Transmission of IPv6 Extension Headers
draft-carpenter-6man-ext-transmit-00

Abstract

Various IPv6 extension headers have been defined since the IPv6 standard was first published. This document updates RFC 2460 to describe how intermediate nodes should deal with such extension headers and with any that are defined in future. It also specifies how extension headers should be registered by IANA, with a corresponding minor update to RFC 2780.

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 February 15, 2013.

Copyright Notice

Copyright (c) 2012 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. Requirement to Transmit Extension Headers .................... 4
3. Security Considerations ....................................... 5
4. IANA Considerations ........................................... 5
5. Acknowledgements .............................................. 5
6. Change log [RFC Editor: Please remove] ....................... 6
7. References .................................................... 6
   7.1. Normative References ..................................... 6
   7.2. Informative References ................................... 6
Authors’ Addresses .............................................. 7
1. Introduction

An initial set of IPv6 extension headers was defined by [RFC2460], which also described how they should be handled by intermediate nodes, with the exception of the hop-by-hop options header:

"...extension headers are not examined or processed by any node along a packet’s delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header."

This provision allowed for the addition of new extension headers, since it means that forwarding nodes should be completely transparent to them. Thus, new extension headers could be introduced progressively, used only by hosts that have been updated to create and interpret them. Several such extension headers have been defined since RFC 2460.

Unfortunately, experience has showed that the network is not transparent to these headers. The main reason for this is that some firewalls attempt to inspect the transport payload. This means that they traverse the chain of extension headers, if present, until they find the payload. If they encounter an unknown extension header type, some of these firewalls treat the packet as suspect and drop it. It is an established fact that several widely used firewalls do not recognise some or all of the extension headers defined since RFC 2460. It has also been observed that a few firewalls do not even recognise all the extension headers in RFC 2460, including the fragment header, causing fundamental problems of connectivity.

Other types of middlebox, such as load balancers or packet classifiers, might also fail in the presence of extension headers that they do not recognise.

A contributory factor to this problem is that, because extension headers are numbered out of the existing IP Protocol Number space, there is no collected list of them. For this reason, it is hard for an implementor to quickly identify the full set of valid extension headers. An implementor who consults only RFC 2460 will miss all extension headers defined subsequently.

[RFC6564] improves the situation by defining a uniform format for any future extension headers, but this in itself is insufficient. The present document clarifies that the above requirement from RFC 2460 applies to all types of node that forward IPv6 packets and to all extension headers defined now and in the future. It also requests IANA to create a subsidiary registry that clearly identifies valid extension header types, and updates RFC 2780 accordingly.
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].

2. Requirement to Transmit Extension Headers

[NOTE IN DRAFT: These requirements may look controversial compared to RFC 2460, and are presented for discussion in the WG. In reality, hop-by-hop options are not handled by many high speed routers, or are processed only on a slow path. Also, many firewalls inspect and filter extension headers. The following text is intended to deal with those realities.]

The IPv6 Hop-by-Hop Options header SHOULD be processed by intermediate nodes as described in [RFC2460]. However, it is to be expected that some high performance routers will either ignore it, or assign packets containing it to a slow processing path. Designers planning to use a Hop-by-Hop option should be aware of this likely behaviour.

Apart from that, any node along an IPv6 packet’s path, which forwards it for any reason, SHOULD do so regardless of any extension headers that are present, as described in RFC 2460. Exceptionally, if this node is designed to examine extension headers for any reason, such as firewalling, it MUST recognise and deal appropriately with all valid IPv6 extension header types. The list of currently valid extension header types is maintained by IANA (see Section 4).

RFC 2460 requires destination hosts to discard packets containing unrecognised extension headers. However, intermediate forwarding nodes MUST NOT do this by default, since that might cause them to inadvertently discard traffic using a recently defined extension header, not yet recognised by the intermediate node.

As mentioned above, firewalls that violate RFC 2460 by discarding packets containing valid extension headers are known to cause connectivity failures. Therefore, it is important that firewalls behave according to the above requirements. If a firewall chooses to discard a packet containing a valid IPv6 extension header, it MUST be the result of an explicit firewall policy, and not just the result of a failure to recognise such a header.

The IPv6 Routing Header Types 0 and 1 have been deprecated and SHOULD NOT be used. However, as specified in [RFC5095], this does not mean that the IPv6 Routing Header can be unconditionally dropped by forwarding nodes. Packets containing undeprecated Routing Headers MUST be forwarded by default.
3. Security Considerations

Firewall devices MUST conform to the requirements in the previous section. In particular, packets containing specific extension headers are only to be discarded as a result of explicit policy, and never by default.

4. IANA Considerations

IANA is requested to replace the existing empty IPv6 Next Header Types registry by an IPv6 Extension Header Types registry, clearly marked as subsidiary to the existing Assigned Internet Protocol Numbers registry. It will contain only those protocol numbers which are also IPv6 Extension Header types. The initial list will be as follows:

- 0, Hop-by-Hop Options, [RFC2460]
- 43, Routing, [RFC2460], [RFC5095]
- 44, Fragment, [RFC2460]
- 50, Encapsulating Security Payload, [RFC4303]
- 51, Authentication, [RFC4302]
- 58, ICMPv6, [RFC2460]
- 59, No Next Header, [RFC2460]
- 60, Destination Options, [RFC2460]
- 135, MIPv6, [RFC6275]
- 139, HIP, [RFC5201]
- 140, shim6, [RFC5533]

Any future IPv6 Extension Header types will be added to this registry as well as to the Assigned Internet Protocol Numbers registry.

The reference to the IPv6 Next Header field in [RFC2780] applies equally to the IPv6 Extension Header field.

5. Acknowledgements

This document was triggered by mailing list discussions including John Leslie, Stefan Marksteiner and others. Valuable comments and contributions were made by TBD and others.

Brian Carpenter was a visitor at the Computer Laboratory, Cambridge University during part of this work.

This document was produced using the xml2rfc tool [RFC2629].
6. Change log [RFC Editor: Please remove]

draft-carpenter-6man-ext-transmission-00: original version, 2012-08-14.

7. References

7.1. Normative References


7.2. Informative References


Authors’ Addresses

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing 100095
P.R. China

Email: jiangsheng@huawei.com