Recommendations on Filtering of IPv6 Packets Containing IPv6 Extension
Headers
draft-gont-opsec-ipv6-eh-filtering-02.txt

Abstract

This document provides advice on the filtering of IPv6 packets based on
the IPv6 Extension Headers and the IPv6 options they contain. Additionally, it discusses the operational and interoperability
implications of discarding packets based on the IPv6 Extension
Headers and IPv6 options they contain.

Status of This Memo

This Internet-Draft is submitted in full conformance with the
provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF). Note that other groups may also distribute
working documents as Internet-Drafts. The list of current Internet-
Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months
and may be updated, replaced, or obsoleted by other documents at any
time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 27, 2015.

Copyright Notice

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

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
1. Introduction

Recent studies (see e.g.[I-D.gont-v6ops-ipv6-ehs-in-real-world]) suggest that there is widespread filtering of IPv6 packets that contain IPv6 Extension Headers (EHs). While some operators "officially" filter packets that contain IPv6 extension headers, 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 discusses the filtering of IPv6 packets based on the IPv6 Extension Headers and the IPv6 options they contain. Since various protocols may use IPv6 Extension Headers (possibly with IPv6 options), discarding packets based on the IPv6 Extension Headers or IPv6 options they contain may have implications on the proper
functioning of such protocols. Thus, this document attempts to
discuss the operational and interoperability implications of such
filtering policies, and provide advice in this area. This document
is similar in nature to [RFC7126], which addresses the same problem
for the IPv4 case.

Section 2 of this document specifies the terminology and conventions
employed throughout this document. Section 3 of this document
discusses IPv6 extension headers and provides advice in the area of
filtering IPv6 packets that contain such IPv6 Extension Headers.
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 "fast path", "slow path", and associated relative terms
("faster path" and "slower path") are loosely defined as in Section 2
of [RFC6398].

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.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

2.2. Conventions

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

- 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.

- 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 configurations, but does not change the implementation defaults required by [RFC7045] and [draft-gont-6man-ipv6-opt-transmit].

We recommend that a configuration option is made available to govern the processing of each IPv6 Extension Header type and each IPv6 option type. Such configuration options may include the following possible settings:

- Permit this IPv6 Extension Header or IPv6 Option type
- Drop (and log) packets containing this IPv6 Extension Header or option type
- Reject (and log) packets containing this IPv6 Extension Header or option type (where the packet drop is signaled with an ICMPv6 error message)
- Rate-limit the processing of packets containing this IPv6 Extension Header or option type
- Ignore this IPv6 Extension Header or option type (forwarding packets that contain them)

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 [RFC2460] Extension Headers allow for the extension of the IPv6 protocol. Since both IPv6 Extension Headers and upper-layer protocols share the same namespace ("Next Header" registry/namespace), [RFC7045] identifies which of the currently assigned...
Internet Protocol numbers identify IPv6 Extension Headers vs. upper-layer protocols. This document discusses the filtering of packets based on the IPv6 Extension Headers (as specified by [RFC7045]) they contain.

NOTE: [RFC7112] specifies that non-fragmented IPv6 datagrams and IPv6 First-Fragments MUST contain the entire IPv6 header chain [RFC7112]. Therefore, intermediate systems can always 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 [RFC7112].

3.2. General Security Implications

Depending on the specific device architecture, IPv6 packets that contain IPv6 Extension Headers may 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 [Cisco-EH] [FW-Benchmark].

Operators are urged to consider IPv6 Extension Header filtering and IPv6 options handling capabilities of different devices as they make deployment decisions in future.

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

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

3.3.1.1. Uses

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

3.3.1.2. Specification

This Extension Header is specified in [RFC2460], and its processing rules have been updated by [RFC7045]. At the time of this writing, the following options have been specified for the Hop-by-Hop Options extension header:

- Type 0x05: Router Alert [RFC2711]
- Type 0xC2: Jumbo Payload [RFC2675]
- Type 0x63: RPL Option [RFC6553]
- Type 0x08: SMF_DPD [RFC6621]
o Type 0x6D: MPL Option [I-D.ietf-roll-trickle-mcast]

o Type 0xEE: IPv6 DFF Header [RFC6971]

o Type 0x26: Quick-Start [RFC4782]

o Type 0x07: CALIPSO [RFC5570]

3.3.1.3. Specific Security Implications

Since this Extension Header should be processed by all intermediate-systems en route, it can be leveraged to perform Denial of Service attacks against the network infrastructure.

3.3.1.4. Operational and Interoperability Impact if Blocked

Discarding packets containing a Hop-by-Hop Option extension 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.

3.3.1.5. Advice

The recommended configuration for the processing of these packets depends on the features and capabilities of the underlying platform. On platforms that allow forwarding of packets with HBH Options on the fast path, we recommend that packets with a HBH Options extension header be forwarded as normal (for instance, [RFC7045] allows for implementations to ignore the HBH Options extension header when forwarding packets). Otherwise, on platforms in which processing of packets with a IPv6 HBH Options extension header 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 extension header 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 extension headers.

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 Extension Header.
3.3.2. Routing Header for IPv6 (Protocol Number=43)

3.3.2.1. 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.

3.3.2.2. Specification

This Extension Header is specified in [RFC2460]. [RFC2460] originally specified the Routing Header Type 0, which has been later obsoleted by [RFC5095].

At the time of this writing, 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]
- Types 4-252: Unassigned
- Type 253: RFC3692-style Experiment 1 [RFC4727]
- Type 254: RFC3692-style Experiment 2 [RFC4727]
- Type 255: Reserved

3.3.2.3. Specific Security Implications

The security implications of RHT0 have been discussed in detail in [Biondi2007] and [RFC5095].

3.3.2.4. Operational and Interoperability Impact if Blocked

Blocking packets containing a RHT0 or RTH1 has no operational implications. However, blocking packets employing other routing header types will break the protocols that rely on them.
3.3.2.5. Advice

Intermediate systems should discard packets containing a RHT0 or RHT1. As required by [RFC7045], packets containing standardised and undeprecated Routing Headers should be permitted.

3.3.3. Fragment Header for IPv6 (Protocol Number=44)

3.3.3.1. Uses

This Extension Header provides the fragmentation functionality for IPv6.

3.3.3.2. Specification

This Extension Header is specified in [RFC2460].

3.3.3.3. 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 [I-D.ietf-6man-predictable-fragment-id].

3.3.3.4. 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]).

3.3.3.5. Advice

Intermediate systems should permit packets that contain a Fragment Header.

3.3.4. Encapsulating Security Payload (Protocol Number=50)

3.3.4.1. Uses

This extension Header is employed for the IPsec suite [RFC4303].

3.3.4.2. Specification

This extension header is specified in [RFC4303].
3.3.4.3. Specific Security Implications

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

3.3.4.4. Operational and Interoperability Impact if Blocked

Discarding packets that employ this extension header would break IPsec deployments.

3.3.4.5. Advice

Intermediate systems should permit packets containing the Encapsulating Security Payload extension header.

3.3.5. Authentication Header (Number=51)

3.3.5.1. Uses

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

3.3.5.2. Specification

This Extension Header is specified in [RFC4302].

3.3.5.3. Specific Security Implications

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

3.3.5.4. Operational and Interoperability Impact if Blocked

Discarding packets that employ this extension header would break IPsec deployments.

3.3.5.5. Advice

Intermediate systems should permit packets containing an Authentication Header.
3.3.6. Destination Options for IPv6 (Protocol Number=60)

3.3.6.1. Uses

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

3.3.6.2. Specification

This Extension Header is specified in [RFC2460]. At the time of this writing, the following options have been specified for this extension header:

- Type 0x04: Tunnel Encapsulation Limit [RFC2473]
- Type 0xC9: Home Address [RFC6275]
- Type 0x8B: ILNP Nonce [RFC6744]
- Type 0x8C: Line-Identification Option [RFC6788]

3.3.6.3. Specific Security Implications

No security implications are known, other than the general implications of IPv6 extension headers.

3.3.6.4. 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.

3.3.6.5. Advice

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

3.3.7. Mobility Header (Number=135)

3.3.7.1. Uses

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

This Extension Header is specified in [RFC6275].

3.3.7.3. Specific Security Implications

TBD.

3.3.7.4. Operational and Interoperability Impact if Blocked

Discarding packets containing this extension header would break Mobile IPv6.

3.3.7.5. Advice

Intermediate systems should permit packets containing this extension header.

3.3.8. Host Identity Protocol (Protocol Number=139)

3.3.8.1. Uses

This extension header 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.

3.3.8.2. Specification

This extension Header is specified in [RFC5201].

3.3.8.3. Specific Security Implications

TBD.

3.3.8.4. Operational and Interoperability Impact if Blocked

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

3.3.8.5. Advice

Intermediate systems should permit packets that contain a Host Identity Protocol extension header.
3.3.9. Shim6 Protocol (Protocol Number=140)

3.3.9.1. Uses

This extension header is employed by the Shim6 [RFC5533] Protocol.

3.3.9.2. Specification

This Extension Header is specified in [RFC5533].

3.3.9.3. Specific Security Implications

TBD.

3.3.9.4. Operational and Interoperability Impact if Blocked

Discarding packets that contain this extension header will break Shim6.

3.3.9.5. Advice

Intermediate systems should permit packets containing this extension header.

3.3.10. Use for experimentation and testing (Protocol Numbers=253 and 254)

3.3.10.1. Uses

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

3.3.10.2. Specification

These Extension Headers are specified in [RFC3692] and [RFC4727].

3.3.10.3. Specific Security Implications

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

3.3.10.4. Operational and Interoperability Impact if Blocked

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

Intermediate systems should discard packets containing these extension headers. Only in specific scenarios in which RFC3692-Style experiments are to be performed should these extension headers be permitted.

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

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

3.4.1.  Uses

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

Since IPv6 Extension Headers 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 Extension Header or an Upper-Layer protocol.

3.4.2.  Specification

The processing of unknown IPv6 extension headers is specified in [RFC2460] and [RFC7045].

3.4.3.  Specific Security Implications

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

3.4.4.  Operational and Interoperability Impact if Blocked

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

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

Intermediate systems should discard packets containing unknown IPv6 extension headers.

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 Extension Headers. 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 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 [RFC2460].

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 extension headers.

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 [RFC2460].

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 extension headers.

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

TBD.

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 is specified in [RFC6553].

4.3.4.3. Specific Security Implications

TBD.

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. Tunnel Encapsulation Limit (Type=0x04)

4.3.5.1. Uses

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

This option is specified in [RFC2473].

4.3.5.3. Specific Security Implications

TBD.

4.3.5.4. Operational and Interoperability Impact if Blocked

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

4.3.5.5. Advice

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

4.3.6. Router Alert (Type=0x05)

4.3.6.1. Uses

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

4.3.6.2. Specification

This option is specified in [RFC2711].

4.3.6.3. 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.

4.3.6.4. Operational and Interoperability Impact if Blocked

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

4.3.6.5. Advice

Intermediate systems should discard packets that contain this option. Only in specific environments where support for RSVP or similar protocols is desired should this option be permitted.
4.3.7. Quick-Start (Type=0x26)

4.3.7.1. 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].

4.3.7.2. Specification

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

4.3.7.3. 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.

4.3.7.4. 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].

4.3.7.5. Advice

Intermediate systems should not discard IPv6 packets based on the presence of this option.
4.3.8. CALIPSO (Type=0x07)

4.3.8.1. 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.

4.3.8.2. Specification

This option is specified in [RFC5570].

4.3.8.3. 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.

4.3.8.4. 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.

4.3.8.5. Advice

Intermediate systems that do not operate in Multi-Level Secure (MLS) networking environments should discard packets that contain this option.

4.3.9. SMF_DPD (Type=0x08)

4.3.9.1. 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.
4.3.9.2. Specification

This option is specified in [RFC6621].

4.3.9.3. Specific Security Implications

TBD.

4.3.9.4. Operational and Interoperability Impact if Blocked

TBD.

4.3.9.5. Advice

TBD.

4.3.10. Home Address (Type=0xC9)

4.3.10.1. 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.

4.3.10.2. Specification

This option is specified in [RFC6275].

4.3.10.3. Specific Security Implications

TBD.

4.3.10.4. Operational and Interoperability Impact if Blocked

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

4.3.10.5. Advice

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

4.3.11. Endpoint Identification (Type=0x8A)

4.3.11.1. Uses

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

This option is specified in [NIMROD-DOC].

4.3.11.3. Specific Security Implications

TBD.

4.3.11.4. Operational and Interoperability Impact if Blocked

None.

4.3.11.5. Advice

Intermediate systems should discard packets that contain this option.

4.3.12. ILNP Nonce (Type=0x8B)

4.3.12.1. 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.

4.3.12.2. Specification

This option is specified in [RFC6744].

4.3.12.3. Specific Security Implications

TBD.

4.3.12.4. Operational and Interoperability Impact if Blocked

Discarding packets that contain this option will break INLPv6 deployments.

4.3.12.5. Advice

Intermediate systems should not discard packets based on the presence of this option.
4.3.13. Line-Identification Option (Type=0x8C)

4.3.13.1. 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.

4.3.13.2. Specification

This option is specified in [RFC6788].

4.3.13.3. Specific Security Implications

TBD.

4.3.13.4. 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.

4.3.13.5. Advice

Intermediate devices should discard packets that contain this option.

4.3.14. Deprecated (Type=0x4D)

4.3.14.1. Uses

No information has been found about this option type.

4.3.14.2. Specification

No information has been found about this option type.

4.3.14.3. Specific Security Implications

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

4.3.14.4. Operational and Interoperability Impact if Blocked

Unknown.
4.3.14.5. Advice

Intermediate systems should discard packets that contain this option.

4.3.15. MPL Option (Type=0x6D)

4.3.15.1. Uses

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

4.3.15.2. Specification

This option is specified in [I-D.ietf-roll-trickle-mcast], and is meant to be included only in Hop-by-Hop Option headers.

4.3.15.3. Specific Security Implications

TBD.

4.3.15.4. Operational and Interoperability Impact if Blocked

TBD.

4.3.15.5. Advice

TBD.

4.3.16. IP_DFF (Type=0xEE)

4.3.16.1. Uses

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

4.3.16.2. Specification

This option is specified in [RFC6971].

4.3.16.3. Specific Security Implications

TBD.
4.3.16.4.  Operational and Interoperability Impact if Blocked

TBD.

4.3.16.5.  Advice

TBD.

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

4.3.17.1.  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.

4.3.17.2.  Specification

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

4.3.17.3.  Specific Security Implications

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

4.3.17.4.  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.

4.3.17.5.  Advice

Intermediate systems should discard packets that contain these options. Only in specific environments where RFC3692-style experiments are meant to be performed should these options be permitted.

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 [RFC2460].

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

Enterprise intermediate systems that process the contents of IPv6 extension headers should discard packets that contain unknown options. Other intermediate systems that process the contents of IPv6 extension headers should permit packets that contain unknown options.

5. IANA Considerations

This document has no actions for IANA.

6. Security Considerations

This document provides advice on the filtering of IPv6 packets that contain IPv6 Extension Headers (and possibly IPv6 options). Discarding such packets can help to mitigate the security issues that arise from the use of different IPv6 Extension Headers and options.

7. Acknowledgements

The authors of this document would like to thank (in alphabetical order) Mikael Abrahamsson, Brian Carpenter, Mike Heard, and Donald Smith, for providing valuable comments on earlier versions of this document.
This document borrows some text an analysis from [RFC7126], authored by Fernando Gont, Randall Atkinson, and Carlos Pignataro.

8. References

8.1. Normative References


8.2. Informative References

[Biondi2007]

[Cisco-EH]

[FW-Benchmark]

[I-D.gont-v6ops-ipv6-ehs-in-real-world]
[I-D.ietf-6man-predictable-fragment-id]

[I-D.ietf-roll-trickle-mcast]

[IANA-IPV6-PARAM]

[IANA-PROTOCOLS]

[NIMROD-DOC]


Authors' Addresses

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

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

Email: liushucheng@huawei.com

Ronald P. Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, VA 20171
US
Phone: 571 250 5819
Email: rbonica@juniper.net