



IPv6 Extension headers and their implications for Network and security operations.

Logan Velvindron

IPv6 extension headers and their implications for network & security operations.

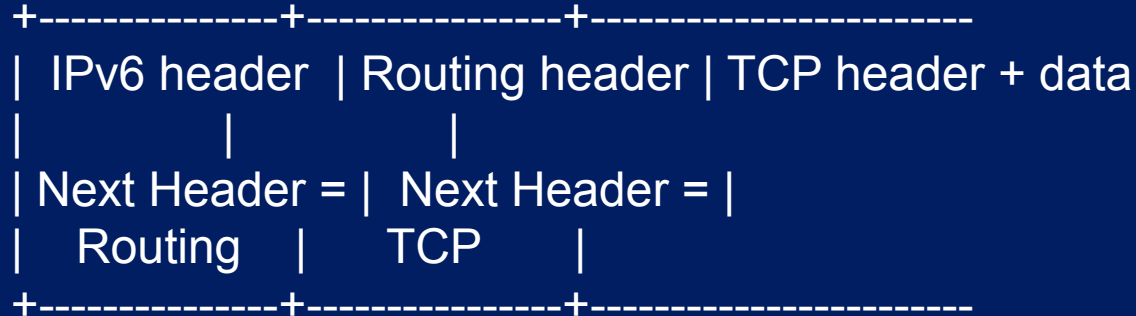
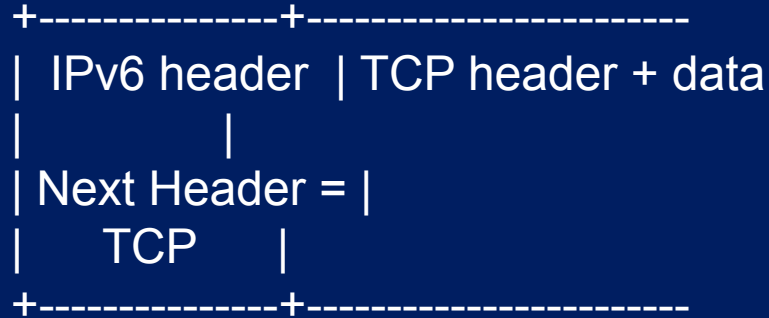
- IPv6 has been around for a long time.
- Reference implementations: KAME (*BSD) and USAGI.

IPv6 Extension headers

RFC 8200:

In IPv6, optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There is a small number of such extension headers, each one identified by a distinct Next Header value.

IPv6 Extension headers



What can go wrong ?

IPv6 extension headers in practice.

- **CISCO IOS:**

A vulnerability in the implementation of the virtual fragmentation reassembly (VFR) feature for IP version 6 (IPv6) in Cisco IOS Software could allow an unauthenticated, remote attacker to cause an affected device to hang or reload, resulting in a denial of service (DoS) condition.

- **FreeBSD:**

IPv6 is a network layer supporting Hop-by-Hop options, which can be sent by applications via the socket API. The memory management for packet handling is done using mbufs.

Current IETF work

- Raise awareness about the operational and security implications of IPv6 Extension Headers specified in [RFC8200], and present reasons why some networks resort to intentionally dropping packets containing IPv6 Extension Headers.
- Highlight areas where current IPv6 support by networking devices may be sub-optimal, such that the aforementioned support is improved.
- Highlight operational issues associated with IPv6 extension headers, such that those issues are considered in IETF standardization efforts.
- <https://datatracker.ietf.org/doc/html/draft-ietf-v6ops-ipv6-ehs-packet-drops-06>

Read further

<https://datatracker.ietf.org/doc/html/draft-ietf-v6ops-ipv6-ehs-packet-drops-06>

Ask your vendor if their features are reliant on ipv6 extension headers ?

1. <https://datatracker.ietf.org/doc/html/draft-li-6man-e2e-ietf-network-slicing>
2. This document defines the mechanism of encapsulating the end-to-end network slice related identifiers in IPv6 packet, which is aligned with the framework as defined in draft-li-teas-e2e-ietf-network-slicing.

What are the benefits of using an IPv6 extension header to carry the meta data? In contrast to embedding it in a tunnel header (like what GRE, Geneve, etc, etc does).



— AFRICA —
INTERNET
— SUMMIT'21 —
ONLINE
31 MAY - 4 JUNE 2021

**Thank you for your
interest in AIS'21**