Operational Implications of IPv6 Packets with Extension Headers
(draft-gont-v6ops-ipv6-ehs-packet-drops)

Fernando Gont
Nick Hilliard
Gert Doering
Will (Shucheng) Liu
Warren Kumari

IETF 95
Buenos Aires, Argentina. April 3-8, 2016
Overview of this document

• Provides an overview of the operational and security implications of IPv6 EHs

• Documents why some operators intentionally drop packets that contain IPv6 EHs, as in:

  "Solicit input from network operators and users to identify operational issues with the IPv6 Internet"

  "document IPv6 operational experience"

• Means to suggest an action plan that could help improve the current state of affairs
Operational Implications (I)

- Some middleboxes and intermediate systems need to obtain layer-4 information
- Requirement to process layer-4 information:
  - Enforcing infrastructure ACLs
  - DDoS Management and Customer Requests for Filtering
  - ECMP and Hash-based Load-Sharing
- When they are unable to obtain that information, they may drop the corresponding packet
- That may happen due to Packet Forwarding Engine Constraints
Operational Implications (II)

- Route-Processor Protection
  - In some implementations, processing the EH chain may punt the packet to a software path
  - HBH Options EH proves to be particularly challenging
Operational Implications (III)

- Inability to Perform Fine-grained Filtering
  - In some implementations, processing the EH chain may punt the packet to a software path
  - HBH Options EH proves to be particularly challenging
Possible Action Plan

• Require better granularity in the specification of filters for IPv6 extension headers

• Provide advice on the filtering of IPv6 packets that contain IPv6 extension headers (as in [I-D.ietf-opsec-ipv6-eh-filtering])

• Consider enforcing a cap on the maximum length of an IPv6 EH chain (e.g., as proposed in [I-D.wkumari-long-headers])
Moving Forward

- Specific areas where this document could be improved?
- Adopt as WG document?