Internet Engineering Task Force
Internet-Draft
Updates: 826, 4861 (if approved)
Intended status: Standards Track
Expires: 30 January 2026

M. Smith

29 July 2025

Identification, Sequence Number and Payload Option for IPv6 NDP and IPv4 ARP Ping

draft-smith-6man-isnp-option-for-ndp-arp-ping-00

Abstract

IPv6 Neighbor Discovery Protocol (NDP) and IPv4 Address Resolution Protocol (ARP) can be used to perform "ping" tests that overcome nodes' refusal to respond to IPv6 and IPv4 ICMP Echo Requests. A drawback is that NDP and ARP do not carry an Identification, Sequence Number and Payload for these ping tests. This memo proposes an IPv6 Neighbor Discovery Option that adds these fields to the NDP and ARP packets used to perform ping tests.

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 30 January 2026.

Copyright Notice

Table of Contents

1. Introduction

The IPv6 Neighbor Discovery Protocol (NDP) [RFC4861] and IPv4 Address Resolution Protocol (ARP) [RFC826] can be used to perform remote node liveness testing by conducting a request/response transaction, using IPv6 Neighbor Solicitation and Neighbor Advertisment packets, or IPv4 ARP Request and Reply packets. This sort of liveness testing is commonly known as a "ping" test.

The reason to perform a ping test via NDP or ARP is that some nodes, in particular hosts, do not respond to the traditional ping tests utilising either ICMPv6 Echo Requests and Echo Replies [RFC4443] or IPv4 ICMP Echo Requests and Echo Replies [RFC792] [WINDOWS10]. The primary motivation for these nodes not to respond to IPv6 or IPv4 pings is to avoid being discovered by malicious nodes on the Internet, as a first step in identifying target hosts to attack.

However, nodes not responding to any IPv6 or IPv4 pings can make innocent node network connectivity testing and troubleshooting harder, in particular for a network operator. Enabling these nodes to respond to traditional ICMP based IPv6 or IPv4 pings may not be an acceptable or possible option because of the security implications, as well as lack of administrative access to the nodes (for example, it is common for network operators to not have any level of administrative access to hosts attached to the network), and the amount of the effort involved when there are large numbers of nodes to enable.

Using NDP or ARP to perform ping tests overcomes this limitation, as nodes must respond to IPv6 Neighbor Solicitations or IPv4 ARP Requests to successfully communicate with other nodes on the link, and other off-link nodes via any locally available routers. A response to an NDP or ARP ping is a absolute and positive confirmation that the node exists, regardless of any IP or higher layer security settings.

A limitation of using NDP or ARP to perform ping tests is that the node performing the test must be attached to the same link as the target node for the test. This is because NDP and ARP packets are not forwarded by routers. However, this limitation addresses the main security reason that nodes do not respond to IPv6 or IPv4 pings - nodes attached to the same link are far more implicitly trusted than off-link nodes.

For a network operator, this same link limitation is not significant for performing remote troubleshooting. The network operator could login to a router directly attached to the link and then perform the NDP and ARP ping test via the local router’s administrative user interface.

Another limitation of using NDP or ARP to perform ping tests is that NDP or ARP packets used to perform the ping test do not contain identifier and sequence number fields, nor a payload field that can be used to further verify reliable data transfer.

Utilities that implement NDP or ARP pings typically build the NDP Neighbor Solicitation or ARP Request within the application, and then send the packet directly onto the link, bypassing the node’s local NDP or ARP implementation. A NDP Neighbor Advertisement or ARP Reply response that arrives within the ping test timeout may be because of the ping test NDP Neighbor Solicitation or ARP Request, or may be because of the testing node’s underying NDP or ARP operations. While these responses show that the NDP or ARP ping target exists, they interfere with the accurate measurement of round trip time measurement for the NDP or ARP ping response, interfere with accurate packet loss measurement, and don’t facilitate any payload validation testing.

This memo specifies an IPv6 NDP Option that contains contains Identification and Sequence Number fields and an optional Payload field to be used to perform more useful and accurate NDP and ARP ping tests. This option is known as the "Identification, Sequence Number and Payload" or ISNP Option.

Note that while this memo describes the ISNP Option use with the NDP and ARP protocols for that purpose of ping testing, the option could be use for other future NDP operations that are not in the scope of this memo.

1.1. Requirements Language

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. Identification, Sequence Number and Payload (ISNP) Option Format

The Identification, Sequence Number and Payload (ISNP) Option Format is as follows:

* Type - An 8 bit option type field, assigned a well-known value by IANA from the IPv6 Neighbor Discovery Option Formats Type values.

* Length - A 8 bit unsigned Length field, containing the Length of the ISNP Option (including the Type and Length fields) in units of 8 octets. Minimum value of 1, to allow for the ISNP Option’s Type, Length, Identifer and Sequence Number fields. Larger values accommodate an optional data Payload field, also a number of multiples of 8 octets in size.

* Reserved - A 16 bit field reserved for future use. All zeros upon transmission, ignored upon receipt.

* Identifier - A 64 bit Identifier field to aid in matching an NDP ping Neighbor Advertisement with a NDP ping Neighbor Solication, or matching an ARP ping Reply with an ARP ping Request. May be zero.

* Sequence Number - A 32 bit Sequence Number field to aid in matching an NDP ping Neighbor Advertisement with a Neighbor Solication, or matching an ARP ping Request with a ARP Reply. May be zero.

* Payload - An optional data payload consisting of arbitrary value octets. The number of payload octets MUST be a multiple of 8 octets to comply with the NDP option specification [RFC4861].

3. ISNP Option Use in NDP Neighbor Solicitations and Advertisements

The ISNP Option is currently only used with NDP Neighbor Solicitations and Advertisements when they are being used to perform NDP ping testing. It is not used for normal [RFC4861] NDP Address Resolution.

The sending node chooses an appropriate 64 bit Identifier and 32 bit Sequence Number.

The sending node also chooses optional arbitrary Payload octets to send and to be returned without modification by the ping target node. If present, the number of the Payload octets MUST be a multiple of 8 octets.

The Identifier and Sequence Number values, and Payload contents, are only of local significance to the sending node performing the ping testing. They are not interpreted in any way by the NDP ping target receiving node.

The ISNP Length is set to 1 plus the size of the optional Payload as a multiple of 8 octets.

Finally, the ISNP Type value is set to the IANA assigned Neighbor Discovery Option Format type value.

The NDP ping testing function then prepares a standard Neighbor Solication [RFC4861] message for ping testing use, adding the ISNP Option.

The Neighbor Solication is then sent to the NDP ping target (or targets in the case of a multicast NDP ping).

If and when the NDP ping target node receives the Neighbor Solication containing the ISNP Option, it prepares a suitable response Neighbor Advertisement per [RFC4861]. It adds the received ISNP Option into the Neighbor Advertisement without modification, and then sends the Neighbor Advertisement back to the Neighbor Solicitation sending node.

If the NDP ping target node does not understand the ISNP Option, it will silently ignore it [RFC4861], and will not add it to its Neighbor Advertisement response.

If the node performing the NDP ping test receives the Neighbor Advertisement containing the ISNP Option within an acceptable time frame, it validates the ISNP Option and reports NDP ping test success. If the Neighbor Advertisement doesn't arrive, or ISNP Option validation fails, a suitable error is reported.

If a Neighbor Advertisement does arrive within an acceptable time frame, however doesn't contain the ISNP Option, then it isn't possible to attribute this Neighbor Advertisement to a Neighbor Solication that carried the ISNP Option. In this case, only a possible NDP ping response should be reported. The NDP ping testing function should continue to wait for a Neighbor Advertisement that contains a ISNP Option until the timeout period. If a Neighbor Advertisment with the correct ISNP Option does arrive it should be reported as a successful NDP ping response.

4. ISNP Option Use in ARP Requests and Replies

The ISNP Option is used with ARP in a similar way to its use in NDP - it is added to an ARP Request, and is reflected back to the ARP Request sender in an ARP Reply without modification.

The ISNP Option field values are set using the same procedure as in the previous use of the ISNP Option with NDP.

When used with an ARP Request, the ISNP Option is appended to the ARP Request packet, directly after the (ar$tpa) field, with the packet size increased to accommodate the ISNP Option.

The Address Resolution Protocol [RFC826] does not perform any total packet length checking on an ARP Request, as there is no total ARP packet length field.

Additionally, an ARP Request and Reply are the same size and have the same fields. Per [RFC826], this allows the packet buffer for the ARP Request to be reused for the corresponding ARP Reply after modification.

This lack of ARP total size checking and reuse of a packet buffer means that an ARP Request and Reply can carry an arbitrary payload after the formal ARP fields, and that the arbitrary payload should be reflected back in an ARP Reply to a corresponding ARP request, without modification, because of the packet buffer reuse. The reflected arbitrary ARP payload carries the ISNP Option.

Some ARP implementations [WINDOWS11][LINUX6.15] do not reuse the ARP Request packet buffer, and instead use a new packet buffer for a corresponding ARP Reply. In this case, the ISNP Option will not be

reflected in an ARP Reply to a ISNP Option holding ARP Request. To support the ISNP Option in these types of implementations, they will need to be updated to reflect an ARP Request arbitrary payload in a corresponding ARP Reply response, either by reusing the ARP Request packet buffer, or appending the received ISNP Option to the new ARP Reply packet buffer (reusing the ARP Request packet buffer for the ARP Reply would also make these implementations slightly more efficient in terms of packet buffer utilisation and allocation).

As an ARP implementaton may not reflect a ISNP Option in an ARP Reply, the node performing an ARP ping will need to treat any ARP Replies received within the ping timeout as only possibly being triggered by the ARP Request with the ISNP Option. These ARP Replies should be reported only as a possible responses to the ARP Request holding the ISNP Option. The ping function should allow for any subsequent ARP Requests with the ISNP Option to arrive within the ping timeout period. If an ISNP Option carrying ARP Reply arrives then ping success should be reported.

5. IANA Considerations

IANA are requested to assign a well-known value from the IPv6 Neighbor Discovery Option Formats Type values for use by the NDP And ARP Ping Option.

6. Security Considerations

As NDP and ARP are essential for successful IPv6 and IPv4 communications on a link, it is not possible to prevent other nodes on the link from using NDP or ARP as ping testing protocols, including the use of the ISNP Option to perform these ping tests.

If certain nodes on a link cannot be trusted to perform NDP and ARP ping tests, including using the ISNP Option, these untrusted nodes should be isolated from the other nodes at the link layer, preventing any on-link NDP or ARP ping testing. This would also mitigate much more significant abuses of the NDP or ARP protocols, such as NDP or ARP Neighbor Advertisement spoofing, or NDP Router Advertisement spoofing [draft-ietf-v6ops-nd-considerations].

7. References

7.1. 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/info/rfc2119>.

[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/info/rfc8174>.

7.2. Informative References

[exampleRefMin]
Surname [REPLACE], Initials [REPLACE]., "Title [REPLACE]", 2006.

[exampleRefOrg]
Organization [REPLACE], "Title [REPLACE]", 1984, <http://www.example.com/>.

Acknowledgements

Your name here!

Author’s Address

Mark Smith
PO BOX 521
Heidelberg Victoria 3084
Australia
Email: markzzzsmith@gmail.com