Internet Engineering Task Force (IETF)
Request for Comments: 9288
Category: Informational
ISSN: 2070-1721

F. Gont
SI6 Networks
W. Liu
Huawei Technologies

August 2022

Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers at Transit Routers

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 document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9288.

Table of Contents

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, as an example, enforcing Access Control Lists (ACLs) or implementing other functions [RFC9098].

Several studies (e.g., [Huston-2022], [JAMES], and [RFC7872]) suggest that there is widespread dropping of IPv6 packets that contain IPv6 EHs. In some cases, such packet drops occur at transit routers. While some operators are known to intentionally drop packets that contain IPv6 EHs, it is possible that some of the measured packet drops are the result of 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 IPv6 EHs and IPv6 options a packet may contain, following a "deny-list" approach; hence, it is likely to be much more permissive than a filtering policy to be employed at, for example, 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 that 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 specifies the terminology and conventions employed throughout this document. Section 3 discusses IPv6 EHs and provides advice in the area of filtering IPv6 packets that contain such IPv6 EHs. Section 4 discusses IPv6 options and provides advice in the area of filtering IPv6 packets that contain such options.

2. Terminology and Assumptions Employed 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 a drop and 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. Router Default Behavior and Features

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

> | 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.

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 policies but does not change the implementation defaults required by [RFC7045].

We recommend that configuration options be 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:

* Permit this IPv6 EH or IPv6 Option Type.

* Drop packets containing this IPv6 EH or IPv6 Option Type.

* Reject packets containing this IPv6 EH or IPv6 Option Type (where the packet drop is signaled with an ICMPv6 error message).

* Rate-limit traffic containing this IPv6 EH or IPv6 Option Type.

* Ignore this IPv6 EH or IPv6 Option Type (as if it was not present), and process the packet according the rules for the remaining headers. We note that if a packet carries forwarding information (e.g., in an IPv6 Routing Header (RH)), 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 EHs [RFC8200] 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.

[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 include the entire IPv6 header chain [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 [RFC9098] [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 the future.

3.3. Rationale for Our Advice on the Handling of IPv6 Packets with

Specific IPv6 Extension Headers

* IPv6 packets with IPv6 Extension Headers (or options) that are not expected to traverse transit routers should be dropped.

* IPv6 packets with IPv6 Extension Headers (or options) that are only expected to traverse transit routers when a specific technology is employed should be permitted (or dropped) based on the knowledge regarding the use of such technology in the transit provider in question (i.e., permit the packets if the technology is employed, or drop them).

* IPv6 packets with IPv6 Extension Headers (or options) that represent a concrete attack vector to network infrastructure devices should be dropped.

* IPv6 packets with any other IPv6 Extension Headers (or options) should be permitted. This is an intentional trade-off made to minimize ossification.

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

This section summarizes the advice provided in Section 3.5, providing references to the specific sections in which a detailed analysis can be found.

EH Type	Filtering Policy	Reference
Hop-by-Hop Options Header (Proto=0)	Drop or Ignore	Section 3.5.1
Routing Header (Proto=43)	Drop only Routing Type 0, Routing Type 1, and Routing Type 3. Permit other Routing Types	Section 3.5.2
Fragment Header (Proto=44)	Permit	Section 3.5.3
Encapsulating Security Payload (Proto=50)	Permit	Section 3.5.4
Authentication Header (Proto=51)	Permit	Section 3.5.5
Destination Options Header(Proto=60)	Permit	Section 3.5.6
Mobility Header (Proto=135)	Permit	Section 3.5.7
Host Identity Protocol (Proto=139)	Permit	Section 3.5.8
Shim6 Protocol (Proto=140)	Permit	Section 3.5.9
Use for experimentation and testing (Proto=253 and 254)	Drop	Section 3.5.10

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

3.5. Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers

3.5.1. IPv6 Hop-by-Hop Options (Protocol Number=0)

3.5.1.1. Uses

The Hop-by-Hop (HBH) 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 all nodes to examine and process 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.

3.5.1.2. Specification

This EH is specified in [RFC8200]. As of May 2022, the following options have been specified for the Hop-by-Hop Options header:

* Type 0x00: Pad1 [RFC8200]
* Type 0x01: PadN [RFC8200]
* Type 0x05: Router Alert [RFC2711]
* Type 0x07: CALIPSO [RFC5570]
* Type 0x08: SMF_DPD [RFC6621]
* Type 0x23: RPL Option [RFC9008]
* Type 0x26: Quick-Start [RFC4782]
* Type 0x4D: (Deprecated)
* Type 0x63: RPL Option [RFC6553]
* Type 0x6D: MPL Option [RFC7731]
* Type 0x8A: Endpoint Identification (Deprecated) [NIMROD-EID]
* Type 0xC2: Jumbo Payload [RFC2675]
* Type 0xEE: IPv6 DFF Header [RFC6971]
* Type 0x1E: RFC3692-style Experiment [RFC4727]
* Type 0x3E: RFC3692-style Experiment [RFC4727]
* Type 0x5E: RFC3692-style Experiment [RFC4727]
* Type 0x7E: RFC3692-style Experiment [RFC4727]
* Type 0x9E: RFC3692-style Experiment [RFC4727]
* Type 0xBE: RFC3692-style Experiment [RFC4727]

* Type 0xDE: RFC3692-style Experiment [RFC4727]

* Type 0xFE: RFC3692-style Experiment [RFC4727]

3.5.1.3. Specific Security Implications

Legacy nodes that process this extension header might be subject to DoS attacks.

> | NOTE: While [RFC8200] has removed the requirement for all nodes to examine and process the Hop-by-Hop Options header, the deployed base may still reflect the legacy [RFC2460] behavior for a while; hence, the potential security problems of this EH are still of concern.

3.5.1.4. Operational and Interoperability Impact If Blocked

Discarding packets containing a Hop-by-Hop Options header 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.

3.5.1.5. Advice

Nodes implementing [RFC8200] would already ignore this extension header unless explicitly required to process it. For legacy nodes [RFC2460], 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 the forwarding of packets with IPv6 HBH Options headers on the fast path, we recommend that packets with IPv6 HBH Options headers be forwarded as normal. Otherwise, on platforms in which the processing of packets with IPv6 HBH Options headers 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 IPv6 HBH Options headers 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 headers.

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

3.5.2. Routing Header (Protocol Number=43)

3.5.2.1. 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.

3.5.2.2. Specification

This EH is specified in [RFC8200]. The Routing Type 0 had originally been specified in [RFC2460] and was later obsoleted by [RFC5095]; thus, it was removed from [RFC8200].

As of May 2022, the following Routing Types have been specified:

* Type 0: Source Route (DEPRECATED) [RFC2460] [RFC5095]

* Type 1: Nimrod (DEPRECATED)

* Type 2: Type 2 Routing Header [RFC6275]

* Type 3: RPL Source Route Header [RFC6554]

* Type 4: Segment Routing Header (SRH) [RFC8754]

* Types 5-252: Unassigned

* Type 253: RFC3692-style Experiment 1 [RFC4727]

* Type 254: RFC3692-style Experiment 2 [RFC4727]

* Type 255: Reserved

3.5.2.3. Specific Security Implications

The security implications of Routing Headers of Routing Type 0 have been discussed in detail in [Biondi-2007] and [RFC5095]. Routing Type 1 was never widely implemented. The security implications of Routing Headers of Routing Type 2, Routing Type 3, and Routing Type 4 (SRH) are discussed in [RFC6275], [RFC6554], and [RFC8754], respectively.

3.5.2.4. Operational and Interoperability Impact If Blocked

Blocking packets containing Routing Headers of Routing Type 0 or Routing Type 1 has no operational implications, since both have been deprecated. Blocking packets containing Routing Headers of Routing Type 2 would break Mobile IPv6. Packets containing Routing Headers of Routing Type 3 may be safely blocked at RPL domain boundaries, since such headers are employed within a single RPL domain. Blocking packets containing Routing Headers of Routing Type 4 (SRH) will break Segment Routing (SR) deployments if the filtering policy is enforced on packets being forwarded within an SR domain.

3.5.2.5. Advice

Intermediate systems should discard packets containing Routing Headers of Routing Type 0, Routing Type 1, or Routing Type 3. Other Routing Types should be permitted, as required by [RFC7045].

3.5.3. Fragment Header (Protocol Number=44)

3.5.3.1. Uses

This EH provides the fragmentation and reassembly functionality for IPv6.

3.5.3.2. Specification

This EH is specified in [RFC8200].

3.5.3.3. Specific Security Implications

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

3.5.3.4. 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].

3.5.3.5. Advice

Intermediate systems should permit packets that contain a Fragment Header.

3.5.4. Encapsulating Security Payload (Protocol Number=50)

3.5.4.1. Uses

This EH is employed for the IPsec suite [RFC4303].

3.5.4.2. Specification

This EH is specified in [RFC4303].

3.5.4.3. 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.

3.5.4.4. Operational and Interoperability Impact If Blocked

Discarding packets that employ this EH would break IPsec deployments.

3.5.4.5. Advice

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

3.5.5. Authentication Header (Protocol Number=51)

3.5.5.1. Uses

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

3.5.5.2. Specification

This EH is specified in [RFC4302].

3.5.5.3. 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.

3.5.5.4. Operational and Interoperability Impact If Blocked

Discarding packets that employ this EH would break IPsec deployments.

3.5.5.5. Advice

Intermediate systems should permit packets containing an Authentication Header.

3.5.6. Destination Options (Protocol Number=60)

3.5.6.1. Uses

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

3.5.6.2. Specification

This EH is specified in [RFC8200]. As of May 2022, the following options have been specified for this EH:

* Type 0x00: Pad1 [RFC8200]

* Type 0x01: PadN [RFC8200]

* Type 0x04: Tunnel Encapsulation Limit [RFC2473]

* Type 0x0F: IPv6 Performance and Diagnostic Metrics (PDM) [RFC8250]

* Type 0x4D: (Deprecated)

* Type 0xC9: Home Address [RFC6275]

* Type 0x8A: Endpoint Identification (Deprecated) [NIMROD-EID]

* Type 0x8B: ILNP Nonce [RFC6744]

* Type 0x8C: Line-Identification Option [RFC6788]

* Type 0x1E: RFC3692-style Experiment [RFC4727]

* Type 0x3E: RFC3692-style Experiment [RFC4727]

* Type 0x5E: RFC3692-style Experiment [RFC4727]

* Type 0x7E: RFC3692-style Experiment [RFC4727]

* Type 0x9E: RFC3692-style Experiment [RFC4727]

* Type 0xBE: RFC3692-style Experiment [RFC4727]

* Type 0xDE: RFC3692-style Experiment [RFC4727]

* Type 0xFE: RFC3692-style Experiment [RFC4727]

3.5.6.3. Specific Security Implications

No security implications are known, other than the general security implications of IPv6 EHs. For a discussion of possible security implications of specific options specified for the DO header, please see Section 4.4.

3.5.6.4. 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 (such as the Identifier-Locator Network Protocol (ILNP) [RFC6740] and Mobile IPv6 [RFC6275]), as well as IPv6 tunnels that employ the Tunnel Encapsulation Limit option [RFC2473].

3.5.6.5. Advice

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

3.5.7. Mobility Header (Protocol Number=135)

3.5.7.1. 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.

3.5.7.2. Specification

This EH is specified in [RFC6275].

3.5.7.3. 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].

3.5.7.4. Operational and Interoperability Impact If Blocked

Discarding packets containing this EH would break Mobile IPv6.

3.5.7.5. Advice

Intermediate systems should permit packets that contain a Mobility Header.

3.5.8. Host Identity Protocol (Protocol Number=139)

3.5.8.1. Uses

This EH is employed with the Host Identity Protocol (HIP), which is a protocol that allows consenting hosts to securely establish and maintain shared IP-layer state, allowing the separation of the identifier and locator roles of IP addresses, thereby enabling continuity of communications across IP address changes.

3.5.8.2. Specification

This EH is specified in [RFC7401].

3.5.8.3. Specific Security Implications

The security implications of the HIP header are discussed in detail in Section 8 of [RFC7401].

3.5.8.4. Operational and Interoperability Impact If Blocked

Discarding packets that contain a HIP header would break HIP deployments.

3.5.8.5. Advice

Intermediate systems should permit packets that contain a HIP header.

3.5.9. Shim6 Protocol (Protocol Number=140)

3.5.9.1. Uses

This EH is employed by the Shim6 protocol [RFC5533].

3.5.9.2. Specification

This EH is specified in [RFC5533].

3.5.9.3. Specific Security Implications

The specific security implications are discussed in detail in Section 16 of [RFC5533].

3.5.9.4. Operational and Interoperability Impact If Blocked

Discarding packets that contain this EH will break Shim6.

3.5.9.5. Advice

Intermediate systems should permit packets containing this EH.

3.5.10. Use for Experimentation and Testing (Protocol Numbers=253 and 254)

3.5.10.1. Uses

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

3.5.10.2. Specification

These EHs are specified in [RFC3692] and [RFC4727].

3.5.10.3. Specific Security Implications

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

3.5.10.4. 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.

3.5.10.5. Advice

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

3.6. 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").

3.6.1. 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.

3.6.2. Specification

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

3.6.3. Specific Security Implications

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

3.6.4. 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, which is [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.

3.6.5. 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 Distributed Denial-of-Service (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. Summary of Advice on the Handling of IPv6 Packets with Specific IPv6 Options

This section summarizes the advice provided in Section 4.4, and it includes references to the specific sections in which a detailed analysis can be found.

Option	Filtering Policy	Reference
Pad1 (Type=0x00)	Permit	Section 4.4.1
PadN (Type=0x01)	Permit	Section 4.4.2
Tunnel Encapsulation Limit (Type=0x04)	Permit	Section 4.4.3
Router Alert (Type=0x05)	Permit based on needed functionality	Section 4.4.4
CALIPSO (Type=0x07)	Permit based on needed functionality	Section 4.4.5
SMF_DPD (Type=0x08)	Permit based on needed functionality	Section 4.4.6
PDM Option (Type=0x0F)	Permit	Section 4.4.7
RPL Option (Type=0x23)	Permit	Section 4.4.8
Quick-Start (Type=0x26)	Permit	Section 4.4.9
Deprecated (Type=0x4D)	Drop	Section 4.4.10

MPL Option (Type=0x6D)	Permit	Section 4.4.12
Jumbo Payload (Type=0xC2)	Permit based on needed functionality	Section 4.4.16
RPL Option (Type=0x63)	Drop	Section 4.4.11
Endpoint Identification (Type=0x8A)	Drop	Section 4.4.13
ILNP Nonce (Type=0x8B)	Permit	Section 4.4.14
Line-Identification Option (Type=0x8C)	Drop	Section 4.4.15
Home Address (Type=0xC9)	Permit	Section 4.4.17
IP_DFF (Type=0xEE)	Permit based on needed functionality	Section 4.4.18
RFC3692-style Experiment (Types = 0x1E, 0x3E, 0x5E, 0x7E, 0x9E, 0xBE, 0xDE, 0xFE)	Permit based on needed functionality	Section 4.4.19

Table 2: Summary of Advice on the Handling of IPv6 Packets with Specific IPv6 Options

4.4. 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.

4.4.1. Pad1 (Type=0x00)

4.4.1.1. 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.

4.4.1.2. Specification

This option is specified in [RFC8200].

4.4.1.3. Specific Security Implications

None.

4.4.1.4. Operational and Interoperability Impact If Blocked

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

4.4.1.5. Advice

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

4.4.2. PadN (Type=0x01)

4.4.2.1. 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.

4.4.2.2. Specification

This option is specified in [RFC8200].

4.4.2.3. Specific Security Implications

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

4.4.2.4. Operational and Interoperability Impact If Blocked

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

4.4.2.5. Advice

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

4.4.3. Tunnel Encapsulation Limit (Type=0x04)

4.4.3.1. Uses

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

4.4.3.2. Specification

This option is specified in [RFC2473].

4.4.3.3. Specific Security Implications

These are discussed in [RFC2473].

4.4.3.4. Operational and Interoperability Impact If Blocked

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

4.4.3.5. Advice

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

4.4.4. Router Alert (Type=0x05)

4.4.4.1. Uses

The Router Alert option [RFC2711] is employed by a number of protocols, including the Resource reSerVation Protocol (RSVP) [RFC2205], Multicast Listener Discovery (MLD) [RFC2710] [RFC3810], Multicast Router Discovery (MRD) [RFC4286], and General Internet Signaling Transport (GIST) [RFC5971]. Its usage is discussed in detail in [RFC6398].

4.4.4.2. Specification

This option is specified in [RFC2711].

4.4.4.3. 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. The security implications of the Router Alert option are discussed in detail in [RFC6398].

4.4.4.4. Operational and Interoperability Impact If Blocked

Discarding packets that contain this option would break any protocols that rely on them, such as RSVP and multicast deployments. Please see Section 4.4.4.3 for further details.

4.4.4.5. Advice

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

4.4.5. CALIPSO (Type=0x07)

4.4.5.1. 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.

4.4.5.2. Specification

This option is specified in [RFC5570].

4.4.5.3. 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.

4.4.5.4. 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 Common Architecture Label IPv6 Security Option (CALIPSO) was stripped by a middlebox (such as a packet scrubber). Associating an incorrect Sensitivity Label can cause the received information to be handled either as more sensitive than it really is ("upgrading") or as less sensitive than it really is ("downgrading"), either of which is problematic. As noted in [RFC5570], IPsec [RFC4301] [RFC4302] [RFC4303] can be employed to protect the CALIPSO.

4.4.5.5. Advice

Recommendations for handling the CALIPSO depend on the deployment environment rather than on 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 that particular intermediate system has been deployed within an 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 [RFC5570], there should be a configuration option to either (a) drop packets containing the CALIPSO or (b) ignore the presence of the CALIPSO 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 [RFC5570], 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 as per [RFC5570]. 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 configuration option 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.

4.4.6. SMF_DPD (Type=0x08)

4.4.6.1. Uses

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

4.4.6.2. Specification

This option is specified in [RFC6621].

4.4.6.3. Specific Security Implications

None. The use of transient numeric identifiers is subject to the security and privacy considerations discussed in [NUMERIC-IDS].

4.4.6.4. Operational and Interoperability Impact If Blocked

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

4.4.6.5. Advice

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

4.4.7. PDM (Type=0x0F)

4.4.7.1. Uses

This option is employed to convey sequence numbers and timing information in IPv6 packets as a basis for measurements.

4.4.7.2. Specification

This option is specified in [RFC8250].

4.4.7.3. Specific Security Implications

These are discussed in [RFC8250]. Additionally, since this option

employs transient numeric identifiers, implementations may be subject to the issues discussed in [NUMERIC-IDS].

4.4.7.4. Operational and Interoperability Impact If Blocked

Dropping packets containing this option will result in negative interoperability implications for traffic employing this option as a basis for measurements.

4.4.7.5. Advice

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

4.4.8. RPL Option (Type=0x23)

4.4.8.1. Uses

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

4.4.8.2. Specification

This option is specified in [RFC9008].

4.4.8.3. Specific Security Implications

These are discussed in [RFC9008].

4.4.8.4. Operational and Interoperability Impact If Blocked

This option can survive outside of a RPL instance. As a result, discarding packets based on the presence of this option would break some use cases for RPL (see [RFC9008]).

4.4.8.5. Advice

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

4.4.9. Quick-Start (Type=0x26)

4.4.9.1. 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].

4.4.9.2. Specification

This option is specified in [RFC4782] on the "Experimental" track.

4.4.9.3. Specific Security Implications

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

* attacks to increase the routers' processing and state load and

* 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.

4.4.9.4. Operational and Interoperability Impact If Blocked

If packets with IPv6 Quick Start options are blocked, the host trying to establish a TCP connection will fall back to not including the Quick Start option -- this means that the feature will be disabled, and additional delays in connection establishment will be introduced (as discussed in 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].

4.4.9.5. Advice

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

4.4.10. Deprecated (Type=0x4D)

4.4.10.1. Uses

No information has been found about this option type.

4.4.10.2. Specification

No information has been found about this option type.

4.4.10.3. Specific Security Implications

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

4.4.10.4. Operational and Interoperability Impact If Blocked

Unknown.

4.4.10.5. Advice

Intermediate systems should discard packets that contain this option.

4.4.11. RPL Option (Type=0x63)

4.4.11.1. Uses

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

4.4.11.2. Specification

This option was originally specified in [RFC6553]. It has been deprecated by [RFC9008].

4.4.11.3. Specific Security Implications

These are discussed in Section 5 of [RFC6553].

4.4.11.4. Operational and Interoperability Impact If Blocked

This option is meant to be employed within a RPL instance. As a result, discarding packets based on the presence of this option outside of a RPL instance will not result in interoperability implications.

4.4.11.5. Advice

Intermediate systems should discard packets that contain a RPL Option.

4.4.12. MPL Option (Type=0x6D)

4.4.12.1. Uses

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

4.4.12.2. Specification

This option is specified in [RFC7731] and is meant to be included only in Hop-by-Hop Options headers.

4.4.12.3. Specific Security Implications

These are discussed in [RFC7731].

4.4.12.4. Operational and Interoperability Impact If Blocked

Dropping packets that contain an MPL Option within an MPL network would break the MPL. However, dropping such packets at the border of such networks will have no negative impact.

4.4.12.5. 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 header, such systems should consider the discussion in Section 3.5.1.

4.4.13. Endpoint Identification (Type=0x8A)

4.4.13.1. Uses

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

4.4.13.2. Specification

This option is specified in [NIMROD-DOC].

4.4.13.3. Specific Security Implications

Undetermined.

4.4.13.4. Operational and Interoperability Impact If Blocked

None.

4.4.13.5. Advice

Intermediate systems should discard packets that contain this option.

4.4.14. ILNP Nonce (Type=0x8B)

4.4.14.1. Uses

This option is employed by the Identifier-Locator Network Protocol for IPv6 (ILNPv6) to provide 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.

4.4.14.2. Specification

This option is specified in [RFC6744].

4.4.14.3. Specific Security Implications

These are discussed in [RFC6744].

4.4.14.4. Operational and Interoperability Impact If Blocked

Discarding packets that contain this option will break ILNPv6 deployments.

4.4.14.5. Advice

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

4.4.15. Line-Identification Option (Type=0x8C)

4.4.15.1. 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.

4.4.15.2. Specification

This option is specified in [RFC6788].

4.4.15.3. Specific Security Implications

These are discussed in [RFC6788].

4.4.15.4. Operational and Interoperability Impact If Blocked

Since this option is meant to be used when tunneling Neighbor Discovery messages in some broadband network deployment scenarios, discarding packets based on the presence of this option at intermediate systems will result in no interoperability implications.

4.4.15.5. Advice

Intermediate systems should discard packets that contain this option.

4.4.16. Jumbo Payload (Type=0XC2)

4.4.16.1. Uses

The Jumbo Payload option provides the means for supporting payloads larger than 65535 bytes.

4.4.16.2. Specification

This option is specified in [RFC2675].

4.4.16.3. Specific Security Implications

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

4.4.16.4. Operational and Interoperability Impact If Blocked

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

4.4.16.5. Advice

An operator should permit this option only in specific scenarios in which support for IPv6 jumbograms is required.

4.4.17. Home Address (Type=0xC9)

4.4.17.1. 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.

4.4.17.2. Specification

This option is specified in [RFC6275].

4.4.17.3. Specific Security Implications

There are no (known) additional security implications, other than those discussed in [RFC6275].

4.4.17.4. Operational and Interoperability Impact If Blocked

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

4.4.17.5. Advice

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

4.4.18. IP_DFF (Type=0xEE)

4.4.18.1. Uses

This option is employed with the (experimental) Depth-First Forwarding (DFF) in unreliable networks.

4.4.18.2. Specification

This option is specified in [RFC6971].

4.4.18.3. Specific Security Implications

These are specified in [RFC6971].

4.4.18.4. 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 operational or interoperability implications.

4.4.18.5. Advice

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

4.4.19. RFC3692-Style Experiment (Types = 0x1E, 0x3E, 0x5E, 0x7E, 0x9E, 0xBE, 0xDE, 0xFE)

4.4.19.1. 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.

4.4.19.2. Specification

These options are specified in [RFC4727] in the context of RFC3692-style experiments.

4.4.19.3. Specific Security Implications

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

4.4.19.4. 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.

4.4.19.5. Advice

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

4.5. 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, which is [IANA-IPV6-PARAM], as "unknown IPv6 options".

4.5.1. Uses

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

4.5.2. Specification

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

4.5.3. Specific Security Implications

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

4.5.4. Operational and Interoperability Impact If Blocked

Discarding unknown IPv6 options may slow down the deployment of new IPv6 options. As noted in [IPv6-OPTIONS], the corresponding IANA registry, which is [IANA-IPV6-PARAM], should be monitored such that IPv6 option filtering rules are updated as new IPv6 options are standardized.

4.5.5. Advice

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

5. IANA Considerations

This document has no IANA actions.

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.

As discussed in Section 3.3, one of the underlying principles for the advice provided in this document is that IPv6 packets with specific EHs or options that may represent an attack vector for infrastructure devices should be dropped. While this policy helps mitigate some specific attack vectors, the recommendations in this document will not help to mitigate vulnerabilities based on implementation errors [RFC9098].

We also note that depending on the router architecture, attempts to filter packets based on the presence of IPv6 EHs or options might itself represent an attack vector to network infrastructure devices [RFC9098].

8. References

8.1. Normative References

[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>.

[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>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC4286] Haberman, B. and J. Martin, "Multicast Router Discovery", RFC 4286, DOI 10.17487/RFC4286, December 2005, <https://www.rfc-editor.org/info/rfc4286>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[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>.

[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>.

[RFC5971] Schulzrinne, H. and R. Hancock, "GIST: General Internet Signalling Transport", RFC 5971, DOI 10.17487/RFC5971, October 2010, <https://www.rfc-editor.org/info/rfc5971>.

[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>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[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>.

[RFC8250] Elkins, N., Hamilton, R., and M. Ackermann, "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option", RFC 8250, DOI 10.17487/RFC8250, September 2017, <https://www.rfc-editor.org/info/rfc8250>.

[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>.

[RFC9008] Robles, M.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", RFC 9008, DOI 10.17487/RFC9008, April 2021, <https://www.rfc-editor.org/info/rfc9008>.

8.2. Informative References

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

[Cisco-EH] Cisco Systems, "IPv6 Extension Headers Review and Considerations", Whitepaper, October 2006, <https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.pdf>.

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

[Huston-2022]
Huston, G. and J. Damas, "IPv6 Fragmentation and EH Behaviours", IEPG Meeting at IETF 113", March 2022, <https://iepg.org/2022-03-20-ietf113/huston-v6frag.pdf>.

[IANA-IPV6-PARAM]
IANA, "Internet Protocol Version 6 (IPv6) Parameters", <https://www.iana.org/assignments/ipv6-parameters>.

[IANA-PROTOCOLS]
IANA, "Protocol Numbers", <https://www.iana.org/assignments/protocol-numbers>.

[IPv6-OPTIONS]
Gont, F., Liu, W., and R. P. Bonica, "Transmission and Processing of IPv6 Options", Work in Progress, Internet-Draft, draft-gont-6man-ipv6-opt-transmit-02, 21 August 2015, <https://datatracker.ietf.org/doc/html/draft-gont-6man-ipv6-opt-transmit-02>.

[JAMES] Iurman, J., "Just Another Measurement of Extension header Survivability (JAMES)", Work in Progress, Internet-Draft, draft-vyncke-v6ops-james-02, 11 July 2022, <https://datatracker.ietf.org/doc/html/draft-vyncke-v6ops-james-02>.

[NIMROD-DOC]
"Nimrod Documentation", <http://ana-3.lcs.mit.edu/~jnc/nimrod>.

[NIMROD-EID]
Lynn, C., "Endpoint Identifier Destination Option", Work in Progress, Internet-Draft, draft-ietf-nimrod-eid-00, 2 March 1996, <https://datatracker.ietf.org/doc/html/draft-ietf-nimrod-eid-00>.

[NUMERIC-IDS]
Gont, F. and I. Arce, "On the Generation of Transient Numeric Identifiers", Work in Progress, Internet-Draft, draft-irtf-pearg-numeric-ids-generation-11, 11 July 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-pearg-numeric-ids-generation-11>.

[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>.

[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>.

[RFC9098] Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. Liu, "Operational Implications of IPv6 Packets with Extension Headers", RFC 9098, DOI 10.17487/RFC9098, September 2021, <https://www.rfc-editor.org/info/rfc9098>.

Acknowledgements

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

The authors of this document would like to thank (in alphabetical order) Mikael Abrahamsson, Brian Carpenter, Tim Chown, Roman Danyliw, Darren Dukes, Lars Eggert, David Farmer, Mike Heard, Bob Hinden, Christian Huitema, Benjamin Kaduk, Erik Kline, Murray Kucherawy, Jen Linkova, Carlos Pignataro, Alvaro Retana, Maria Ines Robles, Zaheduzzaman Sarker, Donald Smith, Pascal Thubert, Ole Troan, Gunter Van de Velde, ric Vyncke, and Robert Wilton for providing valuable comments on earlier draft versions of this document.

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

The authors would like to thank Warren Kumari and ric Vyncke for their guidance during the publication process for 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).

Authors' Addresses

Fernando Gont
SI6 Networks
Segurola y Habana 4310 7mo piso
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
China
Email: liushucheng@huawei.com