Network Working Group
Internet-Draft
Updates: 8200 (if approved)
Intended status: Standards Track
Expires: 26 June 2026

J. Iurman
University of Liege

23 December 2025

Mitigating DoS attacks in IPv6 by clarifying the number of occurrences of Extension Headers
draft-iurman-6man-eh-occurrences-00

Abstract

This document updates RFC 8200 by specifying normative requirements on the number of occurrences of IPv6 Extension Headers. Operational experience has demonstrated that permitting multiple occurrences of the same Extension Header can create parsing ambiguity, increase attack surface, and complicate packet processing in general. This is especially true for both the Hop-by-Hop Options Header and the Destination Options Header, which can contain a number of options. This document restricts IPv6 packets to carry at most one instance of each Extension Header, with the exception of the Destination Options Header, which is permitted to appear twice as specified in RFC 8200.

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 26 June 2026.

Copyright Notice

Table of Contents

1. Introduction 2
2. Conventions 3
3. Update to the number of occurrences of Extension Headers . . 3
4. Security Considerations 4
5. IANA Considerations 4
6. Acknowledgements 4
7. References 4
7.1. Normative References 4
7.2. Informative References 4
Author's Address 5

1. Introduction

Section 4.1 of [RFC8200] recommends, but does not normatively require, that each Extension Header appear at most once, with the exception of the Destination Options Header, which may appear at most twice, once before a Routing header and once before the upper-layer header.

Operational experience has demonstrated that permitting multiple occurrences of the same Extension Header can create parsing ambiguity, increase attack surface, and complicate packet processing in general. This is especially true for both the Hop-by-Hop Options Header and the Destination Options Header, which can contain a number of options.

This document updates [RFC8200], in particular Section 4.1, to enforce normative limits on the number of occurrences of Extension Headers and to remove any ambiguity in the text. This document addresses concerns related to DoS attacks on hosts as specified in [I-D.ietf-6man-eh-limits], although new limits on the number of Hop-by-Hop and Destination Options could be specified in [I-D.ietf-6man-rfc8504-bis] (i.e., smaller than 8).

2. Conventions

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. Update to the number of occurrences of Extension Headers

The following text replaces paragraph 2 of [RFC8200] Section 4.1.

OLD (RFC 8200):

| Each extension header should occur at most once, except for the
| Destination Options header, which should occur at most twice (once
| before a Routing header and once before the upper-layer header).

NEW:

| Each extension header SHOULD occur at most once, except for the
| Destination Options header, which SHOULD occur at most twice (once
| before a Routing header and once before the upper-layer header).

[RFC Editor: please remove this note] An alternative would be to keep the above text as is, without normative language.

The following text replaces paragraph 5 of [RFC8200] Section 4.1.

OLD (RFC 8200):

| IPv6 nodes must accept and attempt to process extension headers in
| any order and occurring any number of times in the same packet,
| except for the Hop-by-Hop Options header, which is restricted to
| appear immediately after an IPv6 header only. Nonetheless, it is
| strongly advised that sources of IPv6 packets adhere to the above
| recommended order until and unless subsequent specifications
| revise that recommendation.

NEW:

> | IPv6 nodes must accept and attempt to process extension headers in
> | any order in the same packet, except for the Hop-by-Hop Options
> | header, which is restricted to appear immediately after an IPv6
> | header only. Nonetheless, it is strongly advised that sources of
> | IPv6 packets adhere to the above recommended order until and
> | unless subsequent specifications revise that recommendation. IPv6
> | nodes MAY discard a packet exceeding the number of occurrences of
> | extension headers.

[RFC Editor: please remove this note] "SHOULD" or even "MUST" would obviously be better, but "MAY" seems to be the only backward compatible solution.

4. Security Considerations

This document does not introduce new security considerations. On the contrary, the change proposed in this document mitigates possible DoS attacks based on an abusive use of Extension Headers in IPv6 packets.

5. IANA Considerations

This document does not require any action from IANA.

6. Acknowledgements

TBD

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>.

[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>.

[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>.

7.2. 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-rfc8504-bis]
Chown, T., Loughney, J. A., and T. Winters, "IPv6 Node Requirements", Work in Progress, Internet-Draft, draft-ietf-6man-rfc8504-bis-02, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-rfc8504-bis-02>.

Author’s Address

Justin Iurman
University of Liege
10, Allee de la decouverte (B28)
4000 Sart-Tilman
Belgium
Email: justin.iurman@uliege.be