](#), 10 July 2012.
- [ILNP-ARP]      R.J. Atkinson & S.N. Bhatti, "ARP Extension for  
ILNPv4", [draft-irtf-rrg-ilnp-arp](#), 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.

## **5.2 Informative References**

- [ID-IPv4-OPT-FILTERING] F. Gont, R. Atkinson, and C. Pignatero,  
"Recommendations on Filtering of IPv4 Packets with  
IPv4 options", [draft-gont-opsec-ip-options-filtering](#),  
March 2012.
- [RFC2780]      S. Bradner & V. Paxson, "IANA Allocation Guidelines  
for Values in the Internet Protocol and Related  
Headers", [RFC 2780](#), March 2000.
- [RFC2827]      P. Ferguson and D. Senie, "Network Ingress  
Filtering: Defeating Denial of Service Attacks  
which employ IP Source Address Spoofing",  
[RFC-2827](#), May 2000.
- [RFC3704]      F. Baker and P. Savola, "Ingress Filtering for  
Multihomed Networks", [RFC-3704](#), March 2004.
- [RFC4086]      D. Eastlake 3rd, J. Schiller, and S. Crocker,  
"Randomness Requirements for Security", [RFC-4086](#),  
June 2005.
- [ILNP-ADV]      R.J. Atkinson & S.N. Bhatti,  
"Optional Advanced Deployment Scenarios for ILNP",  
[draft-irtf-rrg-ilnp-adv](#), 10 July 2012.
- [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.

#### 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](mailto: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](mailto:saleem@cs.st-andrews.ac.uk)

Expires: 10 JAN 2013