

6man Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 12, 2012

S. Krishnan
Ericsson
j h. woodyatt
Apple
E. Kline
Google
J. Hoagland
Symantec
M. Bhatia
Alcatel-Lucent
July 11, 2011

**An uniform format for IPv6 extension headers
draft-ietf-6man-exthdr-04**

Abstract

In IPv6, optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the transport layer header. There are a small number of such extension headers currently defined. This document describes the issues that can arise when defining new extension headers and discusses the alternative extension mechanisms in IPv6. It also provides a format for defining new IPv6 extension headers that would allow implementations to process past unknown 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 <http://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 January 12, 2012.

Copyright Notice

Copyright (c) 2011 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	3
3.	Applicability	3
4.	Proposed IPv6 Extension Header format	5
5.	Backward Compatibility	5
6.	Future work	5
7.	IANA Considerations	6
8.	Security Considerations	6
9.	Acknowledgements	6
10.	Normative References	6
	Authors' Addresses	6

1. Introduction

The base IPv6 standard [[RFC2460](#)] defines extension headers as an expansion mechanism to carry optional internet layer information. Extension headers, with the exception of the hop-by-hop options header, are not usually processed on intermediate nodes. However, some intermediate nodes such as firewalls, may need to look at the transport layer header fields in order to make a decision to allow or deny the packet. If new extension headers are defined and the intermediate node is not aware of them, the intermediate node cannot proceed further in the header chain since it does not know where the unknown header ends and the next header begins. The main issue is that the extension header format is not standardized and hence it is not possible to skip past the unknown header. This document intends to define a standard format for IPv6 extension headers.

Also, Several existing deployed IPv6 routers and several existing deployed IPv6 firewalls are capable of parsing past or ignoring all currently defined IPv6 Extension Headers (e.g. to examine transport-layer header fields) at wire-speed (e.g. by using custom ASICs for packet processing). Hence, one must also consider that any new IPv6 Extension Header will break IPv6 deployments that use these existing capabilities.

Any IPv6 header or option that has hop-by-hop behaviour and is intended for general use in the public IPv6 Internet could be subverted to create an attack on IPv6 routers processing packets containing such a header or option. Reports from the field indicate that some IP routers deployed within the global Internet are configured either to ignore the presence of headers with hop-by-hop behaviour or to drop packets containing headers with hop-by-hop behaviour.

2. Conventions used in this document

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 [[RFC2119](#)].

3. Applicability

The base IPv6 standard [[RFC2460](#)] allows the use of both extension headers and destination options in order to encode optional destination information in an IPv6 packet. The use of destination options to encode this information, provides more flexible handling characteristics and better backward compatibility than using

extension headers. Because of this, implementations SHOULD use destination options as the preferred mechanism for encoding optional destination information, and use a new extension header only if destination options do not satisfy their needs. The request for creation of a new IPv6 extension header MUST be accompanied by an specific explanation of why destination options could not be used to convey this information.

The base IPv6 standard [[RFC2460](#)] defines 3 extension headers (i.e. Routing Header, Destination Options Header, Hop-by-Hop Options Header) to be used for any new IPv6 options. The same standard only allows the creation of new Extension Headers in limited circumstances [[RFC2460](#)] [Section 4.6](#).

As noted above, the use of any option with Hop-by-Hop behaviour can be problematic in the global public Internet. So new IPv6 Extension Header(s) having hop-by-hop behaviour MUST NOT be created or specified. Also, new options for the existing Hop-by-Hop Header SHOULD NOT be created or specified unless no alternative is feasible. Any proposal to create a new option for the existing Hop-by-Hop Header MUST include a detailed explanation of why the hop-by-hop behaviour is absolutely essential in the Internet-Draft proposing the new option with hop-by-hop behaviour.

The use of IPv6 Destination Options to encode information provides more flexible handling characteristics and better backward compatibility than using a new Extension Header. Because of this, new optional information to be sent SHOULD be encoded in a new option for the existing IPv6 Destination Options Header.

Mindful of the need for compatibility with existing IPv6 deployments, new IPv6 extension headers MUST NOT be created or specified, unless no existing IPv6 Extension Header can be used by specifying a new option for that existing IPv6 Extension Header. Any proposal to create or specify a new IPv6 Extension Header MUST include a detailed technical explanation of why no existing IPv6 Extension Header can be used in the Internet-Draft proposing the new IPv6 Extension Header.

4. Proposed IPv6 Extension Header format

If any IPv6 Extension Headers are defined in future, keeping in mind the restrictions specified in [Section 3](#) and also the restrictions specified in [\[RFC2460\]](#), they MUST use the consistent format defined in Figure 1. This enables future IPv6 implementations to skip over unknown IPv6 Extension Headers and continue to further process the IPv6 header chain.

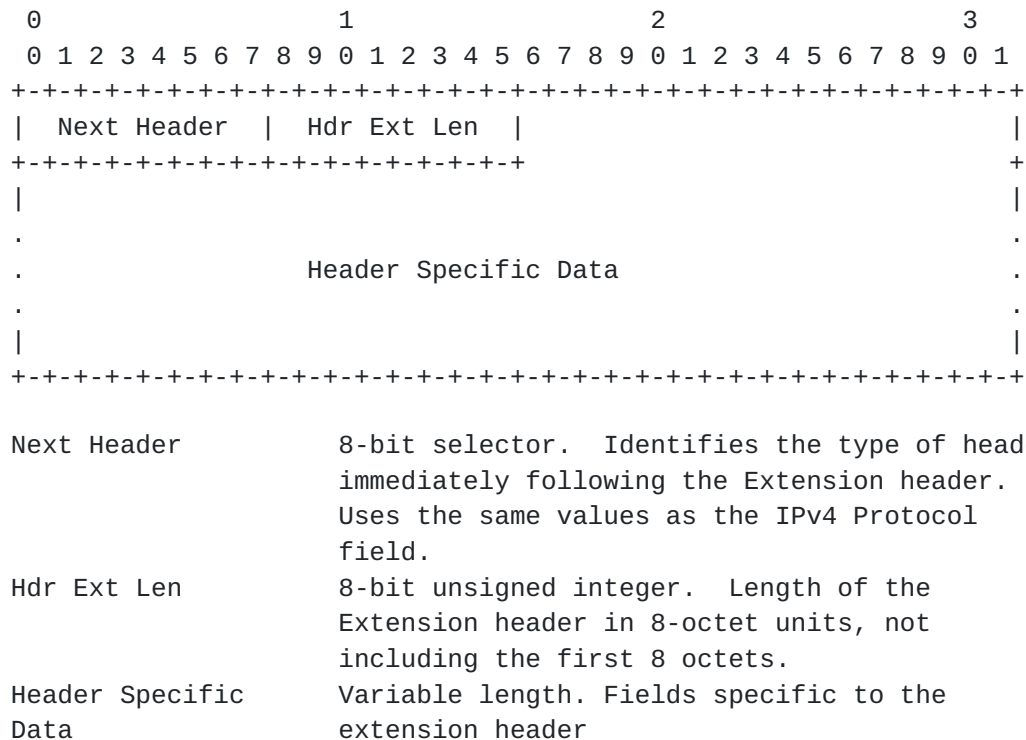


Figure 1: Extension header layout

5. Backward Compatibility

The scheme proposed in this document is not intended to be backward compatible with all the currently defined IPv6 extension headers. It applies only to newly defined extension headers. Specifically, the fragment header predates this document and does not follow the format proposed in this document.

6. Future work

This document proposes one step in easing the inspection of extension headers by middleboxes. There is further work required in this area. Some issues that are left unresolved beyond this document include

- o There can be an arbitrary number of extension headers.
- o Extension headers must be processed in the order they appear.
- o Extension headers may alter the processing of the payload itself, and hence the packet may not be processed properly without knowledge of said header.

7. IANA Considerations

This document does not require any IANA actions.

8. Security Considerations

This document proposes a standard format for the IPv6 extension headers so that intermediate nodes that do not understand the contents of these headers can look past them. Intermediate nodes, such as firewalls, skipping over unknown headers might end up allowing the setup of a covert channel from the outside of the firewall to the inside using the data field(s) of the unknown extension headers.

9. Acknowledgements

The authors would like to thank Albert Manfredi, Bob Hinden, Brian Carpenter, Erik Nordmark, Hemant Singh, Lars Westberg, Markku Savela, Tatuya Jinmei, Thomas Narten, Vishwas Manral, Alfred Hoenes, Joel Halpern, Ran Atkinson and Steven Blake for their reviews and suggestions that made this document better.

10. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.

Authors' Addresses

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

james woodyatt
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014
US

Email: jhw@apple.com

Erik Kline
Google
604 Arizona Avenue
Santa Monica, CA 90401
US

Phone: +1 310 460 4080
Email: ek@google.com

James Hoagland
Symantec Corporation
350 Ellis St.
Mountain View, CA 94043
US

Email: Jim_Hoagland@symantec.com
URI: <http://symantec.com/>

Manav Bhatia
Alcatel-Lucent
Bangalore
India

Email: manav.bhatia@alcatel-lucent.com

