Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 24, 2018

F. Templin, Ed.
Boeing Research & Technology

November 20, 2017

The DHCPv6 Option for IPv6 Neighbor Discovery draft-templin-6man-dhcpv6-ndopt-00.txt

Abstract

IPv6 Neighbor Discovery (IPv6ND) specifies a control message set for nodes to discover neighbors, routers, prefixes and other services on the link. It also supports a manner of StateLess Address AutoConfiguration (SLAAC). The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) specifies a service for the stateful delegation of addresses and prefixes.

Currently, at least two round-trip message exchanges are necessary in order to perform the IPv6ND router discovery and DHCPv6 address/prefix delegation functions. This document presents a protocol for combining these two round trips into a single round trip by joining the two services into a single unified service.

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 May 24, 2018.

Copyright Notice

Table of Contents

1. Introduction

IPv6 Neighbor Discovery (IPv6ND) [RFC4861] specifies a control message set for nodes to discover neighbors, routers, prefixes and other services on the link. It also supports a manner of StateLess Address AutoConfiguration (SLAAC). The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) specifies a service for the stateful delegation of addresses and prefixes [RFC3315][RFC3633].

Currently, at least two round-trip message exchanges are necessary in order to perform the IPv6ND router discovery and DHCPv6 address/ prefix delegation functions. This document presents a protocol for combining these two round trips into a single round trip by joining the two services into a single unified service.

When a node first comes onto the link, it sends a Router Solicitation (RS) message to elicit a Router Advertisement (RA) message from one or more routers for the link. If the node also needs to acquire managed addresses and prefixes (and, if the 'M' bit is set in the RA message) it then sends a DHCPv6 Solicit message to elicit a Reply message from a DHCPv6 server that is authoritative for the link (assuming DHCPv6 Rapid Commit). This two round-trip message exchange can add delay as well as waste critical link bandwidth on low-end links (e.g., VHF wireless).

This document proposes a new IPv6 ND option called the "DHCPv6 Option" that marries the IPv6 ND router discovery and DHCPv6 managed address/prefix acquisition processes into a single round trip message exchange. Nodes include the DHCPv6 option in RS messages to solicit an RA message with a DHCPv6 option in return. This allows the IPv6 ND and DHCPv6 functions to work together to supply the client with all needed configuration information in a single message exchange instead of multiple.

The following sections present considerations for nodes that employ the IPv6 ND DHCPv6 option.

2. The DHCPv6 Option

The DHCPv6 option is a new IPv6 ND option that simply embeds a standard DHCPv6 message per section 6 of [RFC3315], beginning with the msg-type followed by the transaction-id and all DHCPv6 options. The format of the option is as follows:

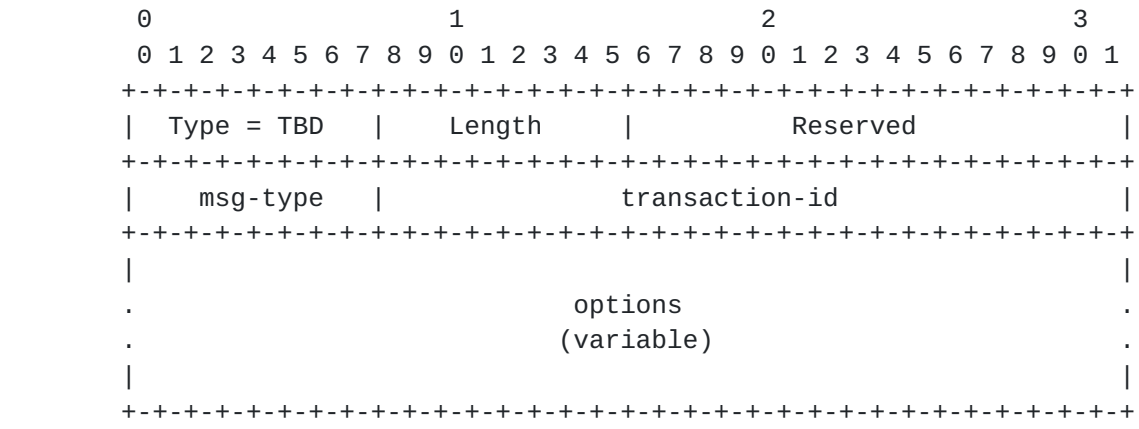

Figure 1: IPv6 ND DHCPv6 Option Format

In this format, Type and Length are exactly as defined in Section 4.6 of [RFC4861], a two-octet Reserved field is included for alignment and potential future use, and the rest of the option is exactly as defined in Section 6 of [RFC3315] (in the above, the field labeled "options" refers to DHCPv6 options, i.e., and not additional IPv6 ND options). The length of the full DHCPv6 message itself is determined by the Length field in the IPv6 ND option header.

3. DHCPv6 Option Usage

When a node first comes onto the link, it creates a Router Solicitation (RS) message containing a DHCPv6 option that embeds a DHCPv6 Solicit message. The node then sends the RS message either to

the unicast address of a specific router on the link, or to the All-Routers multicast address.

When a router receives an RS message with a DHCPv6 option, if it does not recognize the option and/or does not employ a DHCPv6 relay agent or server, it returns a Router Advertisement (RA) message as normal and without including a DHCPv6 option. By receiving the RA message with no DHCPv6 option, the node can determine that router does not recognize the option an/or does not support a DHCPv6 relay/server function. In this way, no harm will have come from the node including the DHCPv6 option in the RS, and the function is fully backwards compatible.

When a router receives an RS message with a DHCPv6 option, if it recognizes the option and employs a DHCPv6 relay agent or server, it extracts the DHCPv6 message from the RS message and forwards the message to the DHCPv6 relay agent or server. When the DHCPv6 message reaches a DHCPv6 server, the server processes the DHCPv6 Solicit message and prepares a DHCPv6 Reply message containing any delegated addresses, prefixes and/or any other information the server is configured to send. The server then returns the Reply message to the router.

When the router receives the DHCPv6 Reply message, it creates a Router Advertisement (RA) message that includes any autoconfiguration information necessary for the link and also embeds the Reply message in a DHCPv6 option within the body of the RA. The router then returns the RA as a unicast message reply to the node that sent the RS.

At any time after the initial RS/RA exchange, the node may need to issue a DHCPv6 Renew, Release or Rebind message, e.g., to extend address/prefix lifetimes. In that case, the node prepares a DHCPv6 message option and inserts it in an RS message which it then sends via unicast to the router. The router in turn processes the message the same as for DHCPv6 Solicit/Reply.

At any time after the initial RS/RA exchange, the DHCPv6 server may need to issue a DHCPv6 Reconfigure message. In that case, when the router receives the DHCPv6 Reconfigure message it prepares a unicast RA message with a DHCPv6 option that encodes the Reconfigure and sends the RA as an unsolicited unicast message to the node.

4. Implementation Considerations

The IPv6ND function and DHCPv6 function are typically implemented in separate router modules. In that case, the IPv6 ND function extracts the DHCPv6 message from the option included in the RS message and

wraps it in IP/UDP headers. The source address in the IP header is set to one of the router's unicast addresses, and the source port in the UDP header is set to the port number associated with the IPv6 ND function. The IPv6 ND function then acts as a Lightweight DHCPv6 Relay Agent (LDRA) [RFC6221] to forward the message to the DHCPv6 relay or server function on-board the router.

The forwarded DHCPv6 message then traverses any additional relays on the reverse path until it reaches the DHCPv6 server. When the DHCPv6 server processes the message, it delegates any necessary resources and sends a Reply via the same relay agent path as had occurred on the reverse path so that the Reply will eventually arrive back at the IPv6 ND function. The IPv6 ND function then prepares an RA message with any autoconfiguration information associated with the link, embeds the DHCPv6 message body in an IPv6 ND DHCPv6 option, and returns the message via unicast to the node that sent the RS.

In a preferred implementation, however, the IPv6ND and DHCPv6 functions could be co-located in the same module on the router. In that way the two functions would be coupled as though they were in fact a single unified function without the need for any IP/UDP encapsulation or LDRA processing.

5. IANA Considerations

The IANA is instructed to assign an IPv6 ND option Type value TBD for the DHCPv6 option.

6. Security Considerations

Security considerations for IPv6 Neighbor Discovery [RFC4861] and DHCPv6 [RFC3315][RFC3633] apply to this document.

.

7. Acknowledgements

This work was motivated by discussions on the 6man and v6ops list.

This work is aligned with the NASA Safe Autonomous Systems Operation (SASO) program under NASA contract number NNA16BD84C.

This work is aligned with the FAA as per the SE2025 contract number DTFAWA-15-D-00030.

This work is aligned with the Boeing Information Technology (BIT) MobileNet program and the Boeing Research & Technology (BR&T) enterprise autonomy program.

8. References

8.1. Normative References

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, DOI 10.17487/RFC3633, December 2003, <https://www.rfc-editor.org/info/rfc3633>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

8.2. Informative References

[RFC6221] Miles, D., Ed., Ooghe, S., Dec, W., Krishnan, S., and A. Kavanagh, "Lightweight DHCPv6 Relay Agent", RFC 6221, DOI 10.17487/RFC6221, May 2011, <https://www.rfc-editor.org/info/rfc6221>.

Author's Address

Fred L. Templin (editor)
Boeing Research & Technology
P.O. Box 3707
Seattle, WA 98124
USA

Email: fltemplin@acm.org