

6MAN  
Internet-Draft  
Intended status: Informational  
Expires: 3 January 2026

Y. Liu  
ZTE  
Y. Liu  
China Mobile  
2 July 2025

Problem Statement with Aggregate Header Limit for IPv6  
draft-liu-6man-aggregate-header-limit-problem-03

## Abstract

This document first proposes introduces the concept of "Aggregate header limit for IPv6"(IPv6-AHL) based on RFC8883 to indicate the total header size that a router is able to process at full forwarding rate for IPv6 packets. Then this document describes the problems for path calculation and function enablement without the awareness of IPv6-AHL, and the considerations for IPv6-AHL collection are also included.

## 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 3 January 2026.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Conventions used in this document . . . . .	4
2.1. Terminology . . . . .	4
2.2. Requirements Language . . . . .	5
3. Problem Statement . . . . .	5
4. IPv6-AHL Collection Considerations . . . . .	6
4.1. PMTUD-style Collection Mechanism . . . . .	6
4.2. HBH-style Collection Mechanism . . . . .	7
4.3. Signaling-style Collection Mechanism . . . . .	7
5. IANA Considerations . . . . .	7
6. Security Considerations . . . . .	7
7. Acknowledgement . . . . .	8
8. References . . . . .	8
8.1. Normative References . . . . .	8
8.2. Informative References . . . . .	8
Authors' Addresses . . . . .	10

## 1. Introduction

The introduction of IPv6 extension headers, especially SRH, and some advanced features/functions have increased the total packet header chain size greatly, which may cause inefficient packet processing due to the header chain size exceeding the processing limit of the router.

As in [RFC8883], some hardware devices implement a parsing buffer of a fixed size to process packets. The parsing buffer is expected to contain all the headers that a device needs to examine. If the aggregate length of headers in a packet exceeds the size of the parsing buffer, a device will either discard the packet or defer processing to a software slow path. [RFC8883] proposes the concept "aggregate header limit" to indicate this size limit. As per [RFC8883], an ICMPv6 Destination Unreachable error with code for "Headers too long" SHOULD be sent when a node discards a packet because the aggregate length of the headers in the packet exceeds the processing limits of the node.

[RFC9098] also mentions that due to packet-forwarding engine constraints, if an IPv6 header chain is sufficiently long such that it exceeds the packet lookup capacity of the router, the router might be unable to determine how the packet should be handled and thus could resort to dropping the packet. And some packet-forwarding engines manage IPv6 header chains using recirculation, but recirculation can impact the forwarding capacity of hardware, as each packet will pass through the processing engine multiple times.

[I-D.ietf-6man-eh-limits] defines various limits that may be applied to receiving, sending, and otherwise processing packets that contain IPv6 extension headers. It provides the minimum baseline of support for use of extension headers on the Internet. The default limit for the IPv6 header chain is 104 bytes, including 64 bytes of extension headers, which is far more than enough for some usecases.

Before discussing the problem, this document proposes the concept of Aggregate Header Limit for IPv6 as below:

"Aggregate Header Limit for IPv6 (IPv6-AHL) is the total header size(i.e, from the IPv6 header chain up to any headers that are part of network encapsulation, e.g, the innermost transport layer, ethernet frame, or another IP header) that a router is able to process at full forwarding rate(e.g, at fast path). For some devices designed with parsing buffer, this limit is related with its buffer size and buffer design."

The different between IPv6-AHL and the existing concepts:

- \* Difference with Aggregate Header Limit(AHL) introduced in RFC8883: There's not a clear definition for AHL in RFC8883. If AHL is understood as the total header size that a router is able to process at full forwarding rate, the values of AHL and IPv6-AHL may be the same or may be difference based on router design.
- \* Difference with extension header chain size limit, the extension header chain size is no bigger than aggregate header size since the packet may contain upper layer headers. As mentioned in [RFC9098], the intermediate nodes/systems may need to process Layer 3/Layer 4 information to make a forwarding decision, in this case, even the extension header chain size limit is not exceeded, an intermediate node may drop the packet due to IPv6-AHL exceeding.

This document describes the problems for path calculation and function enablement without the awareness of IPv6-AHL, and the considerations for IPv6-AHL collection are also included.

## 2. Conventions used in this document

### 2.1. Terminology

MSD: Maximum SID Depth as in [RFC8491].

IPv6-AHL: Aggregate header limit for IPv6. It's the total header size(i.e, from the IPv6 header chain as well as any headers that are part of network encapsulation up to the innermost transport layer) that a router is able to process at full forwarding rate(e.g, at fast path). For some device designed with parsing buffer, this limit is related with its buffer size and buffer design.

The terminology defined in [RFC9673] are used in this document as below:

Forwarding Plane: IPv6 routers exchange user or applications data through the forwarding plane. Routers process fields contained in IPv6 packet headers. However, they do not process information contained in packet payloads.

Control Plane: Routers exchange management and routing information. They also exchange routing information with one another. Management and routing information are processed by its recipient. Management and control information can be forwarded by a router that process fields contained in packet headers.

Fast Path: A path through a router that is optimized for forwarding packets. The Fast Path might be supported by Application Specific Integrated Circuits (ASICs), Network Processor (NP), or other special purpose hardware. This is the usual processing path within a router taken by the forwarding plane.

Slow Path: A path through a router that is capable of general purpose processing and is not optimized for any particular function. This processing path is used for packets that require special processing or differ from assumptions made in Fast Path heuristics or to process router control protocols used by the control plane.

Full Forwarding Rate: This is the rate that a router can forward packets without adversely impacting the aggregate forwarding rate. For example, a router could process packets at a rate that allows it to maintain the full speed on its outgoing interfaces, which is sometimes called "wire speed".

## 2.2. 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.

## 3. Problem Statement

The introduction of IPv6 extension headers, especially SRH, and some further features/functions have increased the total packet header chain size greatly. Following are some possible scenarios that would greatly increase the difficulty of efficient packet processing from the aspects of total header size increasing.

- \* Unlike MPLS, even as an intermediate endpoint, the total SRH should be within the processing buffer to achieve efficient packet forwarding. And SRH itself may carry additional TLVs for additional functions, e.g, the SRH Opaque Metadata TLV and NSH Carrier TLV for SR service programming [I-D.ietf-spring-sr-service-programming]. Besides the headend node, the intermediate nodes may push extra header to the packet as well. For example, for Binding SID, an SR Segment Endpoint nodes would push a new IPv6 header with its own SRH containing an segment list above the original IPv6 header. And in the case of TI-LFA [I-D.ietf-rtgwg-segment-routing-ti-lfa], the PLR node may push a repair SID list to the original packet.
- \* For network performance measurement, several functions have been defined. For IPv6 IOAM pre-allocated trace, the headend attaches the hop-by-hop/destination options header with the IOAM data fields as introduced in [RFC9486]. And to implement the Alternate-Marking Method in IPv6, the AltMark Option is carried by the Hop-by-Hop Options Header or the Destination Options Header[RFC9343].
- \* To improve the service capability of the network, features like network slicing and detnet are proposed. For network slicing, the VTN Option in IPv6 Hop-by-Hop option are provided [I-D.ietf-6man-enhanced-vpn-vtn-id]. For detnet, there're discussion on carrying detnet related within the IPv6 extension headers, either as SRH TLV [draft-wang-detnet-tsn-over-srv6] or as Destination Options and Hop-by-Hop Options [draft-xiong-detnet-6man-queuing-option].

Most of the functions mentioned above are not mutually-exclusive, the possibility of combination of extension headers/TLVs would make total header size even bigger. Normally, there're different models/versions of network devices(i.e, switches, routers) from multiple vendors in an operator's network, different devices may have different aggregate header limits and different behaviors after aggregate header limit exceeding. As more and more functions mentioned above are superimposed in the operator's network, packet dropping or rate limiting due to AHL exceeding is a potential risk, which makes it difficult to management the network.

Path calculation, whether by the controller or the headend, without the awareness of AHL of the nodes in the network and the prediction on which features would be enabled along the path, may result in a path with nodes with lower AHLs than required. If the controller is aware of aforesaid information, e.g, when calculation certain path for SR Policy, and the controller knows that and per-hop IOAM and network slicing would be enabled for this SR Policy, the controller would leave out the space for HBH header with options for IOAM and VTN-ID and to ensure that the packet header size wouldn't exceed the AHLs of the intermediate segment endpoints along the list.

The situation is similar for packet encapsulation triggered by function enablement, whether on the headend or the intermediate nodes, packets may be encapsulated with larger header size than the downstream nodes able to process. If IPv6-AHL information of the nodes/path can be obtained in advance, when the node needs to attach extra data along the existing path, and the aggregate header limit of the downstream nodes along the path are not sufficient to process the headers, the node may choose to not to use the related function and log an error.

#### 4. IPv6-AHL Collection Considerations

##### 4.1. PMTUD-style Collection Mechanism

As per [RFC8883], an ICMPv6 Destination Unreachable error with code for "Headers too long" SHOULD be sent when a node discards a packet because the aggregate length of the headers in the packet exceeds the processing limits of the node. Base on this definition, obtaining the minimum AHL along the path can be achieved by sending detection messages of certain size and receiving the ICMPv6 error messages, which is similar with path MTU discovery for IPv6 in [RFC8201].

This mechanism may works for small networks with static paths in it. But there may be some problems in the following scenarios:

- \* When the number of paths increases, more and more detection messages need to be sent, and the burden of processing the received ICMPv6 error messages also increases.
- \* For SR dynamic candidate paths [RFC9256], the segment lists of the paths may change over time, which makes it more difficult to detect the IPv6-AHLs.

#### 4.2. HBH-style Collection Mechanism

[RFC9268] leverages an Hop-by-Hop Option to collect the limit (i.e, minimum path MTU) along the path. An Hop-by-Hop Option for IPv6-AHL collection purpose might be another option taking example by [RFC9268]. This mechanism works for some cases. But in SRv6, there might be transit routers who just forward the SRv6 packets like normal IPv6 packets without inspecting into the extension header chain. Even if the AHLs of these nodes have smaller AHLs than other nodes, the SRv6 packets would still be processed normally along the path. In this case, if mechanism like [RFC9268] is used, the AHL of the path be collected would be one of the AHLs of these transit nodes, but actually packets with larger header chain size could be sent and processed normally.

#### 4.3. Signaling-style Collection Mechanism

Signaling could be another option. Considering that there're already mechanisms like IGP-MSD [RFC8491][RFC8476] to advertise certain size limit at per node and per link basis. The mechanism for advertising IPv6-AHL is similar with IGP-MSD. In the inter-domain scenario, the BGP signaling may help as well. For the controller, it can get the AHLs of the nodes in the network via BGP-LS, YANG or other south-north mechanisms. The details of signaling mechanism is out of the scope of the document and would be discussed in separated documents.

#### 5. IANA Considerations

This document makes no request of IANA.

#### 6. Security Considerations

If the AHL-collection message (whether as the ICMPv6 error message, the Hop-by-Hop Option for IPv6-AHL or the routing protocol message) is sent to a third party, it allows network reconnaissance, a third party may speculate on the system design of the node based on the AHL information, such as the size of the buffer, and it may indirectly speculate the hardware configuration and system version of the node as well.

The AHL-collection function SHOULD only be used within a trusted domain and proper filtering or authorization method should be considered to prevent the AHL-collection message from being sent to the untrusted third party.

## 7. Acknowledgement

The authors would like to thank Tom Herbert, Alvaro Retana, Eric Vyncke, Jeff Tantsura, Sasha Vainshtein and Acee Lindem for their helpful comments and suggestions.

## 8. References

### 8.1. 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>>.
- [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>>.
- [RFC9673] Hinden, R. and G. Fairhurst, "IPv6 Hop-by-Hop Options Processing Procedures", RFC 9673, DOI 10.17487/RFC9673, October 2024, <<https://www.rfc-editor.org/info/rfc9673>>.

### 8.2. Informative References

- [I-D.ietf-6man-eh-limits] Herbert, T., "Limits on Sending and Processing IPv6 Extension Headers", Work in Progress, Internet-Draft, draft-ietf-6man-eh-limits-19, 27 February 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-6man-eh-limits-19>>.
- [I-D.ietf-6man-enhanced-vpn-vtn-id] Dong, J., Li, Z., Xie, C., Ma, C., and G. S. Mishra, "Carrying Network Resource (NR) related Information in IPv6 Extension Header", Work in Progress, Internet-Draft, draft-ietf-6man-enhanced-vpn-vtn-id-10, 2 March 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-6man-enhanced-vpn-vtn-id-10>>.



- [I-D.ietf-rtgwg-segment-routing-ti-lfa]  
Bashandy, A., Litkowski, S., Filsfils, C., Francois, P., Decraene, B., and D. Voyer, "Topology Independent Fast Reroute using Segment Routing", Work in Progress, Internet-Draft, draft-ietf-rtgwg-segment-routing-ti-lfa-21, 12 February 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-rtgwg-segment-routing-ti-lfa-21>>.
- [I-D.ietf-spring-sr-service-programming]  
Clad, F., Xu, X., Filsfils, C., Bernier, D., Li, C., Decraene, B., Ma, S., Yadlapalli, C., Henderickx, W., and S. Salsano, "Service Programming with Segment Routing", Work in Progress, Internet-Draft, draft-ietf-spring-sr-service-programming-11, 23 February 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-service-programming-11>>.
- [RFC8201] McCann, J., Deering, S., Mogul, J., and R. Hinden, Ed., "Path MTU Discovery for IP version 6", STD 87, RFC 8201, DOI 10.17487/RFC8201, July 2017, <<https://www.rfc-editor.org/info/rfc8201>>.
- [RFC8476] Tantsura, J., Chunduri, U., Aldrin, S., and P. Psenak, "Signaling Maximum SID Depth (MSD) Using OSPF", RFC 8476, DOI 10.17487/RFC8476, December 2018, <<https://www.rfc-editor.org/info/rfc8476>>.
- [RFC8491] Tantsura, J., Chunduri, U., Aldrin, S., and L. Ginsberg, "Signaling Maximum SID Depth (MSD) Using IS-IS", RFC 8491, DOI 10.17487/RFC8491, November 2018, <<https://www.rfc-editor.org/info/rfc8491>>.
- [RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <<https://www.rfc-editor.org/info/rfc8986>>.
- [RFC9098] Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. Liu, "Operational Implications of IPv6 Packets with Extension Headers", RFC 9098, DOI 10.17487/RFC9098, September 2021, <<https://www.rfc-editor.org/info/rfc9098>>.
- [RFC9256] Filsfils, C., Talaulikar, K., Ed., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC 9256, DOI 10.17487/RFC9256, July 2022, <<https://www.rfc-editor.org/info/rfc9256>>.

- [RFC9268] Hinden, R. and G. Fairhurst, "IPv6 Minimum Path MTU Hop-by-Hop Option", RFC 9268, DOI 10.17487/RFC9268, August 2022, <<https://www.rfc-editor.org/info/rfc9268>>.
- [RFC9343] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate-Marking Method", RFC 9343, DOI 10.17487/RFC9343, December 2022, <<https://www.rfc-editor.org/info/rfc9343>>.
- [RFC9486] Bhandari, S., Ed. and F. Brockners, Ed., "IPv6 Options for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9486, DOI 10.17487/RFC9486, September 2023, <<https://www.rfc-editor.org/info/rfc9486>>.

## Authors' Addresses

Yao Liu  
ZTE  
China  
Email: [liu.yao71@zte.com.cn](mailto:liu.yao71@zte.com.cn)

Yisong Liu  
China Mobile  
China  
Email: [liuyisong@chinamobile.com](mailto:liuyisong@chinamobile.com)