                 Transient Hiding of Hop-by-Hop Options
                 <**draft-eastlake-6man-hide-options-04.txt**>

Abstract
    There are an increasing number of IPv6 hop-by-hop options but such
    IPv6 options are poorly handled, particularly by high-speed routers
    in the core Internet where packets having options may be discarded.
    This document proposes a simple method of transiently hiding such
    options for part of a packet's path to protect the packet from
    discard or mishandling.

Status of This Memo

Table of Contents

1. Introduction

As discussed in [Options3] there are an increasing number of IPv6 hop-by-hop options but such IPv6 options, are poorly handled, particularly by high-speed routers in the core Internet where packets having options may be discarded. This document proposes a simple method of transiently hiding such options for part of a packet's path to protect the packet from discard or mishandling.

1.1 Conventions Used in This Document

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.

Terms:

ASIC - Application Specific Integrated Circuit.

field - an area of one or more contiguous bits within a larger
    structure.

[2](#). **IP Options and Option Handling Problems**

   This Section is informational and intended to provide background
   information.

   In the early days of the Internet, much of the traffic was text,
   transmission speeds were slow, and IP routers were commonly small
   general-purpose computers. Under these conditions, parsing IP headers
   with various options or combinations of options, handling variable
   length options, etc., was relatively easy.

   However, as time passed, the Internet increased in size, bandwidth
   grew including more voluminous media such as video, transmission
   speeds increased enormously, and latency/responsiveness requirements
   became more stringent. These requirements have led to IP routers,
   especially in the core of the Internet, becoming less flexible and
   more specialized. To be able to handle data faster and more
   efficiently, such core IP routers are divided into a forwarding plane
   and a control plane where the forwarding plan handles the usual data
   forwarding while the control plan handles routing control messages
   and other packets that the data plane cannot handle. In some IP
   routers, the forwarding plane is implemented with Application
   Specific Integrated Circuits (ASICs) that are inflexible and may need
   fields they examine in an IP packet header to be at a fixed offset
   from the beginning of the packet. Meanwhile, the control plane may be
   implemented through a general-purpose computer which can only handle
   a limited number of packets per unit time.

   For these reasons, many IP routers do not implement many or any types
   of IPv6 Hop-by-Hop options (or IPv4 header options) except through
   the control plane which has limited capacity. Sending packets with
   such options to the control plane can overwhelm the control plane and
   interfere with routing control messages or other critical functions.
   Very often, particularly for IP routers handling a large volume of
   traffic, a strategy is adopted of dropping IP packets with such
   header options or ignoring the header options.

   See [[Options3](#)] for a further discussion of these option handling
   problems.

[2.1](#) IPv6 Options

   Figure 1 shows the IPv6 header [[RFC8200](#)]. The initial 4-bit Version
   field indicates the IP version number and has the value 6.

```
        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
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |Version| Traffic Class |              Flow Label               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |         Payload Length        |  Next Header  |   Hop Limit   |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                               |
       +                                                               +
       |                                                               |
       +                        Source Address                         +
       |                                                               |
       +                                                               +
       |                                                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                               |
       +                                                               +
       |                                                               |
       +                      Destination Address                      +
       |                                                               |
       +                                                               +
       |                                                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
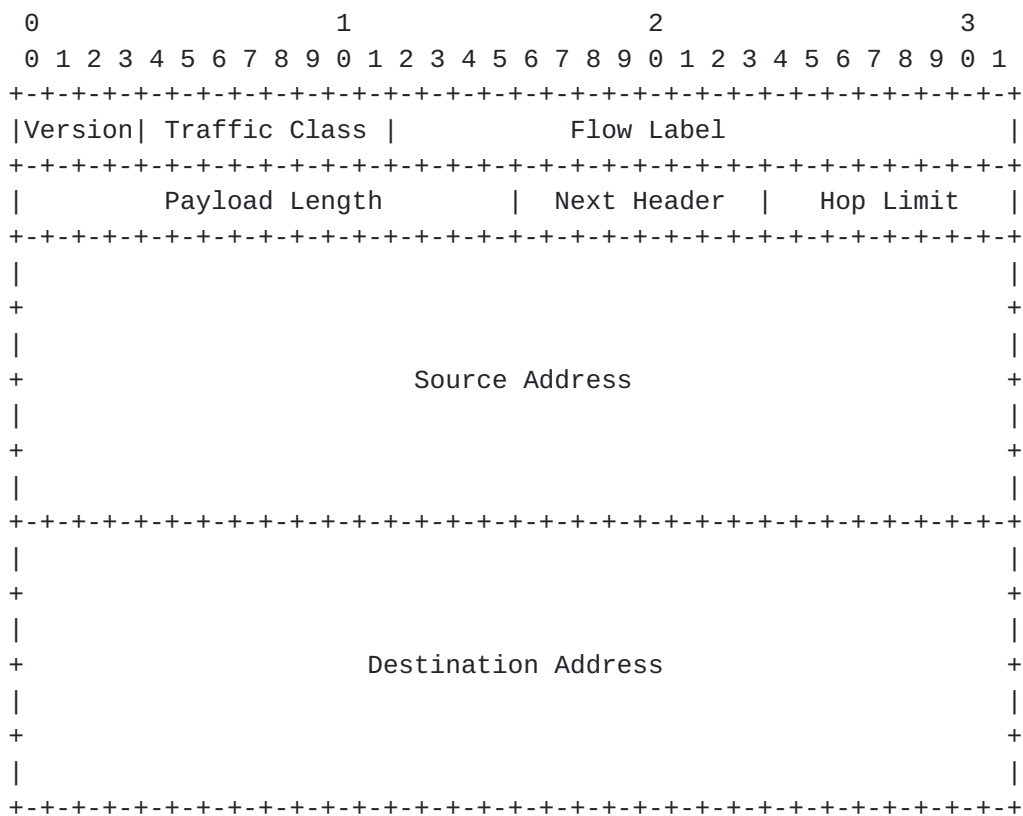
                        Figure 1: IPv6 Header

   The value of the 8-bit Next Header field specifies the type and
   format of information immediately following the header. For example,
   a value of 17 in the Next Header field indicates that the header is
   immediately followed by a User Datagram Protocol (UDP) message and a
   value of 6 would indicate the header is followed by a Transmission
   Control Protocol (TCP) message. In some cases, the data immediately
   after the IPv6 header can be a header that itself includes a Next
   Header field for the type of data following it and so on as shown in
   Figure 2. Such headers, after the initial IPv6 header and before the
   main payload, are called Extension Headers and can be viewed as
   extensions to the IPv6 header. At this time specified extension
   headers include the six listed below, additional extension headers
   have been proposed, and likely more extension headers will be
   proposed and specified in the future.

   Specified extension headers:
        Hop-by-Hop Options
        Fragment
        Destination Options
        Routing
        Authentication

Encapsulating Security Payload

In the two "options" types of extension header, the "Hop-by-Hop
Options" and "Destination Options", the extension header content is
further structured into options each of which, except for a one byte
"pad1" option, is an 8-bit type followed by an 8-bit option length,
followed by the option value. Hop-by-Hop options were initially
specified to require that every router pay attention to them. While
this has been relaxed in the most recent IPv6 specification, they are
still sometimes viewed as imposing a burden on every IP router
through which they pass.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |  Hdr Ext Len  |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                                                               |
.                                                               .
.                            Options                            .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
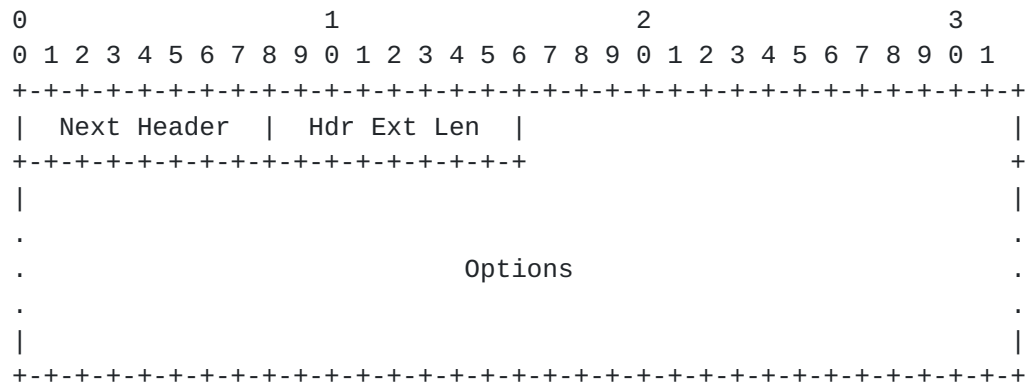
Figure 2: IPv6 Option Extension Header

[3](). **Overview of a Solution**

   Figure 3 shows a high-level view of a network path between two hosts
   within local networks through the Internet core. (In reality there
   are likely to be more levels with a local network, whether a home,
   office, data center, or whatever, usually connected through one or
   more levels of lower tier service provider before connecting to a
   Tier 1 provider that connects to the Internet core, also known as the
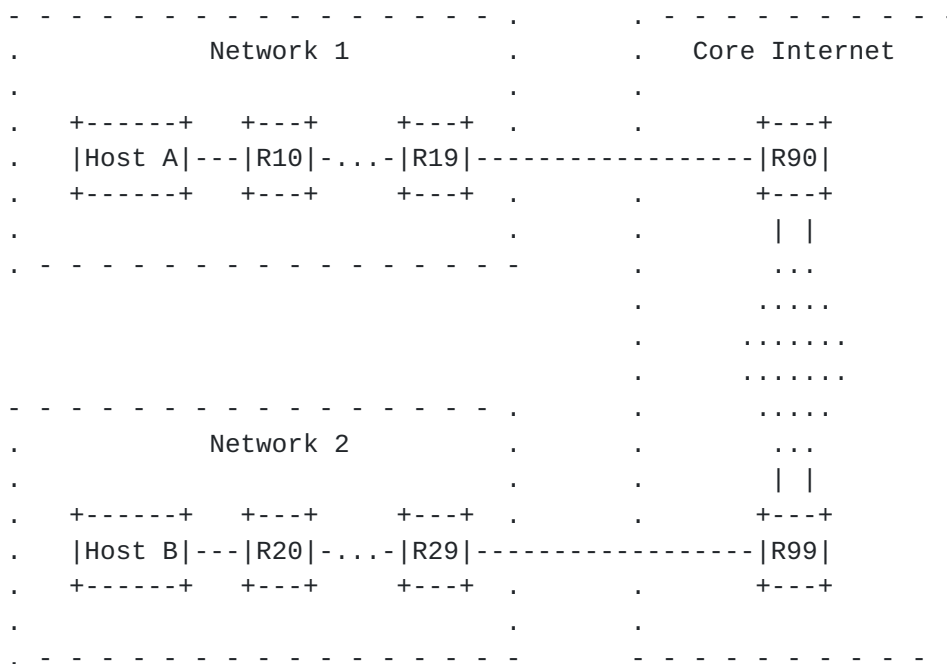   default free zone.)

```
      - - - - - - - - - - - - - - - - - - .     . - - - - - - - - - -
      .               Network 1          .     .     Core Internet    .
      .                                   .     .                      .
      .    +------+   +---+      +---+  .       .          +---+       .
      .    |Host A|---|R10|-...-|R19|------------------|R90|        .
      .    +------+   +---+      +---+  .       .          +---+       .
      .                                   .     .           | |        .
      . - - - - - - - - - - - - - - - - -       .           ...
      .                                         .          .....
      .                                         .         .......
      .                                         .         .......
      - - - - - - - - - - - - - - - - - - .     .          .....
      .               Network 2          .     .           ...
      .                                   .     .           | |        .
      .    +------+   +---+      +---+  .       .          +---+       .
      .    |Host B|---|R20|-...-|R29|------------------|R99|        .
      .    +------+   +---+      +---+  .       .          +---+       .
      .                                   .     .                      .
      . - - - - - - - - - - - - - - - - - - -     - - - - - - - - - - .
```

               Figure 3: High Level View of an Internet Path

   There are efforts to improve and streamline handling of IPv6 Hop-by-
   Hop options such as the methods in [Options1]() and [Options2]().
   However, even if such a method were popular and deployed in some
   network areas, there is likely to be significant delay before it
   would be deployed in most of the Internet core. While some Internet
   core routers may ignore options, others discard packets with options
   and, as long as there is a significant chance of such discard,
   options are rendered essentially useless on paths through the core.

   A solution is to hide options before IP packets arrive at the core.
   This hiding is done in an easily detectable and reversible fashion so
   that options can be unhidden after leaving the core. IPv6 Hop-by-Hop
   options so hidden might not be effective in the core but the
   situation is an improvement over the traffic using such options being
   discarded.

This solution requires destination support but that should be

knowable in many cases such as traffic between branches of the same
company or between a customer and a data center.

To obtain more uniform handling of packets in a flow, it may be
desirable to treat all packet in the flow as if they had such options
in that the packet would be transformed to hide and unhide options
even if there were none. Alternatively, this transformation could be
applied to all packets starting with the first having a problematic
option.

[3.1](#) Transiently Hiding IPv6 Options

IPv6 Hop-by-Hop options are hidden by replacing the zero Next Header
field in the IPv6 Header by the opaque IP protocol number TBD. This
is a very simple modification of one 8-bit field in a fixed location
that has no effect of the size of the packet. They are unhidden by
changing this opaque IP protocol number in the IPv6 header back to
zero. The points of hiding and unhiding in the packet's path (or
paths if multicast) should be chosen to maximize the routers at the
beginning and end of the path (Figure 3) that implement the options
while minimizing the chance of unwanted packet discard or other
damaging behavior.

[3.2](#) Evolution to Greater Option Support

This solution supports the evolution of the Internet toward more
widespread support or beneficent handling of hop-by-hop options as
follows:

o As acceptable option handling is more widely implemented, probably
   starting at lower bandwidth routers nearer the edge, the
   boundaries at which options are hidden and unhidden can migrate
   closer to the core.

o If scattered core routers improve to provide acceptable option
   handling, they can recognize the opaque protocol number and
   perform options, perhaps in a limited way, on packets where those
   options are hidden to unimproved routers.

[4](). IANA Considerations

   IANA is requested to assign a number from the "Assigned Internet
   Protocol Numbers" registry as follows:

```
   Decimal  Keyword   Protocol  IPv6 Ex Hdr     Reference
   -------  --------  --------  -----------  ---------------
     TBD     Opaque    Opaque                [this document]
```

5. Security Considerations

The use of the opaque IP Protocol to mask options is intended to
disable normal analysis of the following packet content, specifically
hop-by-hop options in the IP header. This would make firewalls, deep
packet analysis, and the like less effective. However, such methods
are less likely to be present in the network core where packets might
be obscured. Furthermore, firewalls tend to only admit packets with
known permissible values in protocol header fields such as the IP
protocol field. The rejection by a firewall of a packet with the
opaque IP protocol value will protect the nodes behind that firewall
from possible damage due to the receipt of a packet modified as
specified in this document. If the firewall does know the opaque IP
Protocol value, it should be configured to treat packets with that
value safely, possibly by reversing the option hiding transformation.

Performing the specified option hiding header modification only for
packets with options would reveal which packets have that
characteristic and might cause re-ordering of those packets with
respect to other packets in the same flow. Thus, it may be beneficial
to perform the specified modification on all packets in an order
sensitive flow.

Should an IPv6 packet modified to hide options get through to a host
that does not understand this modification, it would likely be
discarded due to having an unknown IP Protocol.

[More to be added]

6. Acknowledgements

The helpful comments of the following are gratefully acknowledged:

   Peng Shuping

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, <http://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, <http://www.rfc-editor.org/info/rfc8174>

    [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

Informative References

    [Options1] - Li, Z., Peng, S., and G. Mishra, "Hop-by-Hop Forwarding
          Options Header", Internet draft-li-6man-hbh-fwd-hdr-01,
          February 2021,
          https://datatracker.ietf.org/doc/draft-li-6man-hbh-fwd-hdr/

    [Options2] - Hinden, R., and G. Fairhurst, "IPv6 Hop-by-Hop options
          Processing Procedures", Internet draft-hinden-6man-hbh-
          processing-01, June 2021,
          https://datatracker.ietf.org/doc/draft-hinden-6man-hbh-
          processing/

    [Options3] - Peng, S., Li, Z., Xie, C., and Z. Qin, "Operational
          Issues with Processig of the Hop-by-Hop Options Header",
          Internet draft-ietf-v6ops-hbh-02, June 2021,
          https://datatracker.ietf.org/doc/draft-ietf-v6ops-hbh/

Authors' Address

        Donald E. Eastlake 3rd
        Futurewei Technologies, Inc.
        2386 Panoramic Circle
        Apopka, FL 32703 USA

        Tel: +1-508-333-2270
        Email: d3e3e3@gmail.com

Appendix: Revision History

   RFC Editor: Please delete this appendix before publication.

-00 to -01

   Minor editorial changes. Add more Security Considerations. Add
   Acknowledgements section.

-01 to -02

   Delete IPv4 material. It was a bit complex and almost no one really
   cares about IPv4 options. Also, minor editorial changes.

-02 to -03

   Minor changes.

-03 to -04

   Minor changes.

Copyright and IPR Provisions