Network Working Group F. Templin, Ed.
Internet-Draft Boeing Research & Technology
Intended status: Informational July 16, 2018
Expires: January 17, 2019

A Unified Stateful/Stateless Autoconfiguration Service for IPv6
draft-templin-6man-dhcpv6-ndopt-05.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 separate stateful autoconfiguration service. This document presents IPv6ND extensions for providing a unified stateful/stateless autoconfiguration service.

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 separate service for delegation of prefixes, addresses and any other stateful information [RFC3315][RFC3633]. This document presents IPv6ND extensions for providing a unified stateful/stateless autoconfiguration service.

If the netwok can provide such a unified service, complex multi-message procedures can be condensed into a single and concise message exchange. This would ease network management as well as simplify host and router operations. It would further accommodate both SLAAC and DHCPv6 in a way that combines the best aspects of both. The operating model is based on harnessing the IPv6 ND Router

Solicitation (RS) / Router Advertisement (RA) functions to provide all stateless and stateful information in a single message exchange.

When a node first comes onto a link, it sends an RS to elicit an RA from one or more routers for the link. If the node also needs to acquire stateful information it then sends a DHCPv6 Solicit message to elicit a Reply message from a DHCPv6 server. This two round-trip message exchange can add delay as well as waste critical link bandwidth on low-end links (e.g., 6LoWPAN, satellite communications, aeronautical wireless, etc.). While it is possible to conceive of starting both round trip exchanges at the same time (i.e., under a leap-of-faith assumption that the link supports DHCPv6 before examining the 'M' bit) this would still result in twice as many channel access transactions as necessary. Moreover, the multicast nature of these messages could disturb other nodes on the link, e.g., resulting in an unnecessary wakeup from sleep mode.

This document proposes methods for combining stateless and stateful operations into a single, unified exchange based on IPv6ND messaging extensions. It notes that stateful exchanges must include at a minimum:

- o an explicit request for stateful information
- o the identity of the requesting node
- o a transaction ID that the requesting node can use to match replies with their corresponding requests
- o any security parameters necessary for the requesting node to establish its authorization to receive stateful information

The first method is through definition of a new IPv6ND option called the "DHCPv6 Option" that combines the IPv6ND router discovery and DHCPv6 stateful processes into a single message exchange. Nodes include the DHCPv6 option in RS messages to solicit an RA message with a DHCPv6 option in return. This allows the IPv6ND and DHCPv6 functions to work together to supply the client with all needed configuration information in a minimum number of messages.

The second method leverages the PIO-X proposal [I-D.pioxfolks-6man-pio-exclusive-bit] where the router sets the "X (eXclusive)" bit in an RA Prefix Information Option (PIO) to inform the node that the prefix is provided for the node's own exclusive use. This document permits nodes to include PIO-Xs in their RS messages for the purpose of requesting stateful autoconfiguration information from routers.

The third method uses out-of-band messaging for the node to request stateful information outside of the scope of IPv6ND messaging. The out-of-band messaging could entail some sort of network login process (e.g., through Layer-2 (L2) messaging, etc).

The following sections present considerations for nodes that employ these approaches.

2. DHCPv6 Options in IPv6 ND Messages

The first method entails the inclusion of DHCPv6 messages within IPv6ND RS and RA messages, as discussed in the following sections.

2.1. The DHCPv6 Option

The DHCPv6 option is a new IPv6ND 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:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type = TBD   |    Length     | Pad |        Reserved         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    msg-type   |               transaction-id                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                            options                            .
.                           (variable)       ...................
|                                            .  Padding (0-7)  .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: IPv6 ND DHCPv6 Option Format

In this format, 'Type' and 'Length' are exactly as defined in Section 4.6 of [RFC4861], 'Pad' is a 3-bit integer that encodes the padding length, 'Reserved' is included for alignment and future use, and the rest of the option is formatted as specified in Section 6 of [RFC3315] except with trailing null padding added as necessary for 8 octet alignment. The length of the full DHCPv6 message is determined by ((('Length' * 8) - 4) - 'Pad'), for a maximum message length of 2036 octets.

The 'Reserved' field MUST be set to 0 on transmission and ignored on reception. Future specifications MAY define new uses for these bits.

2.2. DHCPv6 Option Usage

When a node first comes onto the link, it creates an RS message containing a DHCPv6 option that embeds a DHCPv6 Solicit message. The Solicit may include a Rapid Commit option if a two-message exchange (i.e., instead of four) is required. 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 an RA message as normal with any stateless configuration information and without including a DHCPv6 option. By receiving the RA message with no DHCPv6 option, the node can determine that the router does not recognize the option and/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 encapsulated DHCPv6 message and forwards it to the relay agent or server. When the DHCPv6 message reaches a DHCPv6 server, the server processes the DHCPv6 Solicit message and prepares either an Advertise (four message) or Reply (two message) DHCPv6 message containing any delegated addresses, prefixes and/or any other information the server is configured to send. The server then returns the Advertise/Reply message to the router.

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

In a two message exchange, the stateless/stateful exchange is completed when the node receives the RA. In a four message exchange, the reqeusting node can Decline any stateful information it does not wish to accept and/or send unicast Request options in subsequent RSes to get RA messages with Reply options back from the router or routers of its choosing.

At any time after the initial RS/RA exchange, the node may need to issue DHCPv6 Renew, Release or Rebind messages to manage 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.

2.3. Stateful Autoconfiguration Requirements

Using the DHCPv6 Option, the message itself includes sub-options to request stateful information. The DHCPv6 Device Unique IDentifier (DUID) provides the the identity of the requesting node, and the DHCPv6 transacation-id provides a unique identifier for matching RS and RA messages. Finally, the message can be protected using SEcure Neighbor Discovery (SEND) [RFC3971].

2.4. Implementation Considerations

The IPv6ND and DHCPv6 functions are typically implemented in separate router modules. In that case, the IPv6ND function extracts the DHCPv6 message from the option included in the RS message and wraps it in IP/UDP headers with the same addresses and port numbers the soliciting node would have used had it send an ordinary IP/UDP/DHCPv6 message. The IPv6ND 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 returns 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 IPv6ND function. The IPv6ND function then prepares an RA message with any autoconfiguration information associated with the link, embeds the DHCPv6 message body in an IPv6ND 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 LDRA processing.

3. PIO Options in RS Messages

The second method entails the inclusion of Prefix Information Options (PIOs) in IPv6ND RS messages, as discussed in the following sections.

3.1. The PIO-X Option

PIOs for stateful autoconfiguration are formatted exactly as specified in [RFC4861] except including the "X" bit as defined in [I-D.pioxfolks-6man-pio-exclusive-bit]. We refer to PIOs with the "X" bit set as "PIO-X" options. The format of the option is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     | Prefix Length |L|A|R|X| Rsrvd1|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Preferred Lifetime                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Reserved2                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                            Prefix                             +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: PIO-X Option Format

In this format, all fields are exactly as defined in Section 4.6 of [RFC4861]. The "X" bit is set to 1 if the prefix is to be provided for the node's own exclusive use. If "X" is set to 0, no statement is made about the prefix's exclusivity.

3.2. PIO-X Option Usage

When a node that wishes to request an eXclusive prefix first comes onto the link, it creates an RS message containing a PIO-X. It sets the Prefix Length to either the length of the prefix it wishes to receive or '0' (unspecified) if it will defer to the router's preference. The node then sets the Valid and Preferred Lifetimes to either its preferred values or '0' (unspecified) if it will defer to

the router's preference. The node then sets the Prefix to either the prefix it wishes to receive, or '0' (unspecified) if it will defer to the router's preference. 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 PIO-X, if it is not configured to accept PIO-Xs in RS messages it returns an RA message as normal and without including a PIO-X. By receiving the RA message with no PIO-X, the node can determine that the router does not recognize the option and/or does not support a PIO-X service. In this way, no harm will have come from the node including the PIO-X in the RS, and the function is fully backwards compatible.

When a router receives an RS message with a PIO-X, if it recognizes the option and can provide stateful autoconfiguration services it examines the fields in the message and selects a prefix to delegate to the node. If the PIO-X included a specific Prefix, the router delegates the node's preferred prefix if possible. Otherwise, the router selects a prefix to delegate to the node with length based on the node's Prefix Length. The router sets lifetimes matching the lifetimes requested by the node if possible, or shorter lifetimes if the node's requested lifetimes are too long. The router finally prepares a PIO-X containing this information and inserts it into an RA message to send back to the source of the RS.

3.3. Stateful Autoconfiguration Requirements

Using the PIO-X, the option itself requests stateful autoconfiguration information. The RS message link-layer addresss can be used as the identity of the requesting node. The RS message SHOULD include a Nonce option [RFC3971] to provide a unique identifier for matching RS and RA messages. Finally, the message can be protected using SEND the same as for the DHCPv6 option [RFC3971].

3.4. Implementation Considerations

Each router can implement a stateful database management service of their own choosing, but a functional alternative would be to use the standard DHCPv6 service as the back-end management service. In this way, all communications between the router's link to the requesting node are via PIO-X RS/RA messaging. But, when the router receives an RS message with a PIO-X it can create a syntehsized DHCPv6 Solicit message to send to the DHCPv6 server. This can be done exactly the same as for the approach discussed in Section 2.4. In this way, the node on the link over which the PIO-X is advertised only ever sees RS/RA messages on the front end, and the router gets to use the

DHCPv6 service for stateful autoconfiguration management on the back end.

Note: In its current form, the PIO-X approach supports only prefix delegation and does not support other stateful configuration services.

4. Out-of-Band Network Login Messaging

The third method entails an out-of-band messaging exchange sometimes known as a "network login" procedure. During the network login, the requesting node could have an out-of-band messaging exchange with the network to set the stage for the router eventually sending an RA message as discusssed in the following sections

4.1. Out-of-Band Network Login

In the out-of-band network login, the node signs into the network using, e.g., a login/password, a security certificate, etc. The node authenticates itself to the network, and can optionally have an iterative exchange to request certain aspects of the node's desired stateful autoconfiguration information. The network then signals the node's first-hop router to prepare an RA message to return to the node.

4.2. Out-of-Band Network Login Usage

When a node that wishes to request stateful autoconfiguration first comes onto the link, it engages in a network login session using some form of out-of-band messaging such as Layer-2 (L2) messaging. The session entails a security exchange where the node authenticates itself to the network and proves its authorization to receive the autoconfiguration information. The network then signals the router to send an RA message to the node, either unsolicited or in response to the node's RS message.

4.3. Stateful Autoconfiguration Requirements

Using out-of-band messaging, the node engages in an iterative exchange where a request for stateful autoconfiguration information is conveyed. The exchange includes an identifiy for the requesting node and provides a unique per-message identifier so that the node can correlate its message requests with the responses it gets back from the network. Finally, the message exchange itself contains security parameters for authenticating the requesting node.

4.4. Implementation Considerations

The network login system and routers must be tightly coupled so that the network login can securely convey the reqesting node's identity to the router.

As for the PIO-X-based autoconfiguration service discussed in Section 3.4, DHCPv6 can be used as the back-end service for managing the stateful autoconfiguration database.

5. Implementation Status

A prototype of the approach discussed in Section 2 has been implemented as extensions to the OpenVPN open source software distribution.

6. IANA Considerations

The IANA is instructed to assign an IPv6ND option Type value TBD for the DHCPv6 option.

The IANA is instructed to create a registry for the DHCPv6 option "Reserved" field (with no initial assignments) so that future uses of the field can be coordinated. The field is to be managed as a "flags" field and not a "value" field.

7. Security Considerations

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

SEcure Neighbor Discovery (SEND) [RFC3971] can provide authentication for the combined DHCPv6/IPv6ND messages with no need for additional securing mechanisms.

8. Acknowledgements

This work was motivated by discussions on the 6man and v6ops list. Those individuals who provided encouragement and critical review are acknowledged.

The following individuals provided useful comments that improved the document: Ron Bonica, Bernie Volz.

The following individuals developed IPv6ND and DHCPv6 extensions for OpenVPN: Kyle Bae, Wayne Benson, Eric Yeh.

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.

9. References

9.1. 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>.

9.2. Informative References

[I-D.pioxfolks-6man-pio-exclusive-bit] Kline, E. and M. Abrahamsson, "IPv6 Router Advertisement Prefix Information Option eXclusive Flag", draft-pioxfolks-6man-pio-exclusive-bit-02 (work in progress), March 2017.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[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