Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 24, 2021

Z. Li
S. Peng
Huawei Technologies
G. Mishra
Verizon Inc.

February 20, 2021

# Hop-by-Hop Forwarding Options Header
# draft-li-6man-hbh-fwd-hdr-01

## Abstract

RFC8200 specifies the HBH header that is assumed to be processed by each hop in the delivery path of the packet. However, RFC8200 also expects that nodes processing the HBH header have been explicitly configured to do so. Therefore, it cannot be assumed that a HBH header present in the packet is processed. It all depends on the configuration of each node across the path. Moreover, in most of networks today, the processing of the HBH header is done in the control plane (slow processing path) which incurs several limitations among which resources consumption and security risk.

For these reasons, over time, the Hop-by-Hop Options header has been sparsely used without any form of large scale deployment. Also, most of already defined HBH options are forwarding options which contain forwarding plane information that needs not to be sent to the control plane.

This document proposes a new Hop-by-Hop Forwarding Options Header in order to carry Hop-by-Hop options that are solely intended to and processed by the forwarding plane. This new HBH header is confined in and dedicated to the forwarding plane while the current HBH header can still be used for control plane options.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

## 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 August 24, 2021.



Table of Contents



## 1. Introduction

As specified in [RFC8200], the Hop-by-Hop (HBH) Options header is used to carry optional information that will be examined and processed by every node along a packet's delivery path if it is

explicitly configured to do so. Since there is no specification on the possible configuration, nodes may be configured to ignore the Hop-by-Hop Options header, drop packets containing a Hop-by-Hop Options header, or assign packets containing a Hop-by-Hop Options header to a slow processing path. [RFC6564] shows the Reports from the field indicating that some IP routers deployed within the global Internet are configured either to ignore or to drop packets having a hop-by-hop header. As stated in [RFC7872], many network operators perceive HBH Options to be a breach of the separation between the forwarding and control planes. Therefore, several network operators configured their nodes so to discard all packets containing the HBH Options Extension Header, while others configured nodes to forward the packet but to ignore the HBH Options. [RFC7045] also states that hop-by-hop options are not handled by many high-speed routers or are processed only on a slow path.

Generally, modern routers maintain the separation between forwarding plane and control plane with plentiful forwarding plane resource but constrained control plane resource. In order to protect the control plane, policies are enforced in order to restrict access from the forwarding plane to the control plane. Some operators severely rate-limit packets containing the HBH Options Extension Header when they are being sent to the control plane which will cause packet drops.

The Hop-by-Hop Options can be categorized into Hop-by-Hop Forwarding Options and Hop-by-Hop Control Options, which contains information for the forwarding plane and the control plane of the nodes, respectively. It is necessary and required to separate the two types of Hop-by-Hop options since they require different process procedures. The packets carrying the Hop-by-Hop Forwarding Options are supposed to be maintained in the forwarding plane while the packets carrying the Hop-by-Hop Control Options are supposed to be sent to the control plane. The current Hop-by-Hop Options header specified in [RFC8200] is used to carry both types of Hop-by-Hop options, and there is no way or indicator to separate the processing of the two kinds of Hop-by-Hop options using the current specifications in [RFC8200].

In the current networks, the common implementation is to send all packets containing a HBH header to the control plane even if they contain only pad options (a forwarding option specified in [RFC8200]), resulting in various possible effects such as a risk of a DoS attack on the router, inconsistent drops among those packets due to rate limiting, or other effects. This will impact the normal end-to-end IP forwarding of the network services.

Therefore, due to these limitations, the HBH header has seen limited use and deployments, and protocol designers are recommended to avoid

using hop-by-hop options in any new protocols. However, there have been over ten HBH options already specified in RFCs as listed in Appendix and the specified Forwarding Options are in the majority. Moreover, as IPv6 is being rapidly and widely deployed worldwide, more and more new services that requires hop-by-hop forwarding process behavior are emerging such as IOAM with IPv6 encapsulation [draft-ietf-ippm-ioam-ipv6-options]. Therefore, these requirements should be addressed urgently and properly by the use of an efficient HBH header when processed in the forwarding plane by transit nodes.

This document proposes a Hop-by-Hop Forwarding Options header to carry the Hop-by-Hop forwarding options while the existing Hop-by-Hop Options header is used to carry the Hop-by-Hop control options only.

## 2. Problem Statement and Motivation

This section describes the problem statement and motivation for defining a new Hop-by-Hop Forwarding Options header.

### 2.1. Specifications in RFC8200

While [RFC2460] required that all nodes must examine and process the Hop-by-Hop Options header, with [RFC8200] it is expected that nodes along a packet's delivery path only examine and process the Hop-by-Hop Options header if explicitly configured to do so. The configuration of the node determines the HBH processing behavior in the node which implies that each node may have a different behavior than the others. As specified in [RFC8200], nodes may be configured to ignore the Hop-by-Hop Options header or drop packets containing a Hop-by-Hop Options header or assign packets containing a Hop-by-Hop Options header to a slow processing path. These various behaviors are observed and described in specifications such as [RFC7045] and [RFC7872]. Due to such behaviors, new hop-by-hop options are not recommended in [RFC8200] hence the usability of HBH options is severely limited.

The Hop-by-Hop Options header is identified by a Next Header value of zero in the IPv6 header. Currently, the behaviors performed by the nodes on the packets containing a Hop-by-Hop Options header is only based on the value of this Next Header in the IPv6 header, that is, the value of the Next Header is the only trigger for the behaviors to be performed.

In current networks, usually, nodes are configured in order to assign packets containing a Hop-by-Hop Options header (indicated by the Next Header = 0) to a slow processing path, i.e. to the control plane of the nodes. Very often, such configuration is embedded in the implementation of the node and cannot be changed or reconfigured.

## 2.2. Classification of HBH Options

The Hop-by-Hop Options header contains one or more Hop-by-Hop Options. Each HBH Option contains a type identifier, i.e. Option Type. The Hop-by-Hop Options can be categorized into two types: HBH Forwarding Options and HBH Control Options. The HBH forward options contain information that is useful to a router's forwarding plane, e.g. the Jumbo Payload Option [RFC2675]. While the HBH Control Options contain information that is useful to a router's control plane, e.g. the Router Alert Option [RFC2711]. Currently, both HBH forwarding and control options are carried in the same HBH Options header. There is no specification defining rules for differentiating the process of the two kinds of options.

According to the common configuration in the current networks, i.e. to assign packets containing a Hop-by-Hop Options header (indicated by the Next Header = 0) to a slow processing path, all the HBH Options will be sent to the control plane of the nodes. It impacts the normal IP forwarding procedure of the packets containing the HBH forwarding options which should be processed in the forwarding plane. As stated above, it also introduces a severe risk of DoS attacks using HBH headers.

If all the HBH Options are forced to be processed first in the forwarding plane and then classified according to the HBH Option Type, it requires the consumption of the forwarding plane resources to make such processing selection, which will impact the forwarding efficiency. Moreover, there are some existing nodes that are configured to assign the packets containing a Hop-by-Hop Options header to the control plane of the nodes cannot be reconfigured.

Appendix of this document provides the classification of the currently defined HBH options into HBH forwarding options and HBH control options, and the HBH forwarding options are in the majority.

IPv6 Extended Header limitations that need to be addressed to make HBH processing more efficient and viable in the fast path:

[RFC8504] defines the IPv6 node requirements and how to protect a node from excessive header chain and excessive header options with various limitations that can be defined on a node. [RFC8883] defines ICMPv6 Errors for discarding packets due to processing limits. Per [RFC8200] HBH options must be processed serially. However, an implementation of options processing can be made to be done with more parallelism in serial processing grouping of similar options to be processed in parallel.

The IPv6 standard does not currently limit the header chain length or number of options that can be encoded.

Each Option is encoded in a TLV and so processing of a long list of TLVs is expensive. Zero data length encoded options TLVs are a valid option. A DOS vector could be easily generated by encoding 1000 HBH options (Zero data length) in a standard 1500 MTU packet. So now Imagine if you have a Christmas tree long header chain to parse each with many options.

Limit length of the header chain.

Reduce the length of the HBH which is currently 2,048 bytes.

Limit the maximum number of HBH.

Limit the maximum number of options in an HBH.

## 2.3. Service Requirements

As listed in the Appendix, there have been over ten HBH options already specified in RFCs and the specified forwarding options are in the majority. As IPv6 is being rapidly and widely deployed worldwide, more and more applications and network services are migrating to or adopting IPv6. More and more new services that requires hop-by-hop forwarding process behavior are emerging and the HBH Options header is going to be utilized by new services in various use scenarios.

As more services start utilizing the HBH Options header, more packets containing HBH Options are going to be injected into the networks. According to the current common configuration in most network deployments, all the packets of the new services are going to be sent to the control plane of the nodes, with the possible consequence of causing a DoS effect on the control plane. The packets will be dropped and the normal IP forwarding may be severely impacted. The deployment of new network services involving multi-vendor interoperability will become impossible.

In-situ OAM with IPv6 encapsulation [draft-ietf-ippm-ioam-ipv6-options] is one of the examples. IOAM in IPv6 is used to enhance diagnostics of IPv6 networks and complements other mechanisms, such as the IPv6 Performance and Diagnostic Metrics Destination Option described in [RFC8250]. The IOAM data fields are encapsulated in "option data" fields of the Hop-by-Hop Options header if Pre-allocated Tracing Option, Incremental Tracing Option, or Proof of Transit Option are carried [I-D.ietf-ippm-ioam-data], that is, the IOAM performs per hop.

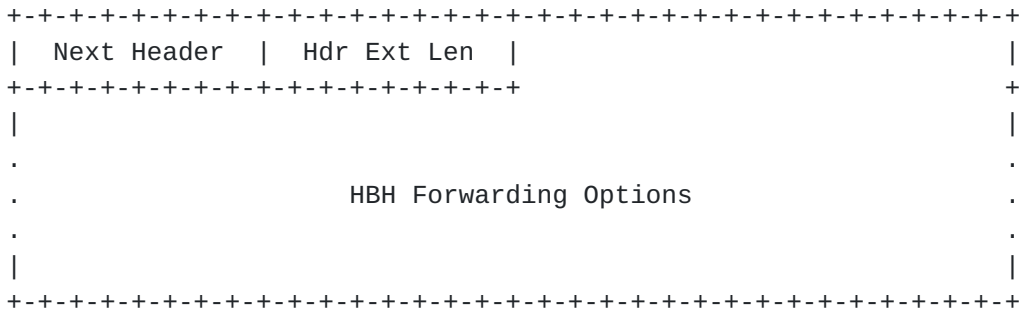
As above mentioned, according to the current common configuration, all the packets employing IOAM are going to be sent to the control plane of every node along the path, it will cause a severe effect DoS on the control plane. The packets will be inconsistently dropped and the normal IP forwarding will be severely impacted. The end-to-end deployment of IOAM in a network involving nodes from multiple vendors is impossible.

## 3. Proposal

### 3.1. Hop-by-Hop Forwarding Options Header

We propose to define a new HBH Forwarding Options header dedicated to carry the HBH Forwarding Options. The IPv6 packets containing this Hop-by-Hop Forwarding Options header will be only processed in the forwarding plane and MUST NOT be sent to the control plane of the network nodes.

The Hop-by-Hop Forwarding Options header is identified by a Next Header value of TBD in the IPv6 header and has the following format:




Next Header: 8-bit selector. Identifies the type of header immediately following the Hop-by-Hop Forwarding Options header.

Hdr Ext Len: 8-bit unsigned integer. Length of the Hop-by-Hop Forwarding Options header in 8-octet units, not including the first 8 octets.

Options: Variable-length field, of length such that the complete Hop-by-Hop Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded HBH forwarding options.

The Hop-by-Hop Forwarding Options header is recommended to be placed immediately after the IPv6 header.

The Hop-by-Hop Forwarding Options follows the formatting guidelines specified in the Appendix A. of [RFC8200].

### 3.2. The usage of the existing Hop-by-Hop Options Header

The existing Hop-by-Hop Options Header, identified by a Next Header value of zero in the IPv6 header, can still be used for carrying the HBH control options. The IPv6 packets carrying such HBH control options will be sent to the control plane anyway, so it follows the exact current processing procedures.

## 4. Security Considerations

It is the same as the Security Considerations in [RFC8200] for the part related with the HBH Options header.

## 5. IANA Considerations

TBD: Next Header for Hop-by-Hop Forwarding Options Header

## 6. Appendix. Existing HBH Options

We further classify the HBH Options into HBH Forwarding and HBH Control Options. We can see that among all the defined HBH Options the HBH Forwarding Options are in the majority.

HBH Forwarding Options:

- PAD Options: PAD1 and PADn [RFC8200]
- Jumbo Payload [RFC2675]
- RPL Option [RFC6553]
- Common Architecture Label 1Pv6 Security Option [RFC5570]
- SMF Option [RFC6621]
- MPL Option [RFC7731]
- DFF Option [RFC6971]
- MTU Option [I-D.ietf-6man-mtu-option]
- AltMark Option [I-D.ietf-6man-ipv6-alt-mark]

HBH Control Options:

- Router Alert Option [RFC2711]

- Quickstart Option [RFC4782]

## 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>.

[RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013, <https://www.rfc-editor.org/info/rfc7045>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/info/rfc7872>.

[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>.

[RFC8504] Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019, <https://www.rfc-editor.org/info/rfc8504>.

[RFC8883] Herbert, T., "ICMPv6 Errors for Discarding Packets Due to Processing Limits", RFC 8883, DOI 10.17487/RFC8883, September 2020, <https://www.rfc-editor.org/info/rfc8883>.

### 7.2. Informative References

[I-D.ietf-6man-ipv6-alt-mark] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate Marking Method", draft-ietf-6man-ipv6-alt-mark-02 (work in progress), October 2020.

[I-D.ietf-6man-mtu-option]
Hinden, R. and G. Fairhurst, "IPv6 Minimum Path MTU Hop-by-Hop Option", draft-ietf-6man-mtu-option-04 (work in progress), October 2020.

[RFC2675] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, DOI 10.17487/RFC2675, August 1999, <https://www.rfc-editor.org/info/rfc2675>.

[RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, DOI 10.17487/RFC2711, October 1999, <https://www.rfc-editor.org/info/rfc2711>.

[RFC4782] Floyd, S., Allman, M., Jain, A., and P. Sarolahti, "Quick-Start for TCP and IP", RFC 4782, DOI 10.17487/RFC4782, January 2007, <https://www.rfc-editor.org/info/rfc4782>.

[RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", RFC 5570, DOI 10.17487/RFC5570, July 2009, <https://www.rfc-editor.org/info/rfc5570>.

[RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, DOI 10.17487/RFC6553, March 2012, <https://www.rfc-editor.org/info/rfc6553>.

[RFC6621] Macker, J., Ed., "Simplified Multicast Forwarding", RFC 6621, DOI 10.17487/RFC6621, May 2012, <https://www.rfc-editor.org/info/rfc6621>.

[RFC6971] Herberg, U., Ed., Cardenas, A., Iwao, T., Dow, M., and S. Cespedes, "Depth-First Forwarding (DFF) in Unreliable Networks", RFC 6971, DOI 10.17487/RFC6971, June 2013, <https://www.rfc-editor.org/info/rfc6971>.

[RFC7731] Hui, J. and R. Kelsey, "Multicast Protocol for Low-Power and Lossy Networks (MPL)", RFC 7731, DOI 10.17487/RFC7731, February 2016, <https://www.rfc-editor.org/info/rfc7731>.

## Authors' Addresses

Zhenbin Li
Huawei Technologies

Email: lizhenbin@huawei.com

Shuping Peng
Huawei Technologies

Email: pengshuping@huawei.com

Gyan Mishra
Verizon Inc.

Email: gyan.s.mishra@verizon.com