

Processing of the Hop-by-Hop Options Header

draft-peng-v6ops-hbh-00

Shuping Peng Huawei

Zhenbin Li Huawei

Chongfeng Xie China Telecom

Zhuangzhuang Qin China Unicom

Motivations

- 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

Some Examples of New Services

- **In-situ OAM with IPv6 encapsulation** [I-D.ietf-ippm-ioam-ipv6-options]
 - Used to enhance diagnostics of IPv6 networks and complements other mechanisms
 - The IOAM data fields are encapsulated in the HBH Options header, i.e., the IOAM per hop.
- **Alternate Marking Method** [I-D.ietf-6man-ipv6-alt-mark]
 - Used as the passive performance measurement tool in an IPv6 domain.
 - The AltMark Option is to encode alternate marking technique and HBH Options Header is considered.
- **The Minimum Path MTU Hop-by-Hop Option** [I-D.ietf-6man-mtu-option]
 - Used to record the minimum Path MTU along the forward path in environments like DCs and on paths between DCs as well as other environments including the general Internet.

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**

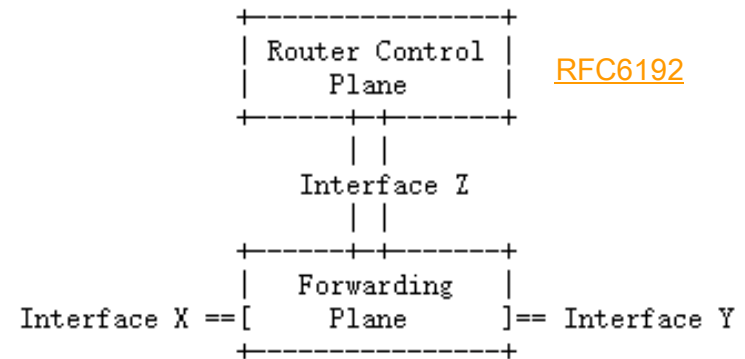


Figure 1. Modern Router Architecture

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

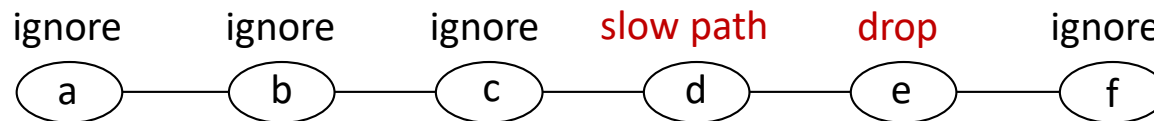
4.3. Hop-by-Hop Options Header

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 RFC8200

- [[RFC8200](#)]: only examine and process the HBH Options header if explicitly configured to do so
- However, there is no explicit specification or recommendation of a given configuration or rule to implement
- [[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)
 1. the traffic is generally rate-limited causing inconsistent packet drops
- This relaxation in the specification actually caused the problems
 - 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

The desired processing behavior

- **Control pane should be protected from undesired traffic**
 - The HBH options that are not supposed to be processed by the control plane should not be sent to the control plane, potentially causing the DoS attack
 - The HBH options header should not be directly sent to the control plane once the packets are received since these options may not aim for the control plane
- **Better to separate the two types of options** that are supposed to be processed by the control plane or by the forwarding plane, respectively
 - The desired processing behaviors for the two types of options are different
 - The options aimed for the control plane are better not to consume the forwarding plane resources
 - For the current common implementation, all the options are sent to the control plane
 - There is no simple way to differentiate the two types of options except inspecting each option type
- The new deployments should be **compatible** with the existing deployments
 - Since default configuration of some devices cannot be changed or reconfigured
 - The update of the entire network cannot be done within one day

Thank you!

One proposal in draft-li-6man-hbh-fwd-hdr

- The HBH Options actually contain information for the use of the forwarding plane and the control plane of the nodes, respectively.
- They can be categorized into HBH Forwarding Options and HBH Control Options [I-D.li-6man-hbh-fwd-hdr].
- It is suggested to separate the two types of HBH options and carry them in different packets since generally they serve for different purposes and require different processing procedures on a node.
- The packets carrying the HBH Forwarding Options are supposed to be maintained in the forwarding plane rather than being directly sent up to the control plane. While the packets carrying the HBH Control Options are supposed to be sent to the control plane.
- If the IPv6 extension header including the HBH options header of a packet cannot be recognized by the node, or the option in the HBH header is unknown to the node, and the node is not the destination of the packet, the packet should not be dropped or sent to the control plane, rather this unrecognized extension header should be skipped and the rest of the packet should be processed.

Corresponding migration strategies

- In order to achieve the desired processing behavior of the HBH options header and facilitate the ever-emerging new services to be deployed in operators' networks across multiple vendors' devices, the migration can happen in three parts as described below:
- 1. The source of the HBH options header encapsulation.
 - The information to be carried in the HBH options header needs to be first categorized and encapsulated into either control options or forwarding options, and then encapsulated in different packets.
- 2. The nodes within the network.
 - The nodes are updated to the proposed behavior introduced in the previous section.
- 3. The edge node of the network.
 - The edge node should check whether the packet contains a HBH header with control or forwarding option. Packet with a control option may still be filtered and dropped while packets with forwarding option should be allowed by the ACL.
 - If it is certain that there is no harm that can be introduced by the HBH options to the nodes and the services, they can also be allowed.
- Note: During the migration stage, the nodes that are not yet updated will stay with their existing configurations.