

IPv6 maintenance Working Group (6man)  
Internet-Draft  
Updates: [2460](#) (if approved)  
Intended status: Standards Track  
Expires: August 20, 2012

F. Gont  
SI6 Networks / UTN-FRH  
V. Manral  
Hewlett-Packard Corp.  
February 17, 2012

**Security and Interoperability Implications of Oversized IPv6 Header  
Chains  
draft-gont-6man-oversized-header-chain-00**

Abstract

The IPv6 specification allows IPv6 header chains of an arbitrary size. The specification also allows options which can in turn extend each of the headers. In those scenarios in which the IPv6 header chain or options are unusually long and packets are fragmented, or scenarios in which the fragment size is very small, the first fragment of a packet may fail to include the entire IPv6 header chain. This document discusses the interoperability and security problems of such traffic, and updates [RFC 2460](#) such that all IPv6 packets are required to contain the entire IPv6 header chain within the 'minimum IPv6 MTU' (1280) bytes of the packet.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

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 August 20, 2012.

Copyright Notice

Copyright (c) 2012 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 to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Interoperability Implications of Oversized IPv6 Header Chains . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Forwarding Implications of Oversized IPv6 Header Chains . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Security Implications of Oversized IPv6 Header Chains . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Updating <a href="#">RFC 2460</a> . . . . .	<a href="#">7</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">8</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">9</a>
<a href="#">8.</a>	Acknowledgements . . . . .	<a href="#">10</a>
<a href="#">9.</a>	References . . . . .	<a href="#">11</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">11</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">11</a>
<a href="#">Appendix A.</a>	Changes from previous versions of the document (to be removed by the RFC Editor before publication of this document as a RFC . . . . .	<a href="#">12</a>
A.1.	Changes from <a href="#">draft-manral-6man-tiny-fragments-issues-00</a> . . . . .	<a href="#">12</a>
Authors' Addresses	. . . . .	<a href="#">13</a>



## **1. Introduction**

[RFC2460] allows for an IPv6 header chain of an arbitrary size. It also allows the headers themselves to have options, which can change the size of the headers. In those scenarios in which the IPv6 header chain is unusually long and packets are fragmented, or scenarios in which the fragment size is very small, the first fragment of a packet may fail to include the entire IPv6 header chain. This document discusses the interoperability and security problems of such traffic, and updates [RFC 2460](#) such that all IPv6 packets are required to contain the entire IPv6 header chain within the 'minimum IPv6 MTU' (1280) bytes of the packet.

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 [RFC 2119](#) [[RFC2119](#)].



## **2.   Interoperability Implications of Oversized IPv6 Header Chains**

Some transition technologies, such as NAT64 [[RFC6146](#)], may need to have access to the entire IPv6 header chain in order to associate an incoming IPv6 packet with an ongoing "session".

For instance, [Section 3.4 of \[RFC6146\]](#) states that "The NAT64 MAY require that the UDP, TCP, or ICMP header be completely contained within the fragment that contains fragment offset equal to zero".

Failure to include the entire IPv6 header chain in the first-fragment may cause the translation function to fail, with the corresponding packets being dropped.



### **3. Forwarding Implications of Oversized IPv6 Header Chains**

A lot of the switches and Routers in the internet do hardware based forwarding. To be able to achieve a level of throughput, there is a fixed maximum number of clock cycles dedicated to each packet. However with the use of unlimited options and header interleaving, larger packets with a lot of interleaving have to be forwarded to the software. It is for this reason that the maximum size of valid packets with interleaved headers needs to be limited.



#### **4. Security Implications of Oversized IPv6 Header Chains**

Most firewalls enforce their filtering policy based on the following parameters:

- o Source IP address
- o Destination IP address
- o Protocol type
- o Source port number
- o Destination port number

Some firewalls reassemble fragmented packets before applying a filtering policy, and thus always have the aforementioned information available when deciding whether to allow or block a packet. However, other stateless firewalls (generally prevalent on small/ home office equipment) do not reassemble fragmented traffic, and hence have to enforce their filtering policy based on the information contained in the received fragment, as opposed to the information contained in the reassembled datagram.

When presented with fragmented traffic, many of such firewalls typically enforce their policy only on the first fragment of a packet, based on the assumption that if the first fragment is dropped, reassembly of the corresponding datagram will fail, and thus such datagram will be effectively blocked. However, if the first fragment fails to include the entire IPv6 header chain, they may have no option other than "blindly" allowing or blocking the corresponding fragment. If they blindly allow the packet, then the firewall can be easily circumvented by intentionally sending fragmented packets that fail to include the entire IPv6 header chain in the first fragment. On the other hand, first-fragments that fail to include the entire IPv6 header chain have never been formally deprecated and thus, in theory, might be legitimately generated.



## **5.   Updating [RFC 2460](#)**

All IPv6 packets MUST contain the entire IPv6 header chain within the first 1280 bytes of the packet. If a packet is fragmented, the first fragment of the packet (i.e., that with a Fragment Offset of 0) must contain the entire IPv6 header chain within the first 1280 bytes.

## **6.   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.

## **7.   Security Considerations**

This document describes the interoperability and security implications of IPv6 packets or first-fragments that fail to include the entire IPv6 header chain. The security implications include the possibility of an attacker evading network security controls such as firewalls and Network Intrusion Detection Systems (NIDS) [[CPNI-IPv6](#)].

This document updates [RFC 2460](#) such that those packets are forbidden, thus preventing the aforementioned issues.

## **8. Acknowledgements**

The authors would like to thank (in alphabetical order) XX for providing valuable comments on earlier versions of this document.

## **9.    References**

### **9.1.    Normative References**

- [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2460]   Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.

### **9.2.    Informative References**

- [RFC6146]   Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", [RFC 6146](#), April 2011.
- [CPNI-IPv6]   Gont, F., "Security Assessment of the Internet Protocol version 6 (IPv6)", UK Centre for the Protection of National Infrastructure, (available on request).





**Appendix A.**    **Changes from previous versions of the document (to be removed by the RFC Editor before publication of this document as a RFC**

**A.1.**    **Changes from [draft-manral-6man-tiny-fragments-issues-00](#)**

- o    The I-D was largely re-written.
- o    The current I-D notes that the problem lies in packets (or first-fragments) missing the entire IPv6 header chain, rather than on the (small) size of the fragments.

Authors' Addresses

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

Phone: +54 11 4650 8472  
Email: fgont@si6networks.com  
URI: <http://www.si6networks.com>

Vishwas Manral  
Hewlett-Packard Corp.  
191111 Pruneridge Ave.  
Cupertino, CA 95014  
US

Phone: 408-447-1497  
Email: vishwas.manral@hp.com

