IPv6 Operations Working Group (v6ops)
Internet-Draft
Intended status: Informational
Expires: February 1, 2021

F. Gont
SI6 Networks
N. Hilliard
INEX
G. Doering
SpaceNet AG
W. Kumari
Google
G. Huston
APNIC
W. Liu
Huawei Technologies
July 31, 2020

Operational Implications of IPv6 Packets with Extension Headers
draft-ietf-v6ops-ipv6-ehs-packet-drops-00

Abstract

This document summarizes the operational implications of IPv6 extension headers, and attempts to analyze reasons why packets with IPv6 extension headers may be dropped in the public Internet.

Status of This Memo

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

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

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

This Internet-Draft will expire on February 1, 2021.

Table of Contents

1. Introduction 2
2. Disclaimer 3
3. Previous Work on IPv6 Extension Headers 3
4. Packet Forwarding Engine Constraints 5
5. Requirement to Process Layer-3/layer-4 information in Intermediate Systems 6
5.1. ECMP and Hash-based Load-Sharing 6
5.2. Enforcing infrastructure ACLs 7
5.3. DDoS Management and Customer Requests for Filtering . . . 7
6. Operational Implications 8
6.1. Inability to Find Layer-4 Information 8
6.2. Route-Processor Protection 8
6.3. Inability to Perform Fine-grained Filtering 8
6.4. Security Concerns Associated with IPv6 Extension Headers 8
7. IANA Considerations 10
8. Security Considerations 10
9. Acknowledgements 10
10. References 10
10.1. Normative References 10
10.2. Informative References 11
Authors' Addresses 15

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 and middle-boxes, and evidence exists that IPv6 packets with EHs may be intentionally dropped in the public Internet in some network deployments.

The authors of this document have been involved in numerous discussions about IPv6 extension headers (both within the IETF and in other fora), and have noticed that the security and operational implications associated with IPv6 EHs were unknown to the larger audience participating in these discussions.

This document has the following goals:

- Raise awareness about the operational and security implications of IPv6 Extension Headers, and presents reasons why some networks may intentionally drop packets containing IPv6 Extension Headers.

- Highlight areas where current IPv6 support by networking devices maybe sub-optimal, such that the aforementioned support is improved.

- Highlight operational issues associated with IPv6 extension headers, such that those issues are considered in IETF standardization efforts.

Section 3 of this document summarizes the previous work that has been carried out in the area of IPv6 extension headers. Section 4 discuses packet forwarding engine constraints in modern routers. Section 5 discusses why modern routers and middle-boxes may need to access Layer-4 information to make a forwarding decision. Finally, Section 6 discusses the operational implications of IPv6 EHs.

2. Disclaimer

This document analyzes the operational challenges represented by packets that employ IPv6 Extension Headers, and documents some of the operational reasons for which these packets may be dropped in the public Internet. This document IS NOT a recommendation to drop such packets, but rather an analysis of why they are dropped.

3. Previous Work on IPv6 Extension Headers

Some of the operational implications of IPv6 Extension Headers have been discussed in IETF circles:

- [I-D.taylor-v6ops-fragdrop] discusses a rationale for which operators drop IPv6 fragments.

- [I-D.wkumari-long-headers] discusses possible issues arising from "long" IPv6 header chains.

- [I-D.kampanakis-6man-ipv6-eh-parsing] describes how inconsistencies in the way IPv6 packets with extension headers are parsed by different implementations may result in evasion of security controls, and presents guidelines for parsing IPv6 extension headers with the goal of providing a common and consistent parsing methodology for IPv6 implementations.

- [I-D.ietf-opsec-ipv6-eh-filtering] analyzes the security implications of IPv6 EHs, and the operational implications of dropping packets that employ IPv6 EHs and associated options.

- [RFC7113] discusses how some popular RA-Guard implementations are subject to evasion by means of IPv6 extension headers.

- [I-D.ietf-intarea-frag-fragile] analyzes the fragility introduced by IP fragmentation.

A number of recent RFCs have discussed issues related to IPv6 extension headers, specifying updates to a previous revision of the IPv6 standard ([RFC2460]), many of which have now been incorporated into the current IPv6 core standard ([RFC8200]) or the IPv6 Node Requirements ([RFC8504]). Namely,

- [RFC5095] discusses the security implications of Routing Header Type 0 (RTH0), and deprecates it.

- [RFC5722] analyzes the security implications of overlapping fragments, and provides recommendations in this area.

- [RFC7045] clarifies how intermediate nodes should deal with IPv6 extension headers.

- [RFC7112] discusses the issues arising in a specific fragmentation case where the IPv6 header chain is fragmented into two or more fragments (and formally forbids such fragmentation case).

- [RFC6946] discusses a flawed (but common) processing of the so-called IPv6 "atomic fragments", and specified improved processing of such packets.

- [RFC8021] deprecates the generation of IPv6 atomic fragments.

- [RFC8504] clarifies processing rules for packets with extension headers, and also allows hosts to enforce limits on the number of options included in IPv6 EHs.

- [RFC7739] discusses the security implications of predictable fragment Identification values, and provides recommendations for the generation of these values.

- [RFC6980] analyzes the security implications of employing IPv6 fragmentation with Neighbor Discovery for IPv6, and formally recommends against such usage.

Additionally, [RFC8200] has relaxed the requirement that "all nodes examine and process the Hop-by-Hop Options header" from [RFC2460], by specifying that only to nodes that have been explicitly configured to process the Hop-by-Hop Options header are required to do so.

A number of studies have measured the extent to which packets employing IPv6 extension headers are dropped in the public Internet:

- [PMTUD-Blackholes], [Gont-IEPG88], [Gont-Chown-IEPG89], and [Linkova-Gont-IEPG90] presented some preliminary measurements regarding the extent to which packet containing IPv6 EHs are dropped in the public Internet.

- [RFC7872] presents more comprehensive results and documents the methodology for obtaining the presented results.

- [Huston-2017] and [Huston-2020] measured packet drops resulting from IPv6 fragmentation when communicating with DNS servers.

4. Packet Forwarding Engine Constraints

Most modern routers use dedicated hardware (e.g. ASICs or NPUs) to determine how to forward packets across their internal fabrics (see [IEPG94-Scudder] and [APNIC-Scudder] for details). One of the common methods of handling next-hop lookup is to send a small portion of the ingress packet to a lookup engine with specialised hardware (e.g. ternary CAM or RLDRAM) to determine the packet's next-hop. Technical constraints mean that there is a trade-off between the amount of data sent to the lookup engine and the overall performance of the lookup engine. If more data is sent, the lookup engine can inspect further into the packet, but the overall performance of the system will be reduced. If less data is sent, the overall performance of the router will be increased but the packet lookup engine may not be able to inspect far enough into a packet to determine how it should be handled.

NOTE:
For example, current high-end routers can use up to 192 bytes of header (Cisco ASR9000 Typhoon) or 384 bytes of header (Juniper MX Trio).

If a hardware forwarding engine on a modern router cannot make a forwarding decision about a packet because critical information is not sent to the look-up engine, then the router will normally drop the packet.

NOTE:

Section 5 discusses some of the reasons for which a modern router might need to access layer-4 information to make a forwarding decision.

Historically, some packet forwarding engines punted packets of this form to the control plane for more in-depth analysis, but this is unfeasible on most current router architectures as a result of the vast difference between the hardware forwarding capacity of the router and processing capacity of the control plane and the size of the management link which connects the control plane to the forwarding plane.

If an IPv6 header chain is sufficiently long that its header exceeds the packet look-up capacity of the router, then it may be dropped due to hardware inability to determine how it should be handled.

5. Requirement to Process Layer-3/layer-4 information in Intermediate Systems

The following subsections discuss some of reasons for which modern routers and middle-boxes may need to process Layer-3/layer-4 information to make a forwarding decision.

5.1. ECMP and Hash-based Load-Sharing

In the case of ECMP (equal cost multi path) load sharing, the router on the sending side of the link needs to make a decision regarding which of the links to use for a given packet. Since round-robin usage of the links is usually avoided in order to prevent packet reordering, forwarding engines need to use a mechanism which will consistently forward the same data streams down the same forwarding paths. Most forwarding engines achieve this by calculating a simple hash using an n-tuple gleaned from a combination of layer-2 through to layer-4 packet header information. This n-tuple will typically use the src/dst MAC address, src/dst IP address, and if possible further layer-4 src/dst port information. As layer-4 port information increases the entropy of the hash, it is normally highly desirable to use it where possible.

We note that in the IPv6 world, flows are expected to be identified by means of the IPv6 Flow Label [RFC6437]. Thus, ECMP and Hash-based Load-Sharing would be possible without the need to process the entire IPv6 header chain to obtain upper-layer information to identify flows. However, we note that for a long time many IPv6 implementations failed to set the Flow Label, and ECMP and Hash-based Load-Sharing devices also did not employ the Flow Label for performing their task.

Clearly, widespread support of [RFC6437] would relieve middle-boxes from having to process the entire IPv6 header chain, making Flow Label-based ECMP and Hash-based Load-Sharing [RFC6438] feasible.

While support of [RFC6437] is currently widespread for current versions of all popular host implementations, there is still only marginal usage of the IPv6 Flow Label for ECMP and load balancing [Cunha-2020] -- possibly as a result of issues that have been found in host implementations and middle-boxes [Jaeggli-2018].

5.2. Enforcing infrastructure ACLs

Generally speaking, infrastructure ACLs (iACLs) drop unwanted packets destined to parts of a provider's infrastructure, because they are not operationally needed and can be used for attacks of different sorts against the router's control plane. Some traffic needs to be differentiated depending on layer-3 or layer-4 criteria to achieve a useful balance of protection and functionality, for example:

- Permit some amount of ICMP echo (ping) traffic towards the router's addresses for troubleshooting.

- Permit BGP sessions on the shared network of an exchange point (potentially differentiating between the amount of packets/seconds permitted for established sessions and connection establishment), but do not permit other traffic from the same peer IP addresses.

5.3. DDoS Management and Customer Requests for Filtering

The case of customer DDoS protection and edge-to-core customer protection filters is similar in nature to the infrastructure ACL protection. Similar to infrastructure ACL protection, layer-4 ACLs generally need to be applied as close to the edge of the network as possible, even though the intent is usually to protect the customer edge rather than the provider core. Application of layer-4 DDoS protection to a network edge is often automated using Flowspec [RFC5575].

For example, a web site which normally only handled traffic on TCP ports 80 and 443 could be subject to a volumetric DDoS attack using NTP and DNS packets with randomised source IP address, thereby rendering traditional [RFC5635] source-based real-time black hole mechanisms useless. In this situation, DDoS protection ACLs could be configured to block all UDP traffic at the network edge without impairing the web server functionality in any way. Thus, being able to block arbitrary protocols at the network edge can avoid DDoS-related problems both in the provider network and on the customer edge link.

6. Operational Implications

6.1. Inability to Find Layer-4 Information

As discussed in Section 5, modern routers and middle-boxes that need to find the layer-4 header must process the entire IPv6 extension header chain. When such devices are unable to obtain the required information, they may simply resort to dropping the corresponding packets.

6.2. Route-Processor Protection

Most modern routers have a fast hardware-assisted forwarding plane and a loosely coupled control plane, connected together with a link that has much less capacity than the forwarding plane could handle. Traffic differentiation cannot be done by the control plane side, because this would overload the internal link connecting the forwarding plane to the control plane.

The Hop-by-Hop Options header has been particularly challenging since, in most (if not all) implementations, it has typically caused the corresponding packet to be punted to a software path. As a result, operators usually drop IPv6 packets containing this extension header. Please see [RFC6192] for advice regarding protection of the router control plane.

6.3. Inability to Perform Fine-grained Filtering

Some router implementations lack fine-grained filtering of IPv6 extension headers. For example, an operator may want to drop packets containing Routing Header Type 0 (RHT0) but may only be able to filter on the extension header type (Routing Header). As a result, the operator may end up enforcing a more coarse filtering policy (e.g. "drop all packets containing a Routing Header" vs. "only drop packets that contain a Routing Header Type 0").

6.4. Security Concerns Associated with IPv6 Extension Headers

The security implications of IPv6 Extension Headers generally fall into one or more of these categories:

- Evasion of security controls
- DoS due to processing requirements
- DoS due to implementation errors
- Extension Header-specific issues

Unlike IPv4 packets where the upper-layer protocol can be trivially found by means of the "IHL" ("Internet Header Length") IPv4 header field, the structure of IPv6 packets is more flexible and complex, and may represent a challenge for devices that need to find this information, since locating upper-layer protocol information requires that all IPv6 extension headers be examined. This has presented implementation difficulties, and packet filtering mechanisms that require upper-layer information (even if just the upper layer protocol type) have been found to be trivially evasible by inserting IPv6 Extension Headers between the main IPv6 header and the upper layer protocol. [RFC7113] describes this issue for the RA-Guard case, but the same techniques can be employed to circumvent other IPv6 firewall and packet filtering mechanisms. Additionally, implementation inconsistencies in packet forwarding engines may result in evasion of security controls [I-D.kampanakis-6man-ipv6-eh-parsing] [Atlasis2014] [BH-EU-2014].

Packets that use IPv6 Extension Headers may have a negative performance impact on the handling devices. Unless appropriate mitigations are put in place (e.g., packet dropping and/or rate-limiting), an attacker could simply send a large amount of IPv6 traffic employing IPv6 Extension Headers with the purpose of performing a Denial of Service (DoS) attack (see Section 6 for further details).

NOTE:

In the most trivial case, a packet that includes a Hop-by-Hop Options header might go through the slow forwarding path, and be processed by the router's CPU. Another possible case might be that in which a router that has been configured to enforce an ACL based on upper-layer information (e.g., upper layer protocol or TCP Destination Port), needs to process the entire IPv6 header chain (in order to find the required information), causing the packet to be processed in the slow path [Cisco-EH-Cons]. We note that, for obvious reasons, the aforementioned performance issues may affect other devices such as firewalls, Network Intrusion Detection Systems (NIDS), etc. [Zack-FW-Benchmark]. The extent to which these devices are affected is typically implementation-dependent.

IPv6 implementations, like all other software, tend to mature with time and wide-scale deployment. While the IPv6 protocol itself has existed for over 20 years, serious bugs related to IPv6 Extension Header processing continue to be discovered. Because there is currently little operational reliance on IPv6 Extension headers, the corresponding code paths are rarely exercised, and there is the potential for bugs that still remain to be discovered in some implementations.

IPv6 Fragment Headers are employed to allow fragmentation of IPv6 packets. While many of the security implications of the fragmentation / reassembly mechanism are known from the IPv4 world, several related issues have crept into IPv6 implementations. These range from denial of service attacks to information leakage, as discussed in [RFC7739], [Bonica-NANOG58] and [Atlasis2012]).

7. IANA Considerations

There are no IANA registries within this document. The RFC-Editor can remove this section before publication of this document as an RFC.

8. Security Considerations

The security implications of IPv6 extension headers are discussed in Section 6.4. This document does not introduce any new security issues.

9. Acknowledgements

The authors would like to thank (in alphabetical order) Mikael Abrahamsson, Fred Baker, Brian Carpenter, Tim Chown, Owen DeLong, Tom Herbert, Lee Howard, Sander Steffann, Eduard Vasilenko, Eric Vyncke, Jingrong Xie, and Andrew Yourtchenko, for providing valuable comments on earlier versions of this document.

Fernando Gont would like to thank Jan Zorz / Go6 Lab <http://go6lab.si/>, Jared Mauch, and Sander Steffann <http://steffann.nl/>, for providing access to systems and networks that were employed to perform experiments and measurements involving packets with IPv6 Extension Headers.

10. References

10.1. Normative References

[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>.

[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>.

[RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, DOI 10.17487/RFC5722, December 2009, <https://www.rfc-editor.org/info/rfc5722>.

[RFC6946] Gont, F., "Processing of IPv6 "Atomic" Fragments", RFC 6946, DOI 10.17487/RFC6946, May 2013, <https://www.rfc-editor.org/info/rfc6946>.

[RFC6980] Gont, F., "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery", RFC 6980, DOI 10.17487/RFC6980, August 2013, <https://www.rfc-editor.org/info/rfc6980>.

[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>.

[RFC8021] Gont, F., Liu, W., and T. Anderson, "Generation of IPv6 Atomic Fragments Considered Harmful", RFC 8021, DOI 10.17487/RFC8021, January 2017, <https://www.rfc-editor.org/info/rfc8021>.

[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>.

[RFC8504] Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019, <https://www.rfc-editor.org/info/rfc8504>.

10.2. Informative References

[APNIC-Scudder]
Scudder, J., "Modern router architecture and IPv6", APNIC Blog, June 4, 2020, <https://blog.apnic.net/2020/06/04/modern-router-architecture-and-ipv6/>.

[Atlasis2012]
Atlasis, A., "Attacking IPv6 Implementation Using Fragmentation", BlackHat Europe 2012. Amsterdam, Netherlands. March 14-16, 2012, <https://media.blackhat.com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-Slides.pdf>.

[Atlasis2014]
Atlasis, A., "A Novel Way of Abusing IPv6 Extension Headers to Evade IPv6 Security Devices", May 2014, <http://www.insinuator.net/2014/05/a-novel-way-of-abusing-ipv6-extension-headers-to-evade-ipv6-security-devices/>.

[BH-EU-2014]
Atlasis, A., Rey, E., and R. Schaefer, "Evasion of High-End IDPS Devices at the IPv6 Era", BlackHat Europe 2014, 2014, <https://www.ernw.de/download/eu-14-Atlasis-Rey-Schaefer-briefings-Evasion-of-HighEnd-IPS-Devices-wp.pdf>.

[Bonica-NANOG58]
Bonica, R., "IPv6 Extension Headers in the Real World v2.0", NANOG 58. New Orleans, Louisiana, USA. June 3-5, 2013, <https://www.nanog.org/sites/default/files/mon.general.fragmentation.bonica.pdf>.

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

[Cunha-2020]
Cunha, I., "IPv4 vs IPv6 load balancing in Internet routes", NPS/CAIDA 2020 Virtual IPv6 Workshop, 2020, <https://www.cmand.org/workshops/202006-v6/slides/cunha.pdf>.

[Gont-Chown-IEPG89]
Gont, F. and T. Chown, "A Small Update on the Use of IPv6 Extension Headers", IEPG 89. London, UK. March 2, 2014, <http://www.iepg.org/2014-03-02-ietf89/fgont-iepg-ietf89-eh-update.pdf>.

[Gont-IEPG88]
Gont, F., "Fragmentation and Extension header Support in the IPv6 Internet", IEPG 88. Vancouver, BC, Canada. November 13, 2013, <http://www.iepg.org/2013-11-ietf88/fgont-iepg-ietf88-ipv6-frag-and-eh.pdf>.

[Huston-2017]
Huston, G., "Dealing with IPv6 fragmentation in the DNS", APNIC Blog, 2017, <https://blog.apnic.net/2017/08/22/dealing-ipv6-fragmentation-dns/>.

[Huston-2020]
Huston, G., "Measurement of IPv6 Extension Header Support", NPS/CAIDA 2020 Virtual IPv6 Workshop, 2020, <https://www.cmand.org/workshops/202006-v6/slides/2020-06-16-xtn-hdrs.pdf>.

[I-D.ietf-intarea-frag-fragile]
Bonica, R., Baker, F., Huston, G., Hinden, R., Troan, O., and F. Gont, "IP Fragmentation Considered Fragile", draft-ietf-intarea-frag-fragile-17 (work in progress), September 2019.

[I-D.ietf-opsec-ipv6-eh-filtering]
Gont, F. and W. LIU, "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers", draft-ietf-opsec-ipv6-eh-filtering-06 (work in progress), July 2018.

[I-D.kampanakis-6man-ipv6-eh-parsing]
Kampanakis, P., "Implementation Guidelines for parsing IPv6 Extension Headers", draft-kampanakis-6man-ipv6-eh-parsing-01 (work in progress), August 2014.

[I-D.taylor-v6ops-fragdrop]
Jaeggli, J., Colitti, L., Kumari, W., Vyncke, E., Kaeo, M., and T. Taylor, "Why Operators Filter Fragments and What It Implies", draft-taylor-v6ops-fragdrop-02 (work in progress), December 2013.

[I-D.wkumari-long-headers]
Kumari, W., Jaeggli, J., Bonica, R., and J. Linkova, "Operational Issues Associated With Long IPv6 Header Chains", draft-wkumari-long-headers-03 (work in progress), June 2015.

[IEPG94-Scudder]
Petersen, B. and J. Scudder, "Modern Router Architecture for Protocol Designers", IEPG 94. Yokohama, Japan. November 1, 2015, <http://www.iepg.org/2015-11-01-ietf94/IEPG-RouterArchitecture-jgs.pdf>.

[Jaeggli-2018]
Jaeggli, G., "Dealing with IPv6 fragmentation in the DNS", APNIC Blog, 2018, <https://blog.apnic.net/2018/01/11/ipv6-flow-label-misuse-hashing/>.

[Linkova-Gont-IEPG90]
Linkova, J. and F. Gont, "IPv6 Extension Headers in the Real World v2.0", IEPG 90. Toronto, ON, Canada. July 20, 2014, <http://www.iepg.org/2014-07-20-ietf90/iepg-ietf90-ipv6-ehs-in-the-real-world-v2.0.pdf>.

[PMTUD-Blackholes]
De Boer, M. and J. Bosma, "Discovering Path MTU black holes on the Internet using RIPE Atlas", July 2012, <http://www.nlnetlabs.nl/downloads/publications/pmtu-black-holes-msc-thesis.pdf>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <https://www.rfc-editor.org/info/rfc5575>.

[RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", RFC 5635, DOI 10.17487/RFC5635, August 2009, <https://www.rfc-editor.org/info/rfc5635>.

[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>.

[RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, DOI 10.17487/RFC6437, November 2011, <https://www.rfc-editor.org/info/rfc6437>.

[RFC6438] Carpenter, B. and S. Amante, "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels", RFC 6438, DOI 10.17487/RFC6438, November 2011, <https://www.rfc-editor.org/info/rfc6438>.

[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>.

[RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014, <https://www.rfc-editor.org/info/rfc7113>.

[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>.

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

Authors' Addresses

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

Email: fgont@si6networks.com
URI: https://www.si6networks.com

Nick Hilliard
INEX
4027 Kingswood Road
Dublin 24
IE

Email: nick@inex.ie

Gert Doering
SpaceNet AG
Joseph-Dollinger-Bogen 14
Muenchen D-80807
Germany

Email: gert@space.net

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Geoff Huston

Email: gih@apnic.net
URI: http://www.apnic.net

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

Email: liushucheng@huawei.com