6man
Internet-Draft
Updates: 8200 (if approved)
Intended status: Standards Track
Expires: 30 November 2026

J. Iurman
University of Liege
T. Herbert
XDPnet

29 May 2026

Enforcement of IPv6 Extension Headers Ordering and Occurrence at Destination Nodes
draft-ietf-6man-eh-occurrences-00

Abstract

Operational experience has demonstrated that permitting multiple occurrences of the same IPv6 Extension Header can create parsing ambiguity, complicate packet processing, and increase potential security risks. Although RFC 8200 recommends that senders follow a specific order of appearance and limit the occurrences of Extension Headers, receivers cannot assume that these recommendations have been followed. This document updates RFC 8200 by allowing an IPv6 destination node, namely a host (i.e., the final destination of an IPv6 packet) or an intermediate destination node addressed by an entry in a Routing header list other than the final one, to enforce strict ordering and limits on the occurrence of Extension Headers.

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 30 November 2026.

Copyright Notice

Table of Contents

1. Introduction

Operational experience has demonstrated that permitting multiple occurrences of the same IPv6 Extension Header can create parsing ambiguity, complicate packet processing, and increase potential security risks. This is particularly true for the Hop-by-Hop Options header and the Destination Options header, which may each carry multiple options.

Although [RFC8200] recommends that senders follow a specific order of appearance and limit the occurrences of Extension Headers, receivers cannot assume that these recommendations have been followed. As a result, they may be exposed to denial-of-service attacks, where Extension Headers are used as the attack vector.

This document updates [RFC8200] by allowing an IPv6 destination node, namely a host (i.e., the final destination of an IPv6 packet) or an intermediate destination node addressed by an entry in a Routing header list other than the final one, to enforce strict ordering and limits on the occurrence of Extension Headers. The specification applies only to IPv6 destination nodes and does not impose requirements on routers forwarding IPv6 packets not explicitly addressed to themselves.

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. Enforcement of IPv6 Extension Headers Ordering and Occurrence

An IPv6 destination, i.e., a host or an intermediate destination node, MAY enforce the recommended ordering and limits on the occurrence of Extension Headers described in Section 4.1 of [RFC8200]. Per the ordering recommendations, each Extension Header can occur at most once in a packet, with the exception of the Destination Options header which can occur twice. The recommended Extension Headers ordering per [RFC8200] is:

1. IPv6 header
2. Hop-by-Hop Options header
3. Destination Options header
4. Routing header
5. Fragment header
6. Authentication header
7. Encapsulating Security Payload header
8. Destination Options header
9. Upper-Layer header

If a host or an intermediate destination node enforces the recommended ordering and a packet is received with out-of-order Extension Headers, or the occurrence of an Extension Header is greater than one (or two for the Destination Options header), then the receiving node MUST discard the packet. In the case of a host, it SHOULD send an ICMP Parameter Problem message with code 1 (Unrecognized Next Header type encountered) [RFC4443] to the packet’s source address. In the case of an intermediate destination node, it SHOULD send an ICMP Parameter Problem message with code 5 (Unrecognized Next Header type encountered by intermediate node) [RFC8883] to the packet’s source address.

4. Operational Considerations

Enforcing strict ordering and occurrence limits may cause packets whose Extension Headers do not follow the recommended order or appear more than suggested to be discarded. While such packets are not formally non-compliant with [RFC8200], they are unexpected and may lead to parsing mbiguities or interoperability issues. In particular, implementations that accept such packets under a permissive interpretation of [RFC8200] may treat them as invalid when enforcing this specification, resulting in different acceptance behavior across implementations. Operators should consider the potential impact on traffic when enabling enforcement at destination nodes, particularly at intermediate destination nodes.

5. Security Considerations

This document mitigates a potential denial-of-service attack based on abusive use of Extension Headers in IPv6 packets. Hosts and intermediate destination nodes are now allowed to enforce strict ordering and limits on the occurrence of Extension Headers to reduce the attack vector.

This document does not introduce any new security concerns.

6. IANA Considerations

This document does not require any action from IANA.

7. Acknowledgements

The authors would like to thank Nick Hilliard, Xiao Min, and Tom Petch for their valuable feedback.

8. 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>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[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>.

[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>.

Authors' Addresses

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

Tom Herbert
XDPnet
Los Gatos, CA,,
United States of America
Email: tom@herbertland.com