Network Working Group
Internet-Draft
Updates: 6740, 6741, 6744 (if approved)
Intended status: Experimental
Expires: 9 November 2026

S. N. Bhatti
University of St Andrews, UK

8 May 2026

Use of the ILNP Nonce Destination Option Header draft-bhatti-ilnp-nonce-00

Abstract

The Identifier Locator Network Protocol (ILNP) for IPv6 is described in Experimental RFCs 6740-6744. ILNP packets for IPv6 are distinguished from normal IPv6 packets by the presence of the Nonce Destination Option Header (aka Nonce Header), as defined in RFC6744. This document clarifies the use of the Nonce Header for ILNP. This document updates RFC6740, RFC6741, RFC6744.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-bhatti-ilnp-nonce/.

Discussion of this document takes place on the Network Network Working Group mailing list (mailto:saleem@st-andrews.ac.uk).

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 9 November 2026.

Table of Contents

1. Introduction

ILNP is designed to be backwards compatible "on-the-wire" with IPv6, and to be incrementally deployable such that only nodes that need to use ILNP need to be modified, typically end-systems only. No modifications are required to switches or routers. ILNP packets can include a Nonce Destination Option Header (aka Nonce Header) to distinguish them from other IPv6 packets. This document clarifies the use of the Nonce Header for ILNP.

The specification of the Nonce Header is given in [RFC6744].

ILNP is defined for use with IPv6 and for use with IPv4, but all references in this document to ILNP are for IPv6 only. It is possible to apply the methods described in this document to ILNP for

IPv4 (with the use of the L32 data-type from [RFC6740] [RFC6742] in place of the L64 data-type), but that exercise is outside the scope of this document. Nevertheless, the list of changes given in Section 4 are directly applicable to the Nonce header Option for IPv4 described in [RFC6746].

1.1. Purpose

The purpose of this document is to clarify for the Nonce Header the following:

1. Purpose: what it is intended for in ILNP.

2. Design: the nature and use of values in the Nonce Value field.

3. Usage: when and how the Nonce Header should be used in ILNP packets.

The current RFC documents are not totally clear on points 1. and 2., and this document changes the description with respect to point 3. The key changes are all summarised in Section 4, and the rest of the document provides context and discussion.

This document does not change the structure of the Nonce Header, which remains as defined in [RFC6744].

1.2. Rationale

The Nonce Header is as defined in [RFC6744], and has been assigned type value 0x8b by IANA: it is essential for the correct operation of ILNP. The current definition and use of the Nonce Header states that it should only be present in some packet exchanges for an ILNP session but not all packets. Clarification is needed to ensure that the design and usage of the Nonce Header is clear and consistent. The clarifications and changes defined in this document will simplify packet processing for ILNP packets.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1. Definitions from other documents

The following terms are defined in [RFC6740]:

* Locator, L64
* Node Identifier, NID
* Identifier-Locator Vector, I-LV
* I-L Communications Cache, ILCC

3. Updates to previous RFC documents

RFC documents that are updated by this document are:

* RFC6740 "Identifier-Locator Network Protocol (ILNP) Architectural Description" [RFC6740].
* RFC6741 "Identifier-Locator Network Protocol (ILNP) Engineering Considerations" [RFC6741].
* RFC6744 "IPv6 Nonce Destination Option for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)" [RFC6744].

3.1. RFC6740 and RFC6741

The use of the Nonce Header is changed, and the use of the Nonce Value field in the Nonce Header is clarified. So, any reference to either should be read in the light of Section 4. Some key examples of how this document impacts text in RFC6740 and RFC6741 are given in Section 5.1.

3.2. RFC6744

The key changes with respect to RFC6744 are listed in Section 4, so, the reading of RFC6744 should now be in the light of Section 4. Some key examples of how this document impacts text in RFC6744 are given in Section 5.2.

4. The use of the Nonce Header and Nonce Value

The two objectives for the use of the Nonce Header for ILNP are:

1. To show clearly that the packet is an ILNP packet, and so allow correct packet handling and processing.

2. To provide for ILNP a lightweight mechanism for protection against certain "off-path" attacks, such as packet forging, flow hijacking, and network-level denial of service.

This document introduces the following changes to the use of the Nonce Header compared to [RFC6744] inline with the two objectives above:

* NC1: The Nonce Header MUST appear in _every_ ILNP packet.

* NC2: The Nonce Value MUST be _randomly generated_ for any new ILNP communication session that is _initiated_ by a node, and MUST be _unique_ with respect to any other Nonce Value still in use for an ILNP communication session that was _initiated_ by this node.

* NC3: The Nonce Value MUST be the _same_ in the Nonce Header for both directions of an ILNP communication session, i.e. it is _bidirectional_.

These changes simplify packet handling and processing for ILNP, as explained and discussed in the rest of this document.

For ease of reference, these changes will be referred to in the rest of this document as NC1, NC2, and NC3, respectively, as marked in the list above.

5. Examples of clarifications and improvements

In a number of places, the original descriptions of the Nonce Header are not clear with respect to the two objectives listed in Section 4. In other places, the text describes dealing with the presence or non-presence of the Nonce Header for ILNP packets, leading to a more complex description and requirements for packet handling and processing. Some particularly relevant examples (but not all instances of such cases) are given in the sub-sections below, with explanations of how NC1, NC2, and NC3 are beneficial.

5.1. Examples from RFC6740 and RFC6741

The core documents for the definition of the ILNP architecture and engineering are [RFC6740] and [RFC6741]. Each makes reference to the Nonce Header or the use of the Nonce Value. Some examples are:

1. From Section 8 of [RFC6740], inclusion of the Nonce Header in ILNP packets:
... will include the ILNP Nonce value in its initial packet(s) to the responder ...

2. From Section 9.1 of [RFC6740], use of the Nonce Header for flow protection:
   To reduce the number of on-path nodes that know the Nonce value for a given session when ILNP is in use, a nonce value is unidirectional, not bidirectional.

3. From Section 5.4 of [RFC6741], use of the Nonce Value for ILCC state management:
   For received packets containing an ILNP Nonce Option, lookups in the ILCC MUST use the <remote Identifier, Nonce> tuple as the lookup key. For all other ILNP packets, lookups in the ILNP Correspondent Cache MUST use the <remote Locator, remote Identifier> tuple, i.e., the remote I-LV, as the lookup key.

The benefits of NC1:

* For example 1 above, similar text appears in a number of places implying that the Nonce Header might not appear in some packets of a flow. However, it is not made explicit that the Nonce Header does not have to appear in every packet of a flow. Having the Nonce header in every ILNP packet avoids the problem where there is an IPv6 flow and an ILNP flow between the same two nodes and the values in the Source Address and Destination Address fields in the IPv6 packets are numerically identical. Without the Nonce Header, it is not possible to determine end-system packet handling at the receiver from inspection of the IPv6 packet header alone.

* For example 2 above, coupled with NC3, the presence of the Nonce Header in every packet of a flow provides better protection for the flow overall.

* For example 3 above, this is an unnecessary complexity: if the Nonce Header is in every packet, then there is no need for an alternative key tuple definition for identifying flows in the ILCC.

The benefits of NC2:

* For example 1 above, this is not relevant.

* For example 2 above, use of a unique Nonce Value for each ILNP communication session prevents an on-path attacker who learns of a Nonce Value from being able to make use of it for an attack on other ILNP communication sessions, e.g. by forging a new ILNP communication session.

* For example 3 above, the management of flow state in the ILCC is simplified by the use of a single key tuple for a flow.

The benefits of NC3:

* For example 1 above, this is not relevant.

* For example 2 above, it can be argued that the use of a bidirectional Nonce Value introduces no degradation of protection compared to use of two unidirectional Nonce Values. A suitably-placed on-path attacker could observe the Nonce Value in the packet exchange regardless of whether it is a unidirectional or bidirectional value. Meanwhile, coupled with NC1, the use of a bidirectional Nonce Value can be used as part of a handshake / synchronisation token for the two communicating parties, e.g. to help prevent off-path forged packets entering a flow at the start of a session when the initiating node is waiting to learn the value of the Nonce Value field in the reverse direction. Additionally, the Nonce Header is designed only to provide some lightweight protection for off-path attackers (please see Section 9 of [RFC6740] and Section 11 of [RFC6741]).

* For example 3 above, the management of flow state in the ILCC is simplified by ensuring that the key tuple is unique.

5.2. Examples from RFC6744

The Nonce Header is defined in [RFC6744] and includes the following text:

1. From Section 3.1 of [RFC6744], inclusion of the Nonce Header in ILNP packets:
   ... initial packet(s) of an IPv6 session ....

2. From Section 5.2 of [RFC6744], use of the Nonce Value in distinguishing between transport flows in case of clashes of NID values (ILCC state management):
   Multiple transport-layer sessions between a given pair of nodes normally share a single entry in the ILNP Communication Cache, provided their network-layer details (e.g., Identifiers, Nonces) are identical. Because two different ILNP nodes at two different locations might share the same Identifier value, it is important for an ILNP implementation to use the ILNP Nonce values to distinguish between different ILNP nodes that happen to be using the same (or some of the same) Identifier value(s).

3. From Section 6 of [RFC6744], the implication of the selective inclusion of the Nonce Header in ILNP packets:
   ILNPv6 nodes MUST include this option in the first few packets of each ILNPv6 session, MUST include this option in all ICMP messages generated by endpoints participating in an ILNPv6

session, and MAY include this option in any and all packets of an ILNPv6 session. It is recommended that this option be included in all packets of the ILNPv6 session if the packet loss for that session is known to be much higher than normal.

4. From Section 7 of [RFC6744], the Nonce Header is used for off-path protection:
The ILNPv6 Nonce Destination Option only seeks to provide protection against off-path attacks on an IP session.

The benefits of NC1:

* For example 1 above, as described in Section 5.1, the inclusion of the Nonce Header in every ILNP packet is beneficial for packet processing.

* For example 2, coupled with NC3, the presence of the Nonce Header in every packet will allow better state management in the ILCC.

* For example 3, the text is now redundant, simplifying the overall description.

* For example 4, this document makes the issue of lightweight off-path protection an explicit objective for the Nonce Header in Section 4, and makes clear that it is a lightweight protection only against off-path attackers.

The benefits of NC2:

* For example 1 above, this is not relevant.

* For example 2 above, the text is now redundant, simplifying the overall description.

* For example 3 above, coupled with NC1, the text is now redundant, simplifying the overall description.

* For example 4 above, coupled with NC1, protection against off-path attacks is improved.

The benefits of NC3:

* For example 1 above, this is not relevant.

* For example 2 above, coupled with NC1, this will help to avoid state clashes in the ILCC.

* For example 3 above, the text is now redundant, simplifying the description.

* For example 4 above, there is a discussion in Section 5.1.

5.3. Example from RFC6748

[RFC6748] describes use cases and scenarios for ILNP. Many of the use cases employ an ILNP-aware Site Border Routers (SBR). RFC6748 is not modified by the contents of this document, but there is an improvement to be noted.

* From Section 3.2 of [RFC6748], the operation of a SBR or firewall would be improved if the Nonce Header is used consistently: Since ILNP requires that all Locator Update messages be authenticated by the ILNP Nonce, the SBR will need to include the appropriate Nonce values as part of its cache of information about ILNP sessions traversing the SBR. (NOTE: Since commercial security gateways available as of this writing reportedly can handle full stateful packet inspection for millions of flows at multi-gigabit speeds, it should be practical for such devices to cache the ILNP flow information, including Nonce values.)

The combination of NC1, NC2, and NC3 would make the operation of SBR or firewall functions for ILNP easier to implement and more consistent.

6. Security Considerations

The purpose of the Nonce Header, to provide a lightweight protection against off-path attacks, is clarified in Section 4. Overall, the protection for an ILNP flow is improved.

As noted in Section 5.3, operations of firewalls should be improved by the presence of the Nonce Header.

The other existing security mechanisms already defined for ILNP remain unchanged (please see Section 9 of [RFC6740], Section 11 of [RFC6741]).

7. Privacy Considerations

There are no new privacy considerations.

The existing identity privacy and location privacy properties already defined for ILNP remain unchanged (please see Section 10 of [RFC6740], Section 12 of [RFC6741], Section 7 of [RFC6748]).

8. IANA Considerations

This document has no IANA actions.

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC6740] Atkinson, RJ. and SN. Bhatti, "Identifier-Locator Network Protocol (ILNP) Architectural Description", RFC 6740, DOI 10.17487/RFC6740, November 2012, <https://www.rfc-editor.org/rfc/rfc6740>.

[RFC6741] Atkinson, RJ. and SN. Bhatti, "Identifier-Locator Network Protocol (ILNP) Engineering Considerations", RFC 6741, DOI 10.17487/RFC6741, November 2012, <https://www.rfc-editor.org/rfc/rfc6741>.

[RFC6742] Atkinson, RJ., Bhatti, SN., and S. Rose, "DNS Resource Records for the Identifier-Locator Network Protocol (ILNP)", RFC 6742, DOI 10.17487/RFC6742, November 2012, <https://www.rfc-editor.org/rfc/rfc6742>.

[RFC6744] Atkinson, RJ. and SN. Bhatti, "IPv6 Nonce Destination Option for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)", RFC 6744, DOI 10.17487/RFC6744, November 2012, <https://www.rfc-editor.org/rfc/rfc6744>.

[RFC6746] Atkinson, RJ. and SN. Bhatti, "IPv4 Options for the Identifier-Locator Network Protocol (ILNP)", RFC 6746, DOI 10.17487/RFC6746, November 2012, <https://www.rfc-editor.org/rfc/rfc6746>.

[RFC6748] Atkinson, RJ. and SN. Bhatti, "Optional Advanced Deployment Scenarios for the Identifier-Locator Network Protocol (ILNP)", RFC 6748, DOI 10.17487/RFC6748, November 2012, <https://www.rfc-editor.org/rfc/rfc6748>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Acknowledgements

The author is grateful to the many members of the IETF community for their feedback on ILNP during IETF meetings, and to the IETF NOC Team who made possible testing and experiments for ILNP during those meetings and the IETF Hackathon events.

Gregor Haywood, Ryo Yanagida, and Rodney Grimes provided feedback on the original text for this document which helped to improve clarity.

This work was partly supported by the _ICANN Grant Program_.

Author’s Address

Saleem N. Bhatti
University of St Andrews, UK
Email: saleem@st-andrews.ac.uk