Operational Issues with Processing of the Hop-by-Hop Options Header

draft-ietf-v6ops-hbh-00

Shuping Peng	Huawei
Zhenbin Li	Huawei
Chongfeng Xie	China Telecom
Zhuangzhuang Qin	China Unicom
Gyan Mishra	**Verizon**

The changes we have updated

1. The title is changed to avoid the misleading towards a solution draft.
2. The purpose of this draft is further clarified in both the abstract and the introduction sections.
3. The scope of this draft is also clarified in section 2.
4. Necessary reference is added.
5. Directly quote the specifications in the existing RFCs wherever are suitable.
6. Requirements in Section 7 are updated according to the received comments but still need more work which will be conducted in the later versions.
7. Section 8 is significantly changed instead of being completely deleted since we believe the migration is also very important to consider.

The plans for the future work

1. Requirements in Section 7 still need more work which will be conducted in the later versions.
2. The migration strategy in Section 8 is very important to consider, which needs the WG work together to give recommendations.
3. New sections on other network scenarios (Enterprise or IoT etc.) are still not yet added.

The clarifications with the existing work

- The goal of RFC 9098 from a IPv6 operations and security perspective is to shed light on the issues surrounding all extension headers generalization as due to the pervasive Christmas tree issue with excessive header chaining to issues related to processing of headers in the slow path.

- Out of all the headers the one and only that has been historically the most problematic is HBH and has resulted in operators filtering HBH to avoid possible DDOS attack vector.

- This draft hones in on HBH as it is the most problematic but it is also one of the most useful for developers to build tools for operators toolbox.

- This document also provides a path forward to make HBH usable and its viability for future development of new features that can be extremely beneficial to the internet community.

Motivations of the work since the very beginning

- The HBH Options Header is a valuable container for facilitating new services
    - The hop-by-hop processing behavior is very desirable
    - New services: IOAM, Alternate Marking, PMTU, etc.
- The HBH Options Header is rarely utilized in the current operators' networks.
    - Preserve the control plane from undesired traffic
- Our main purpose is to
    - enable the HBH options header to be utilized in a safe/secure way without endanger any operation
    - ease the deployments of the new network services in a multi-vendor/operator's scenario

Modern Router Architecture

- Modern router architecture design maintains a strict separation of its control and forwarding plane

- The control plane
  - realized in software on general-purpose processors
  - vulnerable to the DoS attack

- The forwarding plane
  - realized in high-performance ASICs or NPs
  - capable of handling very high packet rates

- The interface between control and forwarding plane
  - a rate-limit mechanism is always implemented to protect the control plane against DoS attack
    - ✓ cause inconsistent packet drops
    - ✓ impact the normal IP forwarding

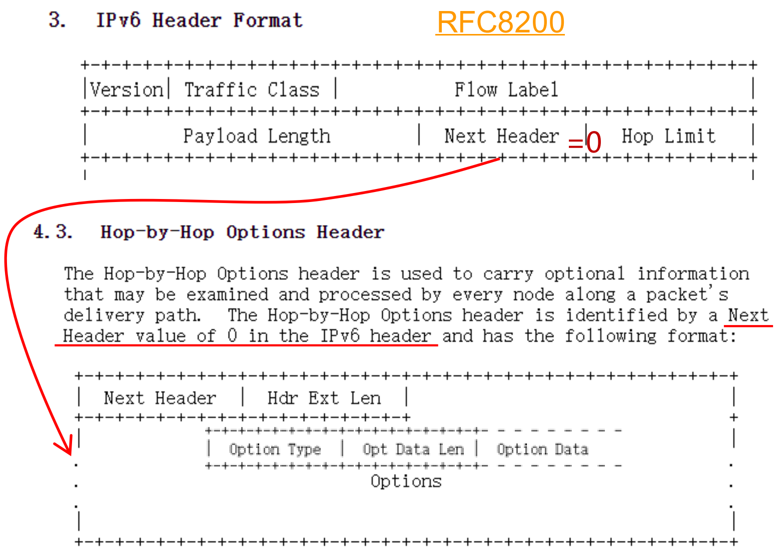
```
                   +----------------+
                   | Router Control |
                   |    Plane       |
                   +------+-+-------+
                          | |
                     Interface Z
                          | |
                   +------+-+-------+
                   |   Forwarding   |
    Interface X ==[     Plane      ]== Interface Y
                   +----------------+
```

RFC6192

Figure 1. Modern Router Architecture

Common Implementations

- The value of the Next Header field in the IPv6 header
  - the only trigger for the default processing behavior of the HBH
- Common implementations
  - Once the device receives an IPv6 packet with its Next Header field set to 0, it will be directly sent to the slow path.
  - The option type of each option will not be examined before the packet is sent to the slow path.
  - In most of the cases, such processing behavior is the default configuration and cannot be changed.
- Historical Reasons
  - HBH options were not yet well-understood
  - ASICs were not so capable as they are today
- Consequences
  - All packets that contain HBH are dispatched to the slow path
  - A risk of a DoS attack on the control plane
  - Congest the slow path, causing other critical functions to fail
  - Rate-limit causes inconsistent packet drops and impact the normal end-to-end IP forwarding of **the new services**



3. IPv6 Header Format

RFC8200

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header =0|  Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
```

4.3. Hop-by-Hop Options Header

The Hop-by-Hop Options header is used to carry optional information that may be examined and processed by every node along a packet's delivery path. The Hop-by-Hop Options header is identified by a Next Header value of 0 in the IPv6 header and has the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |  Hdr Ext Len  |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|          +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - -       |
|          |  Option Type  | Opt Data Len |  Option Data        |
.          +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - -       .
.                           Options                             .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

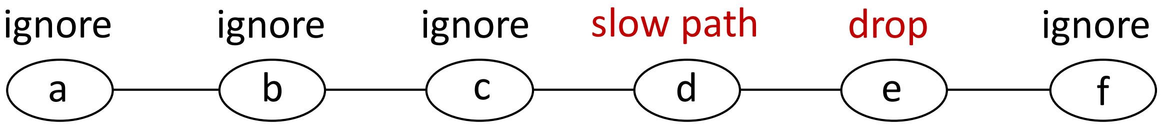
Specifications in Standards

- [RFC2460]: required that all nodes must examine and process the Hop-by-Hop Options header

- [RFC8200]: now expected that nodes along a packet's delivery path only examine and process the Hop-by-Hop Options header if explicitly configured to do so.

- [RFC8200]: the nodes may be configured to
  1. ignore the Hop-by-Hop Options header
  2. drop packets containing a Hop-by-Hop Options header
  3. assign packets containing the HBH Options header to the slow path (Common Implementation)
     - the traffic is generally rate-limited causing inconsistent packet drops

- The current situations
  - Various configurations and operations in operators’ networks
  - Unable to support the service deployment
  - Disturbs the normal IP forwarding



  - Very often, the default configuration is embedded and cannot be changed or reconfigured.
  - The deployment in the network will not be changed within one day.

Operators' typical processing

- Many operators deployed Access Control Lists (ACLs) that discard all packets containing HBH Options

- [RFC6564]
  - Reports from the field indicating that some IP routers deployed within the global Internet are configured either to ignore or to drop packets having a hop-by-hop header.
- [RFC7872]
  - Many network operators perceive HBH Options to be a breach of the separation between the forwarding and control planes.
  - Several network operators configured their nodes so to discard all packets containing the HBH, while others configured nodes to forward the packet but to ignore the HBH Options.
- [RFC7045]
  - HBH options are not handled by many high-speed routers
  - or are processed only on a slow path

- Consequences
  - [RFC8200]: New hop-by-hop options are not recommended
  - The usability of HBH options is severely limited

Shall we break the endless loop?

- Endless Loop:

  -> An implementation choice caused HBH to become a DoS vector

  -> Because HBH is a DoS vector, network operators deployed ACLs that discard packets containing HBH

  -> Because network operators deployed ACLs that discard packets containing HBH, network designers stopped defining new HBH Options

  -> Because network designers stopped defining new HBH Options, the community was not motivated to fix the implementation choice that causes HBH to become a DoS vector

- We would like the community to
  - break the loop
  - fix the problem
  - make HBH actually being utilized in operators' networks
  - allow a better leverage of the HBH capability

We are collecting the requirements and derive the reasonable solution

- draft-ietf-v6ops-hbh is collecting the requirements and provides migration strategy
  - The HBH options header SHOULD NOT become a possible DDoS Vector. Therefore, the control plane MUST be preserved from unwanted incoming traffic due to HBH header present in the packet.
  - HBH options SHOULD be designed in a manner so that they don't reduce the probability of packet delivery.
  - HBH processing MUST be efficient. That is, it MUST be possible to produce implementations that perform well at a reasonable cost without endanger the security of the router.
  - The Router Alert Option MUST NOT impact the processing of other HBH options that should be processed more quickly.
  - HBH Options MAY influence how a packet is forwarded. However, with the exception of the Router Alert Option, an HBH Option MUST NOT cause control plane state to be created, modified or destroyed on the processing node. As per [RFC6398], protocol developers SHOULD avoid future use of the Router Alert Option.
  - More requirements are to be added.
- draft-hinden-6man-hbh-processing-01 is building a solution
  - More details to be presented

Thank you!