Internet Engineering Task Force (IETF)
Request for Comments: 7045
Updates: 2460, 2780
Category: Standards Track
ISSN: 2070-1721

B. Carpenter
Univ. of Auckland
S. Jiang
Huawei Technologies Co., Ltd.

December 2013

# Transmission and Processing of IPv6 Extension Headers

## Abstract

Various IPv6 extension headers have been standardised since the IPv6 standard was first published. This document updates RFC 2460 to clarify how intermediate nodes should deal with such extension headers and with any that are defined in the 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7045.

Table of Contents



## 1. Introduction and Problem Statement

In IPv6, an extension header is any header that follows the initial 40 bytes of the packet and precedes the upper-layer header (which might be a transport header, an ICMPv6 header, or a notional "No Next Header").

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 meant that forwarding nodes should be completely transparent to extension headers. There was no provision for forwarding nodes to modify them, remove them, insert them, or use them to affect forwarding behaviour. Thus, new extension headers could be introduced progressively and used only by hosts that have been updated to create and interpret them [RFC6564]. The extension header mechanism is an important part of the IPv6 architecture, and several new extension headers have been standardised since RFC 2460 was published.

Today, IPv6 packets are not always forwarded by straightforward IP routing based on their first 40 bytes. Some routers, and a variety of intermediate nodes often referred to as middleboxes, such as firewalls, load balancers, or packet classifiers, might inspect other parts of each packet. Indeed, such middlebox functions are often embedded in routers. However, experience has shown that as a result, the network is not transparent to IPv6 extension headers. Contrary to Section 4 of RFC 2460, middleboxes sometimes examine and process

the entire IPv6 packet before making a decision to either forward or discard the packet. This means that they need to traverse the chain of extension headers, if present, until they find the transport header (or an encrypted payload). Unfortunately, because not all IPv6 extension headers follow a uniform TLV format, this process is clumsy and requires knowledge of each extension header's format. A separate problem is that the header chain may even be fragmented [HEADER-CHAIN].

The process is potentially slow as well as clumsy, possibly precluding its use in nodes attempting to process packets at line speed. The present document does not intend to solve this problem, which is caused by the fundamental architecture of IPv6 extension headers. This document focuses on clarifying how the header chain should be handled in the current IPv6 architecture.

If they encounter an unrecognised extension header type, some firewalls treat the packet as suspect and drop it. Unfortunately, it is an established fact that several widely used firewalls do not recognise some or all of the extension headers standardised since RFC 2460 was published. It has also been observed that certain firewalls do not even handle all the extension headers standardised in RFC 2460, including the fragment header [FRAGDROP], causing fundamental problems of end-to-end connectivity. This applies in particular to firewalls that attempt to inspect packets at very high speed, since they cannot take the time to reassemble fragmented packets, especially when under a denial-of-service attack.

Other types of middleboxes, 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 standard extension headers. An implementor who consults only RFC 2460 will miss all extension headers defined subsequently.

This combination of circumstances creates a "Catch-22" situation [Heller] for the deployment of any newly standardised extension header except for local use. It cannot be widely deployed because existing middleboxes will drop it on many paths through the Internet. However, most middleboxes will not be updated to allow the new header to pass until it has been proved safe and useful on the open Internet, which is impossible until the middleboxes have been updated.

The uniform TLV format now defined for extension headers [RFC6564] will improve the situation, but only for future extensions. Some tricky and potentially malicious cases will be avoided by forbidding very long chains of extension headers that need to be fragmented [HEADER-CHAIN]. This will alleviate concerns that stateless firewalls cannot locate a complete header chain as required by the present document.

However, these changes are insufficient to correct the underlying problem. The present document clarifies that the above requirement from RFC 2460 applies to all types of nodes that forward IPv6 packets and to all extension headers standardised now and in the future. It also requests that IANA create a subsidiary registry that clearly identifies extension header types and updates RFC 2780 accordingly. Fundamental changes to the IPv6 extension header architecture are out of scope for this document.

Also, hop-by-hop options are not handled by many high-speed routers or are processed only on a slow path. This document also updates the requirements for processing the Hop-by-Hop Options header to make them more realistic.

## 1.1. 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 [RFC2119].

In the remainder of this document, the term "forwarding node" refers to any router, firewall, load balancer, prefix translator, or any other device or middlebox that forwards IPv6 packets with or without examining the packet in any way.

In this document, "standard" IPv6 extension headers are those specified in detail by IETF Standards Actions [RFC5226]. "Experimental" extension headers include those defined by any Experimental RFC and the header values 253 and 254 defined by [RFC3692] and [RFC4727] when used as experimental extension headers. "Defined" extension headers are the "standard" extension headers plus the "experimental" ones.

## 2. Requirement to Transmit Extension Headers

### 2.1. All Extension Headers

As mentioned above, forwarding nodes that discard packets containing extension headers are known to cause connectivity failures and deployment problems. Therefore, it is important that forwarding nodes that inspect IPv6 headers be able to parse all defined extension headers and deal with them appropriately, as specified in this section.

Any forwarding node along an IPv6 packet's path, which forwards the packet for any reason, SHOULD do so regardless of any extension headers that are present, as required by RFC 2460. Exceptionally, if a forwarding node is designed to examine extension headers for any reason, such as firewalling, it MUST recognise and deal appropriately with all standard IPv6 extension header types and SHOULD recognise and deal appropriately with experimental IPv6 extension header types. The list of standard and experimental extension header types is maintained by IANA (see Section 4), and implementors are advised to check this list regularly for updates.

RFC 2460 requires destination hosts to discard packets containing unrecognised extension headers. However, intermediate forwarding nodes SHOULD NOT do this, since that might cause them to inadvertently discard traffic using a recently standardised extension header not yet recognised by the intermediate node. The exceptions to this rule are discussed next.

If a forwarding node discards a packet containing a standard IPv6 extension header, it MUST be the result of a configurable policy and not just the result of a failure to recognise such a header. This means that the discard policy for each standard type of extension header MUST be individually configurable. The default configuration SHOULD allow all standard extension headers.

Experimental IPv6 extension headers SHOULD be treated in the same way as standard extension headers, including an individually configurable discard policy. However, the default configuration MAY drop experimental extension headers.

Forwarding nodes MUST be configurable to allow packets containing unrecognised extension headers, but the default configuration MAY drop such packets.

The IPv6 Routing Header Types 0 and 1 have been deprecated. Note that Type 0 was deprecated by [RFC5095]. However, this does not mean that the IPv6 Routing Header can be unconditionally dropped by

forwarding nodes. Packets containing standardised and undeprecated Routing Headers SHOULD be forwarded by default. At the time of writing, these include Type 2 [RFC6275], Type 3 [RFC6554], and the experimental Routing Header Types 253 and 254 [RFC4727]. Others may be defined in the future.

### 2.2. Hop-by-Hop Options

The IPv6 Hop-by-Hop Options header SHOULD be processed by intermediate forwarding nodes as described in [RFC2460]. However, it is to be expected that 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 need to be aware of this likely behaviour.

As a reminder, in RFC 2460, it is stated that the Hop-by-Hop Options header, if present, must be first.

## 3. Security Considerations

Forwarding nodes that operate as firewalls MUST conform to the requirements in the previous section in order to respect the IPv6 extension header architecture. In particular, packets containing standard extension headers are only to be discarded as a result of an intentionally configured policy.

These changes do not affect a firewall’s ability to filter out traffic containing unwanted or suspect extension headers, if configured to do so. However, the changes do require firewalls to be capable of permitting any or all extension headers, if configured to do so. The default configurations are intended to allow normal use of any standard extension header, avoiding the connectivity issues described in Sections 1 and 2.1.

As noted above, the default configuration might drop packets containing experimental extension headers. There is no header length field in an IPv6 header, and header types 253 and 254 might be used either for experimental extension headers or for experimental payload types. Therefore, there is no generic algorithm by which a firewall can distinguish these two cases and analyze the remainder of the packet. This should be considered when deciding on the appropriate default action for header types 253 and 254.

When new extension headers are standardised in the future, those implementing and configuring forwarding nodes, including firewalls, will need to take them into account. A newly defined header will exercise new code paths in a host that does recognise it, so caution may be required. Additional security issues with experimental values

or new extension headers are to be found in [RFC4727] and [RFC6564]. As a result, it is to be expected that the deployment process will be slow and will depend on satisfactory operational experience. Until deployment is complete, the new extension will fail in some parts of the Internet. This aspect needs to be considered when deciding to standardise a new extension. Specific security considerations for each new extension should be documented in the document that defines it.

## 4. IANA Considerations

IANA has added an extra column titled "IPv6 Extension Header" to the "Assigned Internet Protocol Numbers" registry to clearly mark those values that are also IPv6 extension header types defined by an IETF Standards Action or IESG Approval (see list below). This also applies to IPv6 extension header types defined in the future.

Additionally, IANA has closed the existing empty "Next Header Types" registry to new entries and is redirecting its users to a new "IPv6 Extension Header Types" registry. This registry contains only those protocol numbers that are also marked as IPv6 Extension Header types in the "Assigned Internet Protocol Numbers" registry. Experimental values will be marked as such. The initial list will be as follows:

- 0, IPv6 Hop-by-Hop Option, [RFC2460]
- 43, Routing Header for IPv6, [RFC2460], [RFC5095]
- 44, Fragment Header for IPv6, [RFC2460]
- 50, Encapsulating Security Payload, [RFC4303]
- 51, Authentication Header, [RFC4302]
- 60, Destination Options for IPv6, [RFC2460]
- 135, Mobility Header, [RFC6275]
- 139, Experimental use, Host Identity Protocol [RFC5201]
- 140, Shim6 Protocol, [RFC5533]
- 253, Use for experimentation and testing, [RFC3692], [RFC4727]
- 254, Use for experimentation and testing, [RFC3692], [RFC4727]

This list excludes type 59, No Next Header, [RFC2460], which is not an extension header as such.

The references to the IPv6 Next Header field in [RFC2780] are to be interpreted as also applying to the IPv6 Extension Header field, and the "IPv6 Extension Header Types" registry will be managed accordingly.

## 5. Acknowledgements

This document was triggered by mailing list discussions including John Leslie, Stefan Marksteiner, and others. Valuable comments and contributions were made by Dominique Barthel, Tim Chown, Lorenzo Colitti, Fernando Gont, C. M. Heard, Bob Hinden, Ray Hunter, Suresh Krishnan, Marc Lampo, Sandra Murphy, Michael Richardson, Dan Romascanu, Dave Thaler, Joe Touch, Bjoern Zeeb, and others.

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

## 6. References

### 6.1. 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.

[RFC2780] Bradner, S. and V. Paxson, "IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers", BCP 37, RFC 2780, March 2000.

[RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, January 2004.

[RFC4727] Fenner, B., "Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", RFC 4727, November 2006.

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

### 6.2. Informative References

[FRAGDROP] Jaeggli, J., Colitti, L., Kumari, W., Vyncke, E., Kaeo, M., and T. Taylor, "Why Operators Filter Fragments and What It Implies", Work in Progress, June 2013.

[HEADER-CHAIN] Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", Work in Progress, October 2013.

[Heller] Heller, J., "Catch-22", Simon and Schuster, November 1961.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.

[RFC5201] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, June 2009.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, March 2012.

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