Network Working Group
Internet-Draft
Expires: February 2, 2014

M. Andrews
ISC
Aug 2013

IPv6 Stateless Fragmentation Identification Options
draft-andrews-6man-fragopt-00.txt

Abstract

Fragmented IPv6 packets are often dropped because there is no way to identify whether a fragment matches a otherwise permitted packet as the L4 header information is not available on all the fragments.

The document defines hop-by-hop options that can be used to supply the missing information in non initial fragments.

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 2, 2014.

Copyright Notice

Table of Contents

1. Introduction

Fragmented IPv6 packets are often dropped because there is no way to identify whether a fragment matches a otherwise permitted packet as the L4 header information is not available on all the fragments.

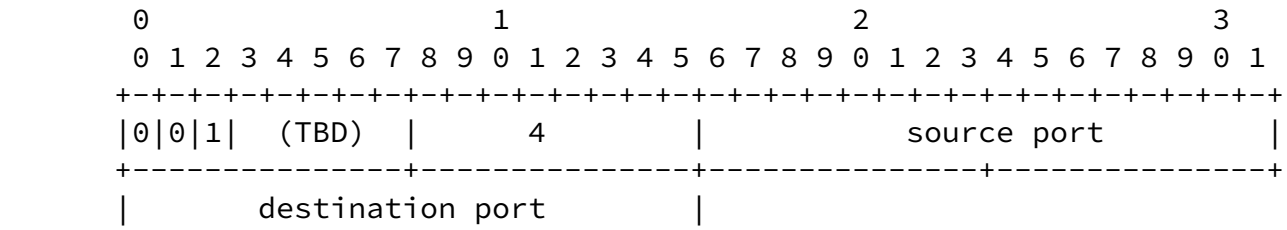
The document defines hop-by-hop options that can be used to supply the missing information in non initial fragments.

The informtion required differs depending upon the L4 packet. For TCP and UDP the source and destination ports are needed. For ICMP the type of ICMP packet is needed.

These options are expected to be used by middle boxes (firewalls and loadbalancers) and end nodes.

2. TCP and UDP Fragements

For TCP and UDP a skippable hop-by-hop option [RFC2460] (for backwards compatibilty) containing the source and destination ports from the TCP and UDP headers is needed. To permit the use of NATs, however undesired, the option contents are marked changable enroute. The option code has nmemonic PORTS and value (TBD) and is added to all fragments of UDP and TCP packets when they are fragmented. By adding the option to all fragments you reduce the amount of fragmentation reassembly failures that would result if you only added the option to non-initial fragments and were dropping non-initial fragments without this option.



3. Security Considerations

The use of these options will expose nodes to more fragmention based attacks and potentually more traffic which will ultimately be dropped if a attacker can guess which option values will be permitted.

With the exception of the fragmentation based attacks, permitting fragments with these options is no worse that permitting multiple unfragmented packets based in the same parameters.

4. Normative References

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

Author's Address

M. Andrews
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
US

Email: marka@isc.org