IPv6 Hop-by-Hop Options Processing Procedures

<draft-hinden-6man-hbh-processing-01>

Bob Hinden
Gorry Fairhurst

November 2021
IETF112

Introduction

- Hop-by-Hop Options are not working in the Internet:
  - Very common for routers on a path to drop packets with HBH Option headers.
  - We need to do something different if we expect to use HBH Options in the future.
- This is a proposal to modify Hop-by-Hop Option Processing.

Background

In the first IPv6 specification:

- HBH Processing was required for all nodes
- Issues were:
  - Inability to process at wire speed in hardware
  - Packets with HBH options sent to the ”Slow Path” would degrade router performance and could be used as a DOS attack
  - Packets could contain multiple HBH options, making the problem worse

Background (continued)

In the current IPv6 Specification (RFC8200):

- HBH processing is only required <u>if router configured.</u>
- This essentially documented current operational behavior.
- *It did not improve the situation!*

Motivation

- **Still not practical for HBH Options to be used widely:**
  - Paths commonly *drop all packets with HBH options;*
  - *Multiple HBH options* in a packet make problem worse;
  - Any mechanism that can be used externally to force packets into the “Slow Path” can be exploited as a *DOS attack.*
- **Our goal is to redefine procedures to make HBH options practical**:
  - This likely won’t work on all paths;
  - Methods can be designed that would still benefit from incremental support where provided.

Proposal Summary (Changes to RFC8200)

- First HBH option MUST be processed in “Fast Path” **
  - Additional HBH options MAY be processed if configured to do so.
- Nodes creating packets with HBH options SHOULD include a single HBH option;
  - MAY include more based on local configuration.
- If there are more than one HBH options, a node MAY skip the rest without examining them (not processed or verified).
- Nodes unable to process an HBH option in the “Fast Path” MUST treat it as an unrecognized option.

** Router Alert is the exception

Proposal Summary (Changes to RFC8200) Continued…

- If HBH Option not recognized, change processing of high-order 2 bits of Option Type “10” and “11” to:

10 **discard the packet** and, regardless of whether or not the packet's Destination Address was a multicast address, **MAY send an ICMP Parameter Problem**, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 **discard the packet** and, only if the packet's Destination Address was not a multicast address, **MAY send an ICMP Parameter Problem**, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

Proposal Summary (Router Alert) Continued….

- **Router Alert**
  - Node SHOULD verify that the Router Alert option contains a supported protocol.
  - Verified packets SHOULD be sent to “Slow Path” for processing.
  - Nodes configured to support Router Alert options MUST protect itself from “Slow Path” infrastructure attacks.

New Hop-by-Hop Options

- New HBH Options should be designed for ”Fast Path” processing:
  - Straight forward to process;
  - Fixed size in 8-octet units, not variable size;
  - Limit the amount of data that needs to be processed in “Fast Path”.

Issues Raised

- Fast/Slow Path, Control/Forwarding Plane terminology
- Is it:
  - Node MUST examine at least one HBH Option in ”Fast Path”, or
  - If a node is configured to process HBH options, Node MUST examine….
- Should there be any “Slow Path” HBH processing (i.e., Router Alert)?

Issues Raised (2)

- Relationship with <draft-ietf-opsec-ipv6-eh-filtering>
- Can existing deployed equipment implement this proposal?
- A HBH option that needs to be in every packet in a flow
  - If first option, any later options might not be supported
  - If second, then the option itself may not be supported

Issues Raised
(Not specific to this proposal)

- Any application or service that uses HBH options needs to work even if no packets with HBH Options are delivered.
- Overall limits on number and size of Extension Headers?

Next Steps

- Thanks for all the feedback and editorial comments!

- Authors think 6MAN should adopt as a w.g. document:
  - There appears to be interest in working on improving IPv6 HBH Processing.
  - We work through issues on mailing list (authors very open to better suggestions).

- If there isn't interest in improving IPv6 HBH processing, should it be deprecated?
  - … Current state isn't tenable.

QUESTIONS / COMMENTS?