

opsec  
Internet-Draft  
Intended status: Informational  
Expires: July 23, 2021

F. Gont  
SI6 Networks  
W. Liu  
Huawei Technologies  
January 19, 2021

**Recommendations on the Filtering of IPv6 Packets Containing IPv6  
Extension Headers at Transit Routers  
draft-ietf-opsec-ipv6-eh-filtering-07**

**Abstract**

This document analyzes the security implications of IPv6 Extension Headers and associated IPv6 options. Additionally, it discusses the operational and interoperability implications of discarding packets based on the IPv6 Extension Headers and IPv6 options they contain. Finally, it provides advice on the filtering of such IPv6 packets at transit routers for traffic *not* directed to them, for those cases where such filtering is deemed as necessary.

**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 July 23, 2021.

**Copyright Notice**

Copyright (c) 2021 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 (<https://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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology and Conventions Used in This Document . . . . .	<a href="#">4</a>
<a href="#">2.1.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">2.2.</a>	Applicability Statement . . . . .	<a href="#">4</a>
<a href="#">2.3.</a>	Conventions . . . . .	<a href="#">4</a>
<a href="#">3.</a>	IPv6 Extension Headers . . . . .	<a href="#">5</a>
<a href="#">3.1.</a>	General Discussion . . . . .	<a href="#">5</a>
<a href="#">3.2.</a>	General Security Implications . . . . .	<a href="#">6</a>
3.3.	Summary of Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers . . . . .	<a href="#">6</a>
3.4.	Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers . . . . .	<a href="#">7</a>
3.5.	Advice on the Handling of Packets with Unknown IPv6 Extension Headers . . . . .	<a href="#">16</a>
<a href="#">4.</a>	IPv6 Options . . . . .	<a href="#">17</a>
<a href="#">4.1.</a>	General Discussion . . . . .	<a href="#">17</a>
<a href="#">4.2.</a>	General Security Implications of IPv6 Options . . . . .	<a href="#">17</a>
4.3.	Advice on the Handling of Packets with Specific IPv6 Options . . . . .	<a href="#">17</a>
4.4.	Advice on the handling of Packets with Unknown IPv6 Options . . . . .	<a href="#">30</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">30</a>
<a href="#">6.</a>	Privacy Considerations . . . . .	<a href="#">30</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">30</a>
<a href="#">8.</a>	Acknowledgements . . . . .	<a href="#">31</a>
<a href="#">9.</a>	References . . . . .	<a href="#">31</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">31</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">35</a>
	Authors' Addresses . . . . .	<a href="#">37</a>

## [1.](#) Introduction

IPv6 Extension Headers (EHs) allow for the extension of the IPv6 protocol, and provide support for core functionality such as IPv6 fragmentation. However, common implementation limitations suggest that EHs present a challenge for IPv6 packet routing equipment, particularly when the IPv6 header chain needs to be processed for e.g. enforcing ACLs or implementing other functions [[I-D.ietf-v6ops-ipv6-ehs-packet-drops](#)].



Recent studies (see e.g. [[RFC7872](#)]) suggest that there is widespread dropping of IPv6 packets that contain IPv6 Extension Headers (EHs). In some cases, such packet drops occur at transit routers. While some operators "officially" drop packets that contain IPv6 EHs, it is possible that some of the measured packet drops be the result of improper configuration defaults, or inappropriate advice in this area.

This document analyzes both the general security implications of IPv6 EHs, as well as the security implications of specific EH and Option types. It also provides advice on the filtering of IPv6 packets based on the IPv6 EHs and the IPv6 options they contain. Since various protocols may use IPv6 EHs (possibly with IPv6 options), discarding packets based on the IPv6 EHs or IPv6 options they contain can have implications on the proper functioning of such protocols. Thus, this document also attempts to discuss the operational and interoperability implications of such filtering policies.

The resulting packet filtering policy typically depends on where in the network such policy is enforced: when the policy is enforced in a transit network, the policy typically follows a "deny-list" approach, where only packets with clear negative implications are dropped. On the other hand, when the policy is enforced closer to the destination systems, the policy typically follows an "accept-list" approach, where only traffic that is expected to be received is allowed. The advice in this document is aimed only at transit routers that may need to enforce a filtering policy based on the EHs and IPv6 options a packet may contain, following a "deny-list" approach, and hence is likely to be much more permissive than a filtering policy to be employed at e.g. the edge of an enterprise network. The advice in this document is meant to improve the current situation of the dropping of packets with IPv6 EHs in the Internet [[RFC7872](#)] in such cases where packets are being dropped due to inappropriate or missing guidelines.

This document is similar in nature to [[RFC7126](#)], which addresses the same problem for the IPv4 case. However, in IPv6, the problem space is compounded by the fact that IPv6 specifies a number of IPv6 EHs, and a number of IPv6 options which may be valid only when included in specific EH types.

This document completes and complements the considerations for protecting the control plane from packets containing IP options that can be found in [[RFC6192](#)].

[Section 2](#) of this document specifies the terminology and conventions employed throughout this document. [Section 3](#) of this document discusses IPv6 EHs and provides advice in the area of filtering IPv6



packets that contain such IPv6 EHs. [Section 4](#) of this document discusses IPv6 options and provides advice in the area of filtering IPv6 packets that contain such options.

## **2. Terminology and Conventions Used in This Document**

### **2.1. Terminology**

The terms "permit" (allow the traffic), "drop" (drop with no notification to sender), and "reject" (drop with appropriate notification to sender) are employed as defined in [\[RFC3871\]](#). Throughout this document we also employ the term "discard" as a generic term to indicate the act of discarding a packet, irrespective of whether the sender is notified of such drops, and irrespective of whether the specific filtering action is logged.

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.

### **2.2. Applicability Statement**

This document provides advice on the filtering of IPv6 packets with EHs at transit routers for traffic *\*not\** explicitly destined to them, for cases in which such filtering is deemed as necessary.

### **2.3. Conventions**

This document assumes that nodes comply with the requirements in [\[RFC7045\]](#). Namely,

- o If a forwarding node discards a packet containing a standard IPv6 EH, it **MUST** be the result of a configurable policy and not just the result of a failure to recognise such a header.
- o The discard policy for each standard type of EH **MUST** be individually configurable.
- o The default configuration should allow all standard IPv6 EHs.

The advice provided in this document is only meant to guide an operator in configuring forwarding devices, and is *\*not\** to be interpreted as advice regarding default configuration settings for network devices. That is, this document provides advice with respect to operational configurations, but does not change the implementation defaults required by [\[RFC7045\]](#).



We recommend that configuration options are made available to govern the processing of each IPv6 EH type and each IPv6 option type. Such configuration options should include the following possible settings:

- o Permit this IPv6 EH or IPv6 Option type.
- o Discard (and log) packets containing this IPv6 EH or option type.
- o Reject (and log) packets containing this IPv6 EH or option type (where the packet drop is signaled with an ICMPv6 error message).
- o Rate-limit traffic containing this IPv6 EH or option type.
- o Ignore this IPv6 EH or option type (as if it was not present) and forward the packet. We note that if a packet carries forwarding information (e.g., in an IPv6 Routing Header) this might be an inappropriate or undesirable action.

We note that special care needs to be taken when devices log packet drops/rejects. Devices should count the number of packets dropped/rejected, but the logging of drop/reject events should be limited so as to not overburden device resources.

Finally, we note that when discarding packets, it is generally desirable that the sender be signaled of the packet drop, since this is of use for trouble-shooting purposes. However, throughout this document (when recommending that packets be discarded) we generically refer to the action as "discard" without specifying whether the sender is signaled of the packet drop.

### **3. IPv6 Extension Headers**

#### **3.1. General Discussion**

IPv6 [[RFC8200](#)] EHs allow for the extension of the IPv6 protocol. Since both IPv6 EHs and upper-layer protocols share the same namespace ("Next Header" registry/namespace), [[RFC7045](#)] identifies which of the currently assigned Internet Protocol numbers identify IPv6 EHs vs. upper-layer protocols. This document discusses the filtering of packets based on the IPv6 EHs (as specified by [[RFC7045](#)]) they contain.

NOTE: [[RFC8200](#)] specifies that non-fragmented IPv6 datagrams and IPv6 First-Fragments must contain the entire IPv6 header chain [[RFC7112](#)]. Therefore, intermediate systems can enforce the filtering policies discussed in this document, or resort to simply discarding the offending packets when they fail to comply with the requirements in [[RFC8200](#)]. We note that, in order to implement



filtering rules on the fast path, it may be necessary for the filtering device to limit the depth into the packet that can be inspected before giving up. In circumstances where such a limitation exists, it is recommended that implementations provide a configuration option that specifies whether to discard packets if the aforementioned limit is encountered. Operators may then determine according to their own circumstances how such packets will be handled.

### **3.2. General Security Implications**

In some device architectures, IPv6 packets that contain IPv6 EHs can cause the corresponding packets to be processed on the slow path, and hence may be leveraged for the purpose of Denial of Service (DoS) attacks [[I-D.ietf-v6ops-ipv6-ehs-packet-drops](#)] [[Cisco-EH](#)] [[FW-Benchmark](#)].

Operators are urged to consider the IPv6 EH and IPv6 options handling capabilities of their devices as they make deployment decisions in future.

### **3.3. Summary of Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers**

This section summarizes the advice provided in [Section 3.4](#), providing references to the specific sections in which a detailed analysis can be found.



EH type	Filtering policy	Reference
IPv6 Hop-by-Hop Options (Proto=0)	Drop or Ignore	<a href="#">Section 3</a> .4.1
Routing Header for IPv6 (Proto=43)	Drop only RHT0 and RHT1. Permit other RH Types	<a href="#">Section 3</a> .4.2
Fragment Header for IPv6 (Proto=44)	Permit	<a href="#">Section 3</a> .4.3
Encapsulating Security Payload (Proto=50)	Permit	<a href="#">Section 3</a> .4.4
Authentication Header (Proto=51)	Permit	<a href="#">Section 3</a> .4.5
Destination Options for IPv6 (Proto=60)	Permit	<a href="#">Section 3</a> .4.6
Mobility Header (Proto=135)	Permit	<a href="#">Section 3</a> .4.7
Host Identity Protocol (Proto=139)	Permit	<a href="#">Section 3</a> .4.8
Shim6 Protocol (Proto=140)	Permit	<a href="#">Section 3</a> .4.9
Use for experimentation and testing (Proto=253 and 254)	Drop	<a href="#">Section 3</a> .4.10

Table 1: Summary of Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers

### **3.4. Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers**

#### **3.4.1. IPv6 Hop-by-Hop Options (Protocol Number=0)**

##### **3.4.1.1. Uses**

The Hop-by-Hop Options header is used to carry optional information that may be examined by every node along a packet's delivery path.



It is expected that nodes will examine the Hop-by-Hop Options header if explicitly configured to do so.

NOTE: A previous revision of the IPv6 core specification, [\[RFC2460\]](#), originally required that all nodes examine and processed the Hop-by-Hop Options header. However, even before the publication of [\[RFC8200\]](#) a number of implementations already provided the option of ignoring this header unless explicitly configured to examine it.

#### **[3.4.1.2](#). Specification**

This EH is specified in [\[RFC8200\]](#). At the time of this writing, the following options have been specified for the Hop-by-Hop Options EH:

- o Type 0x00: Pad1 [\[RFC8200\]](#)
- o Type 0x01: PadN [\[RFC8200\]](#)
- o Type 0x05: Router Alert [\[RFC2711\]](#)
- o Type 0x07: CALIPSO [\[RFC5570\]](#)
- o Type 0x08: SMF\_DPD [\[RFC6621\]](#)
- o Type 0x23: RPL Option [\[I-D.ietf-roll-useofrplinfo\]](#)
- o Type 0x26: Quick-Start [\[RFC4782\]](#)
- o Type 0x4D: (Deprecated)
- o Type 0x63: RPL Option [\[RFC6553\]](#)
- o Type 0x6D: MPL Option [\[RFC7731\]](#)
- o Type 0x8A: Endpoint Identification (Deprecated) [\[draft-ietf-nimrod-eid\]](#)
- o Type 0xC2: Jumbo Payload [\[RFC2675\]](#)
- o Type 0xEE: IPv6 DFF Header [\[RFC6971\]](#)
- o Type 0x1E: [RFC3692](#)-style Experiment [\[RFC4727\]](#)
- o Type 0x3E: [RFC3692](#)-style Experiment [\[RFC4727\]](#)
- o Type 0x5E: [RFC3692](#)-style Experiment [\[RFC4727\]](#)
- o Type 0x7E: [RFC3692](#)-style Experiment [\[RFC4727\]](#)



- o Type 0x9E: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0xBE: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0xDE: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0xFE: [RFC3692](#)-style Experiment [[RFC4727](#)]

#### **3.4.1.3. Specific Security Implications**

Legacy nodes that process this extension header might be subject to Denial of Service attacks.

NOTE: While [[RFC8200](#)] has removed this requirement, the deployed base may still reflect the traditional behavior for a while, and hence the potential security problems of this EH are still of concern.

#### **3.4.1.4. Operational and Interoperability Impact if Blocked**

Discarding packets containing a Hop-by-Hop Options EH would break any of the protocols that rely on it for proper functioning. For example, it would break RSVP [[RFC2205](#)] and multicast deployments, and would cause IPv6 jumbograms to be discarded.

#### **3.4.1.5. Advice**

Nodes implementing [[RFC8200](#)] would already ignore this extension header unless explicitly required to process it. For legacy ([[RFC2460](#)]) nodes, the recommended configuration for the processing of these packets depends on the features and capabilities of the underlying platform, the configuration of the platform, and also the deployment environment of the platform. On platforms that allow forwarding of packets with HBH Options on the fast path, we recommend that packets with a HBH Options EH be forwarded as normal. Otherwise, on platforms in which processing of packets with a IPv6 HBH Options EH is carried out in the slow path, and an option is provided to rate-limit these packets, we recommend that this option be selected. Finally, when packets containing a HBH Options EH are processed in the slow-path, and the underlying platform does not have any mitigation options available for attacks based on these packets, we recommend that such platforms discard packets containing IPv6 HBH Options EHs.

Finally, we note that, for obvious reasons, RPL (Routing Protocol for Low-Power and Lossy Networks) [[RFC6550](#)] routers must not discard packets based on the presence of an IPv6 Hop-by-Hop Options EH.



### **3.4.2. Routing Header for IPv6 (Protocol Number=43)**

#### **3.4.2.1. Uses**

The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination.

#### **3.4.2.2. Specification**

This EH is specified in [[RFC8200](#)]. [[RFC2460](#)] had originally specified the Routing Header Type 0, which was later obsoleted by [[RFC5095](#)], and thus removed from [[RFC8200](#)].

At the time of this writing, the following Routing Types have been specified:

- o Type 0: Source Route (DEPRECATED) [[RFC2460](#)] [[RFC5095](#)]
- o Type 1: Nimrod (DEPRECATED)
- o Type 2: Type 2 Routing Header [[RFC6275](#)]
- o Type 3: RPL Source Route Header [[RFC6554](#)]
- o Type 4: Segment Routing Header (SRH) [[RFC8754](#)]
- o Types 5-252: Unassigned
- o Type 253: [RFC3692](#)-style Experiment 1 [[RFC4727](#)]
- o Type 254: [RFC3692](#)-style Experiment 2 [[RFC4727](#)]
- o Type 255: Reserved

#### **3.4.2.3. Specific Security Implications**

The security implications of RHT0 have been discussed in detail in [[Biondi2007](#)] and [[RFC5095](#)]. The security implications of RHT4 (SRH) are discussed in [[RFC8754](#)].

#### **3.4.2.4. Operational and Interoperability Impact if Blocked**

Blocking packets containing a RHT0 or RHT1 has no operational implications, since both have been deprecated. Blocking packets with a RHT4 (SRH) will break Segment Routing (SR) deployments, if the filtering policy is enforced on packets being forwarded within an SR domain.



#### **3.4.2.5. Advice**

Intermediate systems should discard packets containing a RHT0 or RHT1. Other routing header types should be permitted, as required by [\[RFC7045\]](#).

### **3.4.3. Fragment Header for IPv6 (Protocol Number=44)**

#### **3.4.3.1. Uses**

This EH provides the fragmentation functionality for IPv6.

#### **3.4.3.2. Specification**

This EH is specified in [\[RFC8200\]](#).

#### **3.4.3.3. Specific Security Implications**

The security implications of the Fragment Header range from Denial of Service attacks (e.g. based on flooding a target with IPv6 fragments) to information leakage attacks [\[RFC7739\]](#).

#### **3.4.3.4. Operational and Interoperability Impact if Blocked**

Blocking packets that contain a Fragment Header will break any protocol that may rely on fragmentation (e.g., the DNS [\[RFC1034\]](#)). However, IP fragmentation is known to introduce fragility to Internet communication [\[RFC8900\]](#).

#### **3.4.3.5. Advice**

Intermediate systems should permit packets that contain a Fragment Header.

### **3.4.4. Encapsulating Security Payload (Protocol Number=50)**

#### **3.4.4.1. Uses**

This EH is employed for the IPsec suite [\[RFC4303\]](#).

#### **3.4.4.2. Specification**

This EH is specified in [\[RFC4303\]](#).



#### **3.4.4.3. Specific Security Implications**

Besides the general implications of IPv6 EHs, this EH could be employed to potentially perform a DoS attack at the destination system by wasting CPU resources in validating the contents of the packet.

#### **3.4.4.4. Operational and Interoperability Impact if Blocked**

Discarding packets that employ this EH would break IPsec deployments.

#### **3.4.4.5. Advice**

Intermediate systems should permit packets containing the Encapsulating Security Payload EH.

### **3.4.5. Authentication Header (Protocol Number=51)**

#### **3.4.5.1. Uses**

The Authentication Header can be employed for provide authentication services in IPv4 and IPv6.

#### **3.4.5.2. Specification**

This EH is specified in [[RFC4302](#)].

#### **3.4.5.3. Specific Security Implications**

Besides the general implications of IPv6 EHs, this EH could be employed to potentially perform a DoS attack at the destination system by wasting CPU resources in validating the contents of the packet.

#### **3.4.5.4. Operational and Interoperability Impact if Blocked**

Discarding packets that employ this EH would break IPsec deployments.

#### **3.4.5.5. Advice**

Intermediate systems should permit packets containing an Authentication Header.

### **3.4.6. Destination Options for IPv6 (Protocol Number=60)**



#### **3.4.6.1. Uses**

The Destination Options header is used to carry optional information that needs be examined only by a packet's destination node(s).

#### **3.4.6.2. Specification**

This EH is specified in [[RFC8200](#)]. At the time of this writing, the following options have been specified for this EH:

- o Type 0x00: Pad1 [[RFC8200](#)]
- o Type 0x01: PadN [[RFC8200](#)]
- o Type 0x04: Tunnel Encapsulation Limit [[RFC2473](#)]
- o Type 0x4D: (Deprecated)
- o Type 0xC9: Home Address [[RFC6275](#)]
- o Type 0x8A: Endpoint Identification (Deprecated) [[draft-ietf-nimrod-eid](#)]
- o Type 0x8B: ILNP Nonce [[RFC6744](#)]
- o Type 0x8C: Line-Identification Option [[RFC6788](#)]
- o Type 0x1E: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0x3E: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0x5E: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0x7E: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0x9E: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0xBE: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0xDE: [RFC3692](#)-style Experiment [[RFC4727](#)]
- o Type 0xFE: [RFC3692](#)-style Experiment [[RFC4727](#)]

#### **3.4.6.3. Specific Security Implications**

No security implications are known, other than the general implications of IPv6 EHs. For a discussion of possible security



implications of specific options specified for the D0 header, please see the [Section 4.3](#).

#### **[3.4.6.4](#). Operational and Interoperability Impact if Blocked**

Discarding packets that contain a Destination Options header would break protocols that rely on this EH type for conveying information, including protocols such as ILNP [[RFC6740](#)] and Mobile IPv6 [[RFC6275](#)], and IPv6 tunnels that employ the Tunnel Encapsulation Limit option.

#### **[3.4.6.5](#). Advice**

Intermediate systems should permit packets that contain a Destination Options Header.

#### **[3.4.7](#). Mobility Header (Protocol Number=135)**

##### **[3.4.7.1](#). Uses**

The Mobility Header is an EH used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings in Mobile IPv6.

##### **[3.4.7.2](#). Specification**

This EH is specified in [[RFC6275](#)].

##### **[3.4.7.3](#). Specific Security Implications**

A thorough security assessment of the security implications of the Mobility Header and related mechanisms can be found in [Section 15 of \[RFC6275\]](#).

##### **[3.4.7.4](#). Operational and Interoperability Impact if Blocked**

Discarding packets containing this EH would break Mobile IPv6.

##### **[3.4.7.5](#). Advice**

Intermediate systems should permit packets containing this EH.

#### **[3.4.8](#). Host Identity Protocol (Protocol Number=139)**

##### **[3.4.8.1](#). Uses**

This EH is employed with the Host Identity Protocol (HIP), an experimental protocol that allows consenting hosts to securely establish and maintain shared IP-layer state, allowing separation of



the identifier and locator roles of IP addresses, thereby enabling continuity of communications across IP address changes.

#### **[3.4.8.2.](#) Specification**

This EH is specified in [[RFC5201](#)].

#### **[3.4.8.3.](#) Specific Security Implications**

The security implications of the HIP header are discussed in detail in [Section 8 of \[RFC6275\]](#).

#### **[3.4.8.4.](#) Operational and Interoperability Impact if Blocked**

Discarding packets that contain the Host Identity Protocol would break HIP deployments.

#### **[3.4.8.5.](#) Advice**

Intermediate systems should permit packets that contain a Host Identity Protocol EH.

### **[3.4.9.](#) Shim6 Protocol (Protocol Number=140)**

#### **[3.4.9.1.](#) Uses**

This EH is employed by the Shim6 [[RFC5533](#)] Protocol.

#### **[3.4.9.2.](#) Specification**

This EH is specified in [[RFC5533](#)].

#### **[3.4.9.3.](#) Specific Security Implications**

The specific security implications are discussed in detail in [Section 16 of \[RFC5533\]](#).

#### **[3.4.9.4.](#) Operational and Interoperability Impact if Blocked**

Discarding packets that contain this EH will break Shim6.

#### **[3.4.9.5.](#) Advice**

Intermediate systems should permit packets containing this EH.



### **[3.4.10.](#) Use for experimentation and testing (Protocol Numbers=253 and 254)**

#### **[3.4.10.1.](#) Uses**

These IPv6 EHs are employed for performing [RFC3692](#)-Style experiments (see [[RFC3692](#)] for details).

#### **[3.4.10.2.](#) Specification**

These EHs are specified in [[RFC3692](#)] and [[RFC4727](#)].

#### **[3.4.10.3.](#) Specific Security Implications**

The security implications of these EHs will depend on their specific use.

#### **[3.4.10.4.](#) Operational and Interoperability Impact if Blocked**

For obvious reasons, discarding packets that contain these EHs limits the ability to perform legitimate experiments across IPv6 routers.

#### **[3.4.10.5.](#) Advice**

Operators should determine according to their own circumstances whether to discard packets containing these EHs.

### **[3.5.](#) Advice on the Handling of Packets with Unknown IPv6 Extension Headers**

We refer to IPv6 EHs that have not been assigned an Internet Protocol Number by IANA (and marked as such) in [[IANA-PROTOCOLS](#)] as "unknown IPv6 extension headers" ("unknown IPv6 EHs").

#### **[3.5.1.](#) Uses**

New IPv6 EHs may be specified as part of future extensions to the IPv6 protocol.

Since IPv6 EHs and Upper-layer protocols employ the same namespace, it is impossible to tell whether an unknown "Internet Protocol Number" is being employed for an IPv6 EH or an Upper-Layer protocol.

#### **[3.5.2.](#) Specification**

The processing of unknown IPv6 EHs is specified in [[RFC7045](#)].



### **3.5.3. Specific Security Implications**

For obvious reasons, it is impossible to determine specific security implications of unknown IPv6 EHs.

### **3.5.4. Operational and Interoperability Impact if Blocked**

As noted in [[RFC7045](#)], discarding unknown IPv6 EHs may slow down the deployment of new IPv6 EHs and transport protocols. The corresponding IANA registry ([[IANA-PROTOCOLS](#)]) should be monitored such that filtering rules are updated as new IPv6 EHs are standardized.

We note that since IPv6 EHs and upper-layer protocols share the same numbering space, discarding unknown IPv6 EHs may result in packets encapsulating unknown upper-layer protocols being discarded.

### **3.5.5. Advice**

Operators should determine according to their own circumstances whether to discard packets containing unknown IPv6 EHs.

## **4. IPv6 Options**

### **4.1. General Discussion**

The following subsections describe specific security implications of different IPv6 options, and provide advice regarding filtering packets that contain such options.

### **4.2. General Security Implications of IPv6 Options**

The general security implications of IPv6 options are closely related to those discussed in [Section 3.2](#) for IPv6 EHs. Essentially, packets that contain IPv6 options might need to be processed by an IPv6 router's general-purpose CPU, and hence could present a DDoS risk to that router's general-purpose CPU (and thus to the router itself). For some architectures, a possible mitigation would be to rate-limit the packets that are to be processed by the general-purpose CPU (see e.g. [[Cisco-EH](#)]).

### **4.3. Advice on the Handling of Packets with Specific IPv6 Options**

The following subsections contain a description of each of the IPv6 options that have so far been specified, a summary of the security implications of each of such options, a discussion of possible interoperability implications if packets containing such options are



discarded, and specific advice regarding whether packets containing these options should be permitted.

#### **[4.3.1.](#) Pad1 (Type=0x00)**

##### **[4.3.1.1.](#) Uses**

This option is used when necessary to align subsequent options and to pad out the containing header to a multiple of 8 octets in length.

##### **[4.3.1.2.](#) Specification**

This option is specified in [[RFC8200](#)].

##### **[4.3.1.3.](#) Specific Security Implications**

None.

##### **[4.3.1.4.](#) Operational and Interoperability Impact if Blocked**

Discarding packets that contain this option would potentially break any protocol that relies on IPv6 options.

##### **[4.3.1.5.](#) Advice**

Intermediate systems should not discard packets based on the presence of this option.

#### **[4.3.2.](#) PadN (Type=0x01)**

##### **[4.3.2.1.](#) Uses**

This option is used when necessary to align subsequent options and to pad out the containing header to a multiple of 8 octets in length.

##### **[4.3.2.2.](#) Specification**

This option is specified in [[RFC8200](#)].

##### **[4.3.2.3.](#) Specific Security Implications**

Because of the possible size of this option, it could be leveraged as a large-bandwidth covert channel.



#### **4.3.2.4. Operational and Interoperability Impact if Blocked**

Discarding packets that contain this option would potentially break any protocol that relies on IPv6 options.

#### **4.3.2.5. Advice**

Intermediate systems should not discard IPv6 packets based on the presence of this option.

### **4.3.3. Jumbo Payload (Type=0XC2)**

#### **4.3.3.1. Uses**

The Jumbo payload option provides the means of specifying payloads larger than 65535 bytes.

#### **4.3.3.2. Specification**

This option is specified in [[RFC2675](#)].

#### **4.3.3.3. Specific Security Implications**

There are no specific issues arising from this option, except for improper validity checks of the option and associated packet lengths.

#### **4.3.3.4. Operational and Interoperability Impact if Blocked**

Discarding packets based on the presence of this option will cause IPv6 jumbograms to be discarded.

#### **4.3.3.5. Advice**

Intermediate systems should discard packets that contain this option. An operator should permit this option only in specific scenarios in which support for IPv6 jumbograms is desired.

### **4.3.4. RPL Option (Type=0x63)**

#### **4.3.4.1. Uses**

The RPL Option provides a mechanism to include routing information with each datagram that an RPL router forwards.



#### **4.3.4.2. Specification**

This option was originally specified in [[RFC6553](#)]. It has been deprecated by [[I-D.ietf-roll-useofrplinfo](#)].

#### **4.3.4.3. Specific Security Implications**

Those described in [[RFC6553](#)].

#### **4.3.4.4. Operational and Interoperability Impact if Blocked**

This option is meant to be employed within an RPL instance. As a result, discarding packets based on the presence of this option (e.g. at an ISP) will not result in interoperability implications.

#### **4.3.4.5. Advice**

Non-RPL routers should discard packets that contain an RPL option.

### **4.3.5. RPL Option (Type=0x23)**

#### **4.3.5.1. Uses**

The RPL Option provides a mechanism to include routing information with each datagram that an RPL router forwards.

#### **4.3.5.2. Specification**

This option is specified in [[I-D.ietf-roll-useofrplinfo](#)].

#### **4.3.5.3. Specific Security Implications**

Those described in [[I-D.ietf-roll-useofrplinfo](#)].

#### **4.3.5.4. Operational and Interoperability Impact if Blocked**

This option is meant to survive outside of an RPL instance. As a result, discarding packets based on the presence of this option would break some use cases for RPL (see [[I-D.ietf-roll-useofrplinfo](#)]).

#### **4.3.5.5. Advice**

Intermediate systems should not discard IPv6 packets based on the presence of this option.



#### **4.3.6. Tunnel Encapsulation Limit (Type=0x04)**

##### **4.3.6.1. Uses**

The Tunnel Encapsulation Limit option can be employed to specify how many further levels of nesting the packet is permitted to undergo.

##### **4.3.6.2. Specification**

This option is specified in [[RFC2473](#)].

##### **4.3.6.3. Specific Security Implications**

Those described in [[RFC2473](#)].

##### **4.3.6.4. Operational and Interoperability Impact if Blocked**

Discarding packets based on the presence of this option could result in tunnel traffic being discarded.

##### **4.3.6.5. Advice**

Intermediate systems should not discard packets based on the presence of this option.

#### **4.3.7. Router Alert (Type=0x05)**

##### **4.3.7.1. Uses**

The Router Alert option [[RFC2711](#)] is typically employed for the RSVP protocol [[RFC2205](#)] and the MLD protocol [[RFC2710](#)].

##### **4.3.7.2. Specification**

This option is specified in [[RFC2711](#)].

##### **4.3.7.3. Specific Security Implications**

Since this option causes the contents of the packet to be inspected by the handling device, this option could be leveraged for performing DoS attacks.

##### **4.3.7.4. Operational and Interoperability Impact if Blocked**

Discarding packets that contain this option would break RSVP and multicast deployments.



#### **4.3.7.5. Advice**

Packets containing this option should be permitted in environments where support for RSVP, multicast routing, or similar protocols is desired.

#### **4.3.8. Quick-Start (Type=0x26)**

##### **4.3.8.1. Uses**

This IP Option is used in the specification of Quick-Start for TCP and IP, which is an experimental mechanism that allows transport protocols, in cooperation with routers, to determine an allowed sending rate at the start and, at times, in the middle of a data transfer (e.g., after an idle period) [[RFC4782](#)].

##### **4.3.8.2. Specification**

This option is specified in [[RFC4782](#)], on the "Experimental" track.

##### **4.3.8.3. Specific Security Implications**

[Section 9.6 of \[RFC4782\]](#) notes that Quick-Start is vulnerable to two kinds of attacks:

- o attacks to increase the routers' processing and state load, and,
- o attacks with bogus Quick-Start Requests to temporarily tie up available Quick-Start bandwidth, preventing routers from approving Quick-Start Requests from other connections.

We note that if routers in a given environment do not implement and enable the Quick-Start mechanism, only the general security implications of IP options (discussed in [Section 4.2](#)) would apply.

##### **4.3.8.4. Operational and Interoperability Impact if Blocked**

The Quick-Start functionality would be disabled, and additional delays in TCP's connection establishment (for example) could be introduced. (Please see [Section 4.7.2 of \[RFC4782\]](#).) We note, however, that Quick-Start has been proposed as a mechanism that could be of use in controlled environments, and not as a mechanism that would be intended or appropriate for ubiquitous deployment in the global Internet [[RFC4782](#)].



#### **4.3.8.5. Advice**

Intermediate systems should not discard IPv6 packets based on the presence of this option.

#### **4.3.9. CALIPSO (Type=0x07)**

##### **4.3.9.1. Uses**

This option is used for encoding explicit packet Sensitivity Labels on IPv6 packets. It is intended for use only within Multi-Level Secure (MLS) networking environments that are both trusted and trustworthy.

##### **4.3.9.2. Specification**

This option is specified in [[RFC5570](#)].

##### **4.3.9.3. Specific Security Implications**

Presence of this option in a packet does not by itself create any specific new threat. Packets with this option ought not normally be seen on the global public Internet.

##### **4.3.9.4. Operational and Interoperability Impact if Blocked**

If packets with this option are discarded or if the option is stripped from the packet during transmission from source to destination, then the packet itself is likely to be discarded by the receiver because it is not properly labeled. In some cases, the receiver might receive the packet but associate an incorrect sensitivity label with the received data from the packet whose CALIPSO was stripped by an intermediate router or firewall. Associating an incorrect sensitivity label can cause the received information either to be handled as more sensitive than it really is ("upgrading") or as less sensitive than it really is ("downgrading"), either of which is problematic.

##### **4.3.9.5. Advice**

Recommendations for handling the CALIPSO option depend on the deployment environment, rather than whether an intermediate system happens to be deployed as a transit device (e.g., IPv6 transit router).

Explicit configuration is the only method via which an intermediate system can know whether or not that particular intermediate system has been deployed within a Multi-Level Secure (MLS) environment. In



many cases, ordinary commercial intermediate systems (e.g., IPv6 routers and firewalls) are the majority of the deployed intermediate systems inside an MLS network environment.

For Intermediate systems that DO NOT implement [RFC-5570](#), there should be a configuration option to EITHER (a) drop packets containing the CALIPSO option OR (b) to ignore the presence of the CALIPSO option and forward the packets normally. In non-MLS environments, such intermediate systems should have this configuration option set to (a) above. In MLS environments, such intermediate systems should have this option set to (b) above. The default setting for this configuration option should be set to (a) above, because MLS environments are much less common than non-MLS environments.

For Intermediate systems that DO implement [RFC-5570](#), there should be configuration options (a) and (b) from the preceding paragraph and also a third configuration option (c) to process packets containing a CALIPSO option as per [RFC-5570](#). When deployed in non-MLS environments, such intermediate systems should have this configuration option set to (a) above. When deployed in MLS environments, such intermediate systems should have this set to (c). The default setting for this configuration option MAY be set to (a) above, because MLS environments are much less common than non-MLS environments.

#### [4.3.10.](#) SMF\_DPD (Type=0x08)

##### [4.3.10.1.](#) Uses

This option is employed in the (experimental) Simplified Multicast Forwarding (SMF) for unique packet identification for IPv6 I-DPD, and as a mechanism to guarantee non-collision of hash values for different packets when H-DPD is used.

##### [4.3.10.2.](#) Specification

This option is specified in [[RFC6621](#)].

##### [4.3.10.3.](#) Specific Security Implications

None. The use of transient numeric identifiers is subject to the security and privacy considerations discussed in [[I-D.irtf-pearq-numeric-ids-generation](#)].



#### **4.3.10.4. Operational and Interoperability Impact if Blocked**

Dropping packets containing this option within a MANET domain would break SMF. However, dropping such packets at the border of such domain would have no negative impact.

#### **4.3.10.5. Advice**

Intermediate systems that are not within a MANET domain should discard packets that contain this option.

#### **4.3.11. Home Address (Type=0xC9)**

##### **4.3.11.1. Uses**

The Home Address option is used by a Mobile IPv6 node while away from home, to inform the recipient of the mobile node's home address.

##### **4.3.11.2. Specification**

This option is specified in [[RFC6275](#)].

##### **4.3.11.3. Specific Security Implications**

No (known) additional security implications than those described in [[RFC6275](#)].

##### **4.3.11.4. Operational and Interoperability Impact if Blocked**

Discarding IPv6 packets based on the presence of this option will break Mobile IPv6.

##### **4.3.11.5. Advice**

Intermediate systems should not discard IPv6 packets based on the presence of this option.

#### **4.3.12. Endpoint Identification (Type=0x8A)**

##### **4.3.12.1. Uses**

The Endpoint Identification option was meant to be used with the Nimrod routing architecture [[NIMROD-DOC](#)], but has never seen widespread deployment.



#### [4.3.12.2.](#) **Specification**

This option is specified in [[NIMROD-DOC](#)].

#### [4.3.12.3.](#) **Specific Security Implications**

Undetermined.

#### [4.3.12.4.](#) **Operational and Interoperability Impact if Blocked**

None.

#### [4.3.12.5.](#) **Advice**

Intermediate systems should discard packets that contain this option.

### [4.3.13.](#) **ILNP Nonce (Type=0x8B)**

#### [4.3.13.1.](#) **Uses**

This option is employed by Identifier-Locator Network Protocol for IPv6 (ILNPv6) for providing protection against off-path attacks for packets when ILNPv6 is in use, and as a signal during initial network-layer session creation that ILNPv6 is proposed for use with this network-layer session, rather than classic IPv6.

#### [4.3.13.2.](#) **Specification**

This option is specified in [[RFC6744](#)].

#### [4.3.13.3.](#) **Specific Security Implications**

Those described in [[RFC6744](#)].

#### [4.3.13.4.](#) **Operational and Interoperability Impact if Blocked**

Discarding packets that contain this option will break ILNPv6 deployments.

#### [4.3.13.5.](#) **Advice**

Intermediate systems should not discard packets based on the presence of this option.



#### **4.3.14. Line-Identification Option (Type=0x8C)**

##### **4.3.14.1. Uses**

This option is used by an Edge Router to identify the subscriber premises in scenarios where several subscriber premises may be logically connected to the same interface of an Edge Router.

##### **4.3.14.2. Specification**

This option is specified in [[RFC6788](#)].

##### **4.3.14.3. Specific Security Implications**

Those described in [[RFC6788](#)].

##### **4.3.14.4. Operational and Interoperability Impact if Blocked**

Since this option is meant to be employed in Router Solicitation messages, discarding packets based on the presence of this option at intermediate systems will result in no interoperability implications.

##### **4.3.14.5. Advice**

Intermediate devices should discard packets that contain this option.

#### **4.3.15. Deprecated (Type=0x4D)**

##### **4.3.15.1. Uses**

No information has been found about this option type.

##### **4.3.15.2. Specification**

No information has been found about this option type.

##### **4.3.15.3. Specific Security Implications**

No information has been found about this option type, and hence it has been impossible to perform the corresponding security assessment.

##### **4.3.15.4. Operational and Interoperability Impact if Blocked**

Unknown.



#### **[4.3.15.5.](#) Advice**

Intermediate systems should discard packets that contain this option.

#### **[4.3.16.](#) MPL Option (Type=0x6D)**

##### **[4.3.16.1.](#) Uses**

This option is used with the Multicast Protocol for Low power and Lossy Networks (MPL), that provides IPv6 multicast forwarding in constrained networks.

##### **[4.3.16.2.](#) Specification**

This option is specified in [[RFC7731](#)], and is meant to be included only in Hop-by-Hop Option headers.

##### **[4.3.16.3.](#) Specific Security Implications**

Those described in [[RFC7731](#)].

##### **[4.3.16.4.](#) Operational and Interoperability Impact if Blocked**

Dropping packets that contain an MPL option within an MPL network would break the Multicast Protocol for Low power and Lossy Networks (MPL). However, dropping such packets at the border of such networks will have no negative impact.

##### **[4.3.16.5.](#) Advice**

Intermediate systems should not discard packets based on the presence of this option. However, since this option has been specified for the Hop-by-Hop Options, such systems should consider the discussion in [Section 3.4.1](#).

#### **[4.3.17.](#) IP\_DFF (Type=0xEE)**

##### **[4.3.17.1.](#) Uses**

This option is employed with the (Experimental) Depth-First Forwarding (DFF) in Unreliable Networks.

##### **[4.3.17.2.](#) Specification**

This option is specified in [[RFC6971](#)].



#### **[4.3.17.3.](#) Specific Security Implications**

Those specified in [[RFC6971](#)].

#### **[4.3.17.4.](#) Operational and Interoperability Impact if Blocked**

Dropping packets containing this option within a routing domain that is running DFF would break DFF. However, dropping such packets at the border of such domains will have no security implications.

#### **[4.3.17.5.](#) Advice**

Intermediate systems that do not operate within a routing domain that is running DFF should discard packets containing this option.

#### **[4.3.18.](#) [RFC3692](#)-style Experiment (Types = 0x1E, 0x3E, 0x5E, 0x7E, 0x9E, 0xBE, 0xDE, 0xFE)**

##### **[4.3.18.1.](#) Uses**

These options can be employed for performing [RFC3692](#)-style experiments. It is only appropriate to use these values in explicitly configured experiments; they must not be shipped as defaults in implementations.

##### **[4.3.18.2.](#) Specification**

Specified in [RFC 4727](#) [[RFC4727](#)] in the context of [RFC3692](#)-style experiments.

##### **[4.3.18.3.](#) Specific Security Implications**

The specific security implications will depend on the specific use of these options.

##### **[4.3.18.4.](#) Operational and Interoperability Impact if Blocked**

For obvious reasons, discarding packets that contain these options limits the ability to perform legitimate experiments across IPv6 routers.

##### **[4.3.18.5.](#) Advice**

Operators should determine according to their own circumstances whether to discard packets containing these IPv6 options.



#### **4.4. Advice on the handling of Packets with Unknown IPv6 Options**

We refer to IPv6 options that have not been assigned an IPv6 option type in the corresponding registry ([[IANA-IPV6-PARAM](#)]) as "unknown IPv6 options".

##### **4.4.1. Uses**

New IPv6 options may be specified as part of future protocol work.

##### **4.4.2. Specification**

The processing of unknown IPv6 options is specified in [[RFC8200](#)].

##### **4.4.3. Specific Security Implications**

For obvious reasons, it is impossible to determine specific security implications of unknown IPv6 options.

##### **4.4.4. Operational and Interoperability Impact if Blocked**

Discarding unknown IPv6 options may slow down the deployment of new IPv6 options. As noted in [[draft-gont-6man-ipv6-opt-transmit](#)], the corresponding IANA registry ([[IANA-IPV6-PARAM](#)]) should be monitored such that IPv6 option filtering rules are updated as new IPv6 options are standardized.

##### **4.4.5. Advice**

Operators should determine according to their own circumstances whether to discard packets containing unknown IPv6 options.

#### **5. IANA Considerations**

This document has no actions for IANA.

#### **6. Privacy Considerations**

There are no privacy considerations associated with this document.

#### **7. Security Considerations**

This document provides advice on the filtering of IPv6 packets that contain IPV6 EHs (and possibly IPv6 options) at IPv6 transit routers. It is meant to improve the current situation of widespread dropping of such IPv6 packets in those cases where the drops result from improper configuration defaults, or inappropriate advice in this area.



## **8. Acknowledgements**

The authors would like to thank Ron Bonica for his work on earlier versions of this document.

The authors of this document would like to thank (in alphabetical order) Mikael Abrahamsson, Brian Carpenter, Darren Dukes, David Farmer, Mike Heard, Bob Hinden, Christian Huitema, Jen Linkova, Carlos Pignataro, Maria Ines Robles, Donald Smith, Pascal Thubert, Ole Troan, Gunter Van De Velde, and Eric Vyncke, for providing valuable comments on earlier versions of this document.

This document borrows some text and analysis from [[RFC7126](#)], authored by Fernando Gont, Randall Atkinson, and Carlos Pignataro.

The authors would like to thank Eric Vyncke for his guidance during the publication process of this document.

Fernando would also like to thank Brian Carpenter and Ran Atkinson who, over the years, have answered many questions and provided valuable comments that have benefited his protocol-related work (including the present document).

## **9. References**

### **9.1. Normative References**

- [I-D.ietf-roll-useofrplinfo]  
Robles, I., Richardson, M., and P. Thubert, "Using RPI Option Type, Routing Header for Source Routes and IPv6-in-IPv6 encapsulation in the RPL Data Plane", [draft-ietf-roll-useofrplinfo-44](#) (work in progress), January 2021.
- [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), DOI 10.17487/RFC1034, November 1987, <<https://www.rfc-editor.org/info/rfc1034>>.
- [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>>.
- [RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", [RFC 2205](#), DOI 10.17487/RFC2205, September 1997, <<https://www.rfc-editor.org/info/rfc2205>>.



- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), DOI 10.17487/RFC2460, December 1998, <<https://www.rfc-editor.org/info/rfc2460>>.
- [RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", [RFC 2473](#), DOI 10.17487/RFC2473, December 1998, <<https://www.rfc-editor.org/info/rfc2473>>.
- [RFC2675] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", [RFC 2675](#), DOI 10.17487/RFC2675, August 1999, <<https://www.rfc-editor.org/info/rfc2675>>.
- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", [RFC 2710](#), DOI 10.17487/RFC2710, October 1999, <<https://www.rfc-editor.org/info/rfc2710>>.
- [RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", [RFC 2711](#), DOI 10.17487/RFC2711, October 1999, <<https://www.rfc-editor.org/info/rfc2711>>.
- [RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", [BCP 82](#), [RFC 3692](#), DOI 10.17487/RFC3692, January 2004, <<https://www.rfc-editor.org/info/rfc3692>>.
- [RFC4302] Kent, S., "IP Authentication Header", [RFC 4302](#), DOI 10.17487/RFC4302, December 2005, <<https://www.rfc-editor.org/info/rfc4302>>.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", [RFC 4303](#), DOI 10.17487/RFC4303, December 2005, <<https://www.rfc-editor.org/info/rfc4303>>.
- [RFC4727] Fenner, B., "Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", [RFC 4727](#), DOI 10.17487/RFC4727, November 2006, <<https://www.rfc-editor.org/info/rfc4727>>.
- [RFC4782] Floyd, S., Allman, M., Jain, A., and P. Sarolahti, "Quick-Start for TCP and IP", [RFC 4782](#), DOI 10.17487/RFC4782, January 2007, <<https://www.rfc-editor.org/info/rfc4782>>.
- [RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", [RFC 5095](#), DOI 10.17487/RFC5095, December 2007, <<https://www.rfc-editor.org/info/rfc5095>>.



- [RFC5201] Moskowitz, R., Nikander, P., Jokela, P., Ed., and T. Henderson, "Host Identity Protocol", [RFC 5201](#), DOI 10.17487/RFC5201, April 2008, <<https://www.rfc-editor.org/info/rfc5201>>.
- [RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", [RFC 5533](#), DOI 10.17487/RFC5533, June 2009, <<https://www.rfc-editor.org/info/rfc5533>>.
- [RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", [RFC 5570](#), DOI 10.17487/RFC5570, July 2009, <<https://www.rfc-editor.org/info/rfc5570>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", [RFC 6275](#), DOI 10.17487/RFC6275, July 2011, <<https://www.rfc-editor.org/info/rfc6275>>.
- [RFC6398] Le Faucheur, F., Ed., "IP Router Alert Considerations and Usage", [BCP 168](#), [RFC 6398](#), DOI 10.17487/RFC6398, October 2011, <<https://www.rfc-editor.org/info/rfc6398>>.
- [RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", [RFC 6550](#), DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.
- [RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", [RFC 6553](#), DOI 10.17487/RFC6553, March 2012, <<https://www.rfc-editor.org/info/rfc6553>>.
- [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](#), DOI 10.17487/RFC6554, March 2012, <<https://www.rfc-editor.org/info/rfc6554>>.
- [RFC6621] Macker, J., Ed., "Simplified Multicast Forwarding", [RFC 6621](#), DOI 10.17487/RFC6621, May 2012, <<https://www.rfc-editor.org/info/rfc6621>>.



- [RFC6740] Atkinson, RJ. and SN. Bhatti, "Identifier-Locator Network Protocol (ILNP) Architectural Description", [RFC 6740](#), DOI 10.17487/RFC6740, November 2012, <<https://www.rfc-editor.org/info/rfc6740>>.
- [RFC6744] Atkinson, RJ. and SN. Bhatti, "IPv6 Nonce Destination Option for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)", [RFC 6744](#), DOI 10.17487/RFC6744, November 2012, <<https://www.rfc-editor.org/info/rfc6744>>.
- [RFC6788] Krishnan, S., Kavanagh, A., Varga, B., Ooghe, S., and E. Nordmark, "The Line-Identification Option", [RFC 6788](#), DOI 10.17487/RFC6788, November 2012, <<https://www.rfc-editor.org/info/rfc6788>>.
- [RFC6971] Herberg, U., Ed., Cardenas, A., Iwao, T., Dow, M., and S. Cespedes, "Depth-First Forwarding (DFF) in Unreliable Networks", [RFC 6971](#), DOI 10.17487/RFC6971, June 2013, <<https://www.rfc-editor.org/info/rfc6971>>.
- [RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", [RFC 7045](#), DOI 10.17487/RFC7045, December 2013, <<https://www.rfc-editor.org/info/rfc7045>>.
- [RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", [RFC 7112](#), DOI 10.17487/RFC7112, January 2014, <<https://www.rfc-editor.org/info/rfc7112>>.
- [RFC7731] Hui, J. and R. Kelsey, "Multicast Protocol for Low-Power and Lossy Networks (MPL)", [RFC 7731](#), DOI 10.17487/RFC7731, February 2016, <<https://www.rfc-editor.org/info/rfc7731>>.
- [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>>.
- [RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", [RFC 8754](#), DOI 10.17487/RFC8754, March 2020, <<https://www.rfc-editor.org/info/rfc8754>>.



[RFC8900] Bonica, R., Baker, F., Huston, G., Hinden, R., Troan, O., and F. Gont, "IP Fragmentation Considered Fragile", [BCP 230](#), [RFC 8900](#), DOI 10.17487/RFC8900, September 2020, <<https://www.rfc-editor.org/info/rfc8900>>.

## 9.2. Informative References

[Biondi2007]

Biondi, P. and A. Ebalard, "IPv6 Routing Header Security", CanSecWest 2007 Security Conference, 2007, <[http://www.secdev.org/conf/IPv6\\_RH\\_security-csw07.pdf](http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf)>.

[Cisco-EH]

Cisco Systems, "IPv6 Extension Headers Review and Considerations", Whitepaper. October 2006, <[http://www.cisco.com/en/US/technologies/tk648/tk872/technologies\\_white\\_paper0900aecd8054d37d.pdf](http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.pdf)>.

[[draft-gont-6man-ipv6-opt-transmit](#)]

Gont, F., Liu, W., and R. Bonica, "Transmission and Processing of IPv6 Options", IETF Internet Draft, work in progress, August 2014.

[[draft-ietf-nimrod-eid](#)]

Lynn, C., "Endpoint Identifier Destination Option", IETF Internet Draft, [draft-ietf-nimrod-eid-00.txt](#), November 1995.

[FW-Benchmark]

Zack, E., "Firewall Security Assessment and Benchmarking IPv6 Firewall Load Tests", IPv6 Hackers Meeting #1, Berlin, Germany. June 30, 2013, <<http://www.ipv6hackers.org/meetings/ipv6-hackers-1/zack-ipv6hackers1-firewall-security-assessment-and-benchmarking.pdf>>.

[I-D.ietf-6man-hbh-header-handling]

Baker, F. and R. Bonica, "IPv6 Hop-by-Hop Options Extension Header", [draft-ietf-6man-hbh-header-handling-03](#) (work in progress), March 2016.

[I-D.ietf-v6ops-ipv6-ehs-packet-drops]

Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. LIU, "Operational Implications of IPv6 Packets with Extension Headers", [draft-ietf-v6ops-ipv6-ehs-packet-drops-03](#) (work in progress), January 2021.



[I-D.irtf-pearg-numeric-ids-generation]

Gont, F. and I. Arce, "On the Generation of Transient Numeric Identifiers", [draft-irtf-pearg-numeric-ids-generation-06](#) (work in progress), January 2021.

[IANA-IPV6-PARAM]

Internet Assigned Numbers Authority, "Internet Protocol Version 6 (IPv6) Parameters", December 2013, <<http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml>>.

[IANA-PROTOCOLS]

Internet Assigned Numbers Authority, "Protocol Numbers", 2014, <<http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>>.

[NIMROD-DOC]

Nimrod Documentation Page,  
"http://ana-3.lcs.mit.edu/~jnc/nimrod/".

[RFC3871] Jones, G., Ed., "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", [RFC 3871](#), DOI 10.17487/RFC3871, September 2004, <<https://www.rfc-editor.org/info/rfc3871>>.

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", [RFC 6192](#), DOI 10.17487/RFC6192, March 2011, <<https://www.rfc-editor.org/info/rfc6192>>.

[RFC7126] Gont, F., Atkinson, R., and C. Pignataro, "Recommendations on Filtering of IPv4 Packets Containing IPv4 Options", [BCP 186](#), [RFC 7126](#), DOI 10.17487/RFC7126, February 2014, <<https://www.rfc-editor.org/info/rfc7126>>.

[RFC7739] Gont, F., "Security Implications of Predictable Fragment Identification Values", [RFC 7739](#), DOI 10.17487/RFC7739, February 2016, <<https://www.rfc-editor.org/info/rfc7739>>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", [RFC 7872](#), DOI 10.17487/RFC7872, June 2016, <<https://www.rfc-editor.org/info/rfc7872>>.



Authors' Addresses

Fernando Gont  
SI6 Networks  
Seguro y Habana 4310, 7mo Piso  
Villa Devoto, Ciudad Autonoma de Buenos Aires  
Argentina

Email: fgont@si6networks.com

URI: <https://www.si6networks.com>

Will(Shucheng) Liu  
Huawei Technologies  
Bantian, Longgang District  
Shenzhen 518129  
P.R. China

Email: liushucheng@huawei.com

