IPv6 Hop-by-Hop Options Processing Procedures

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

Bob Hinden
Gorry Fairhurst

July 2021
IETF111
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
Terminology*

- Fast Path
  - Hardware, NP, or ASIC packet processing
  - Usual router processing for most packets
  - Also called the “Forwarding Plane”

- Slow Path
  - Software packet processing
  - Router path for special processing
  - Also called “Control Plane”

* Other terms would also be acceptable
Background

- HBH Processing in first IPv6 specification was required for all nodes, issues were:
  - Inability to process at wire speed in hardware
  - Packets with HBH options sent to "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)

- Current IPv6 Specification (RFC8200)
  - Changed this requirement to only require HBH processing if router configured to do so.
  - This essentially documented current operational behavior.
- Did not improve the situation
Motivation

- HBH Options still not practical to be used widely
  - Paths commonly drop all packets with HBH options
  - Multiple HBH options in the same 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
- Goal is to redefine HBH procedures to make HBH options practical
  - This likely won’t work on all paths, but methods can be designed that would still benefit from incremental support.
Changes from -00 draft

- Expanded terminology section to include Forwarding Plane and Control Plane.
- Changed draft that only one HBH Option MUST be processed and additional HBH Options MAY be processed based on local configuration.
- Clarified that all HBH options (with one exception) must be processed on the Fast Path.
- Kept the Router Alert options as the single exception for Slow Path processing.
- Rewrote and expanded section on New Hop-by-Hop Options.
- Removed requirement for HBH Option size and alignment.
- Removed sections evaluating currently defined HBH Options.
- Added content to the Security Considerations section.
- Added people to the acknowledgements section.
- Numerous editorial changes
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 that can not 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 - 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?