

IPv6 Extension Headers in the Real World

(draft-gont-v6ops-ipv6-ehs-in-real-world-01)

**Fernando Gont
Jen Linkova
Tim Chown
Will Liu**

**IETF 91
Honolulu, Hawaii, USA. November 9-14, 2014**

Problem Statement

- IPv6 packets with extension headers are widely dropped in the public Internet
- This has implications on protocols:
 - Existing: what should we do about them?
 - Future: they probably need a fall-back mechanism
- But also on operations:
 - How to troubleshoot issues arising from filtering
 - Security implications of such filtering

Goals of our Internet-Draft

- Agree on the problem statement
- Provide real-world data regarding support of IPv6 EHs in the real world
- Summarize the issues associated with IPv6 EHs (performance, security, etc.)
- Send a signal to protocol-development/maintenance WGs about possible future work
- Discuss the security implications of such filtering, and discusses possible workarounds

Filtering of packets with IPv6 EHs

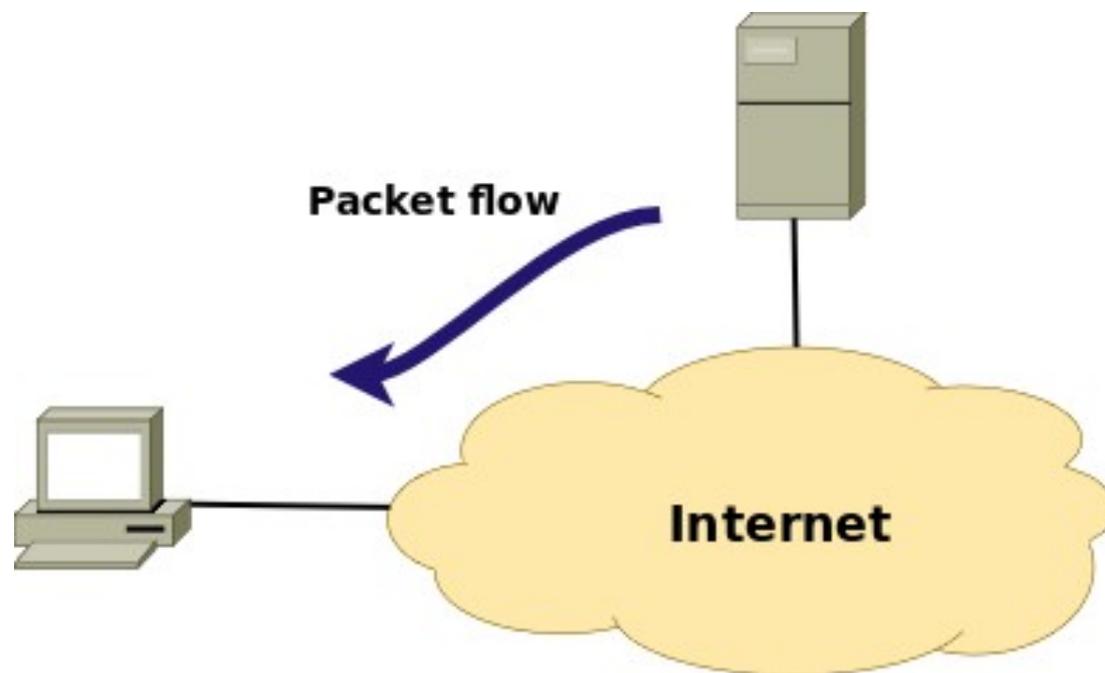
- Approximate drop rates for Internet servers:
 - > 10% for Destination Options
 - > 40% for Hop-by-Hop Options
 - > 25% for fragmented traffic
- Location of dropping nodes:
 - 20%-60% of drops occur at an AS other than the Destination AS

General Implications of IPv6 EHs

- Performance
- Security
- Reliability

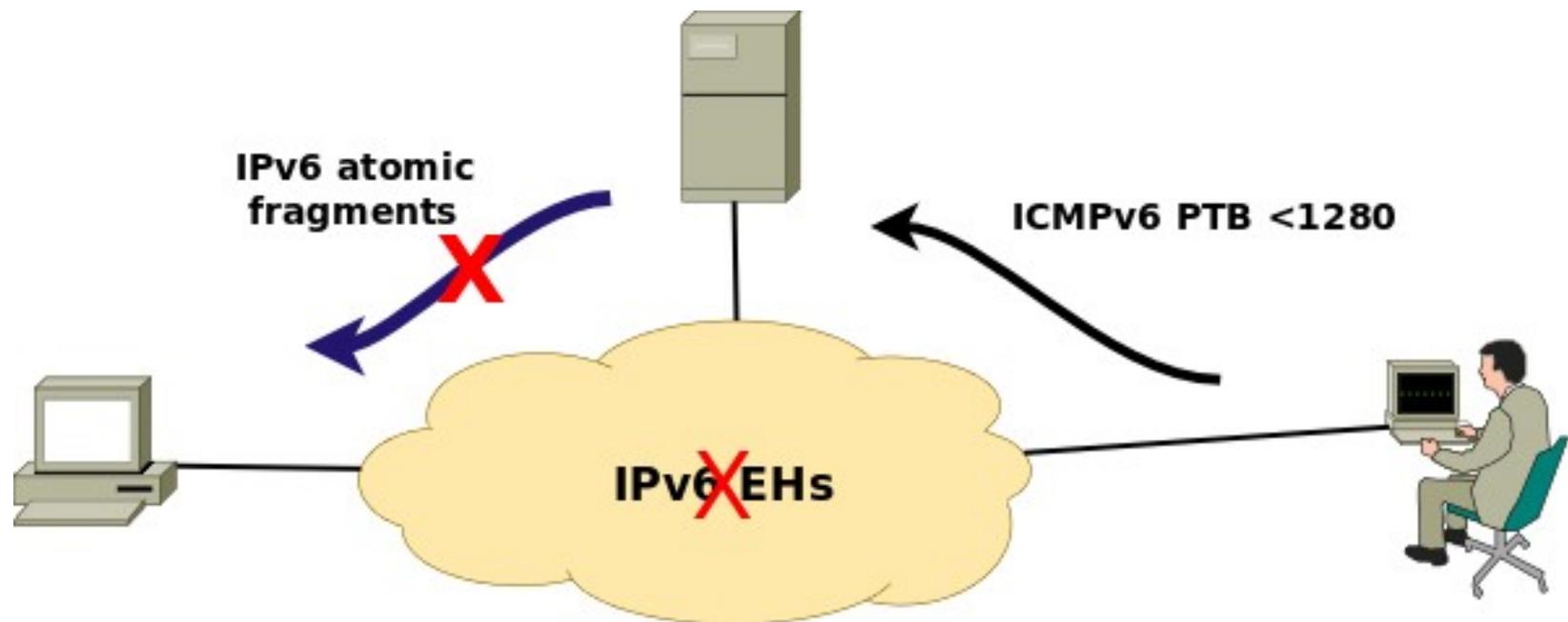
Sec. Impl. of Widespread Filtering

- Client communicates with a server



Sec. Impl. of Widespread Filtering

- Attacking client-server communications



Specific Attack scenario: BGP

- Say:
 - We have two BGP peers
 - They drop IPv6 fragments “for security reasons”
 - But they do process ICMPv6 PTBs
- Attack:
 - Fire an ICMPv6 PTB <1280 (probably one in each direction)
- Outcome:
 - Packets get dropped (despite TCP MD5, IPsec, etc.)
 - Denial of Service

Feedback to other WGs

- Essentially:
 - “If your protocol relies on IPv6 EHs, it will probably break if deployed on the Internet”
- New protocols:
 - Incorporate a fall-back mechanism
- Existing protocols:
 - Evaluate whether modifications are warranted

Moving Forward

- Question heard at yesterday's IEPG meeting:
 - “We have discussed the topic at four different IEPG meetings... why doesn't the IETF act on the topic?”
- **Adopt as a v6ops wg item?**