IPv6 Universal Extension Header
draft-gont-6man-ipv6-universal-extension-header-01

Abstract

This document analyzes a problem in the Uniform Format for IPv6 Extension Headers specified in RFC 6564, which results in nodes not being able to process an IPv6 Header Chain if it contains an unrecognized IPv6 Extension Header that follows the aforementioned Uniform Format. It analyzes the implications of the aforementioned problem, and discusses a number of possible solutions, including the specification of a new IPv6 Extension Header – the Universal Extension Header – that overcomes the aforementioned issues.

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 October 10, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction

There has recently been a lot of work in the area of IPv6 Extension Headers. Firstly, there has been research about the extent to which IPv6 Extension Headers are dropped in the public Internet [GONT-IEPG-Nov13] [GONT-IEPG-Mar14], and debate about the motivation behind such policy [I-D.taylor-v6ops-fragdrop]. Secondly, there has been a fair share of work to improve some technicalities of IPv6 Extension Headers [RFC7112] [RFC7045], in the hopes that they can be reliably used in the public Internet.

A key challenge for IPv6 Extension Headers to be "deployable" in the public Internet is that they should not impair any nodes’s ability to process the entire IPv6 header chain. One of the steps meant in that direction has been the specification of a Uniform Format for IPv6
Extension Headers [RFC6564], which was meant to be employed by any IPv6 Extension Headers that might be defined in the future, such that middle-boxes can still process the entire IPv6 header chain if the new extension headers employ the Uniform Format. However, a problem in the aforementioned specification prevents such uniform format from being of use in practice.

Section 3 discusses the aforementioned flaw in the Uniform Format for Extension Headers specified in [RFC6564]. Section 4 explicitly describes the implications of the aforementioned flaw. Section 5 discusses possible workarounds for the aforementioned problem.

2. Terminology

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 RFC 2119 [RFC2119].

3. A Problem with RFC 6564

A key problem with the Uniform Format for IPv6 Extension Headers [RFC6564] lies in that both IPv6 Extension Headers and Transport Protocols share the same namespace ("Next Header" registry/namespace). Thus, given an "unknown Next Header value", it is impossible to tell whether the aforementioned value refers to an IPv6 Extension Header that employs the aforementioned uniform format, or an "unknown" upper-layer protocol (e.g. an "unknown" transport protocol). That is, while [RFC6564] specifies the syntax for the Uniform Format for IPv6 Extension Headers, but it does not provide a mechanism for a node to identify whether the aforementioned format is being employed in the first place.

4. Implications

The current impossibility to parse an IPv6 header chain that includes unknown Next Header values results in concrete implications for the extensibility of the IPv6 protocol, and the deployability of IPv6 extension headers. Namely,

- New IPv6 extension headers cannot be incrementally deployed.
- New transport protocols cannot be deployed.

Since there is no way for a node to process IPv6 extension headers that employ unknown next header values, an IPv6 host that receives a packet that employs a new IPv6 extension header will not be able to parse the IPv6 header chain past that unknown extension header, and hence it will drop the aforementioned packet. In a similar way, a
middlebox that needs to process the transport-protocol header will be faced with the dilemma of what to do with packets that employ unknown Next Header values. Since they will not be able to parse the IPv6 header chain past the unknown Next Header, it is very likely that they will drop such packets.

Unfortunately, since transport protocols share the same namespace as IPv6 Extension Headers, new transport protocols will pose the same challenge to middle-boxes, and hence they will be likely dropped in the network.

We believe that the current situation has implications that are generally overlooked, and that, whatever the outcome, it should be the result of an explicit decision by our community, rather than simply "omission".

5. Possible Solutions

The following subsections describe alternative solutions to the problem described in this document. Section 5.1 proposes to specify a new (and last) IPv6 header, such that any further IPv6 extensions employ such header. Section 5.2 simply proposes to reserve a range of "Next Header" values to be used with the Uniform Extension Header format specified in [RFC6564]. Finally, Section 5.3 simply proposes that no new IPv6 Extension Headers be allowed, and hence any unknown Next Header value is assumed to be an unknown upper-layer header (e.g. transport protocol header). Section 5.4 provides a summary and comparison of the properties of each of the different alternative solutions.

NOTE: We expect that the 6man wg arrives to consensus on pursuing any of these alternative solutions, and that the rest be abandoned in future revisions of this document.

5.1. Specification of a Universal Extension Header (UEH)

This solution implies the specification of a new (and last) IPv6 Extension Header, the IPv6 Universal Extension Header (UEH), which should be employed by any further IPv6 extensions. Additionally, specification of any further IPv6 Extension Headers are forbidden.

The advantages of this approach is that a single "Next Header" value is used for any future IPv6 Extensions (a new namespace is created by means of the "Subtype" field).

NOTE: Procedurally-speaking, the specification of the UEH could be performed by an update to RFC6564 (as proposed in the next
subsection), or by a new RFC that completely obsoletes [RFC6564], as in [rfc6564bis].

5.1.1. UEH Specification

The entire Section 4 of [RFC6564] is hereby replaced as follows:

New IPv6 Extension Headers MUST NOT be specified. Any IPv6 extensions that would require a new IPv6 Extension Header MUST be implemented with the Universal Extension Header specified in this document. This minimizes breakage in intermediate nodes that examine these extension headers.

This document specifies a new IPv6 Extension Header: Universal Extension Header. This Extension Header is identified by the value [TBD] of [IANA-IP-PROTO]. The syntax of the Universal Extension Header is:

```
+-------------+-------------+-------------+
| Next Header | Hdr Ext Len | Subtype     |
+-------------+-------------+-------------+
```

where:

**Next Header**
8-bit selector. Identifies the type of header immediately following the extension header. Uses the same values as the IPv4 Protocol field [IANA-IP-PROTO].

**Hdr Ext Len**
8-bit unsigned integer. Length of the extension header in 8-octet units, not including the first 8 octets.

**Subtype**
8-bit unsigned integer. Specifies the subtype for this extension header. It uses a new namespace managed by IANA [IANA-UEH].

**Subtype Specific Data**
Variable length. Fields specific to this extension header/Subtype.

The Universal Extension Header specified in this document MAY appear multiple times in the same IPv6 packet.

5.1.2. IANA Considerations for UEH

IANA is requested to create a new registry to maintain the Universal Extension Header Subtypes [IANA-UEH].

5.1.3. Operation of the UEH

This section discusses the operation of the Universal Extension Header.

The goal of the UEH is to provide for a common syntax for all future IPv6 extensions. Any future extension headers will be encoded in a UEH, and will be identified by a specific UEH Subtype assigned by IANA at the time the corresponding specification is published. The UEH thus provides for the "common syntax" required to process "unrecognized extensions", and the Subtype field identifies the specific extension being encoded in the UEH. Any "future extension headers" would actually be new Subtypes (assigned by IANA) of the UEH.

As a result, in the event an unrecognized Next Header value is encountered by a node, the node will be able to assume that such Next Header value identifies an upper-layer protocol, rather than an extension header.

5.2. Reserving a Next Header range for RFC 6564

Another possible solution would be to instruct IANA to reserve a range of Next Header values to be employed for IPv6 Extension Headers employing the Uniform Extension Header format specified in [RFC6564]. Thus, a node that receives a packet with an unknown Next Header value would proceed as follows:

- If the unknown Next Header value is in the range assigned by IANA for RFC6564, the aforementioned header is assumed to follow the Uniform Extension Header specified in [RFC6564].

- Otherwise, the Next Header value is assumed to refer to an upper-layer protocol header (e.g., a transport protocol).
The advantage of this solution is that it requires very little standardization effort. The drawback is that a potentially large number of "Next Header" values might be wasted.

5.3. Prohibiting New Extension Headers

Among the possible solutions is to simply prohibit the specification of any new IPv6 Extension Headers. Thus, an unknown "Next Header" value would unambiguously refer to an upper-layer protocol (e.g. a transport protocol).

The advantage of this approach is that it requires minimum standardization work. The drawback is that, while it is generally assumed that any new extensions could be implemented with the existing IPv6 Extension Headers, it might be premature to forbid the specification of new extension headers at this point in time.

5.4. Summary and comparison of the possible solutions

<table>
<thead>
<tr>
<th>Solution</th>
<th>Pros</th>
<th>Cons</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEH</td>
<td>Uses only one Next Header value</td>
<td>?</td>
<td>Section 5.1</td>
</tr>
<tr>
<td>Range for RFC 6564</td>
<td>Less std effort?</td>
<td>Potentially wastes NH values</td>
<td>Section 5.2</td>
</tr>
<tr>
<td>Forbid all new EHs</td>
<td>?</td>
<td>May limit future extensions</td>
<td>Section 5.3</td>
</tr>
</tbody>
</table>

Table 1: Summary of alternative solutions

6. IANA Considerations

The contents of this section will depend on the solution the 6man wg adopts.

7. Security Considerations

The inability to parse an entire IPv6 header chain prevents the enforcement of even simple ACLs. This document describes possible solutions to this problem such that, if deemed necessary, middle-boxes can process the entire IPv6 header chain to Enabling middle-boxes such as firewalls to inspect the entire IPv6 header chain even in the presence of unrecognized extensions allows for security
mechanisms to be implemented, and for proper functioning of other
middle-boxes such as load-balancers.

8. Acknowledgements

The solution specified in Section 5.2 had originally been proposed in
[I-D.pfeifer-6man-exthdr-res].

The authors would like to thank (in alphabetical order) Ran Atkinson,
Brian Carpenter, Ray Hunter, and Thomas Narten, for providing
valuable input on earlier versions of this document.

9. Contributors

C.M. Heard identified the problems related with the Uniform Format
for IPv6 Extension Headers specified in [RFC6564], and participated
in the brainstorming that led to this document.

10. References

10.1. Normative References


[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

[RFC6564] Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., and
M. Bhatia, "A Uniform Format for IPv6 Extension Headers",
RFC 6564, April 2012.


10.2. Informative References

[RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of

[I-D.taylor-v6ops-fragdrop]
Jaeggli, J., Colitti, L., Kumari, W., Vyncke, E., Kaeo,
M., and T. Taylor, "Why Operators Filter Fragments and
What It Implies", draft-taylor-v6ops-fragdrop-02 (work in
progress), December 2013.
[I-D.pfeifer-6man-exthdr-res]
Pfeifer, H., "IPv6 Extension Headers Reserved Space",
draft-pfeifer-6man-exthdr-res-01 (work in progress),
September 2011.

[GONT-IEPG-Nov13]
Gont, F., "Fragmentation and Extension Header Support in
the IPv6 Internet", IEPG 88, November 3, 2013. Vancouver,

[GONT-IEPG-Mar14]
Gont, F. and T. Chown, "More results from measurements of
gont-iepg-ietf89-eh-update.pdf>.

[IANA-IP-PROTO]
Internet Assigned Numbers Authority, "Assigned Internet
assignments/protocol-numbers/protocol-numbers.xhtml>.

[IANA-UEH]
Internet Assigned Numbers Authority, "Universal Extension
Header Subtypes", 2014.

[rfc6564bis]
Gont, F., Liu, W., Pfeifer, H., and S. Krishnan, "A
Uniform Format for IPv6 Extension Headers",
draft-gont-6man-rfc6564bis-00, Work in Progress, April 2014.

Authors’ Addresses

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires  1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI:    http://www.si6networks.com
Will (Shucheng) Liu
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com

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

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

Hagen Paul Pfeifer
Rohde & Schwarz
Muehldorfstrasse 15
Munich 81671
Germany

Phone: +49 89 4129 15515
Email: hagen.pfeifer@rohde-schwarz.com
URI: http://www.rohde-schwarz.com/