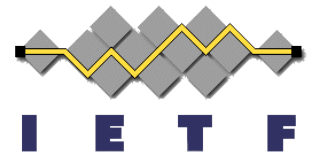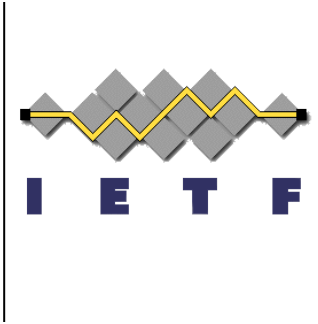# IPv6 Hop-by-Hop Header Handling
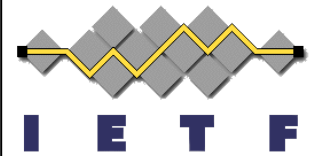
draft-baker-6man-hbh-header-handling

I E T F

# Issues: HBH header an attack vector

- RFC 2460 unclarity on requirements language (RFC 2119 not used)
- RFC 7045 acceptance of guidance regarding HBH punt to software resulting from that unclarity and difficulty of implementation at speed
- ietf-v6ops-ipv6-ehs-in-real-world and other observations on extension headers

# Issues: OAM requirements

- It would be nice if we could do something akin to RH0 routing, and verify the path actually taken
  - See Segment Routing
- It might be nice to pick up network data en route (details TBD)

Section 2.1 recommendation
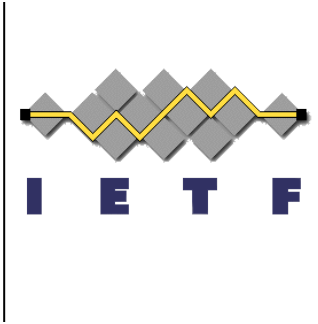
- The presence of HBH options SHOULD not slow forwarding rate.

- Skipable HBH options that have no effect in a given router MUST be skipped

  - Only punt to a software path (Router Alert Option) if configured for RSVP operation
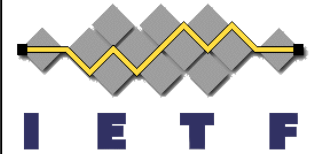
Section 2.2: changing options in transit
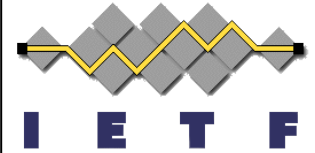
- Change-in-place supported by RFC 2460
- This allows us to capture OAM information in transit

- But – what if the originating host was unaware that the network wanted to perform an OAM measurement?

# Section 2.3: Adding headers or options in transit

- To perform an OAM measurement, we would like to be able to add a HBH option, and if necessary a HBH header, to a datagram being forwarded

- In some use cases, it may be appropriate or necessary to remove the header and/or option in the last router prior to delivery

- Discussed in section 2.4

Section 2.4: Security Extension Header
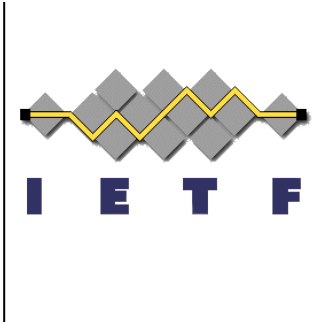
- There are some interactions with AH and ESP when playing with such options:

  - The integrity check may fail, especially if a header was added or its length is changed.

  - To avoid this, IPv6 header must be restored to original condition before final delivery
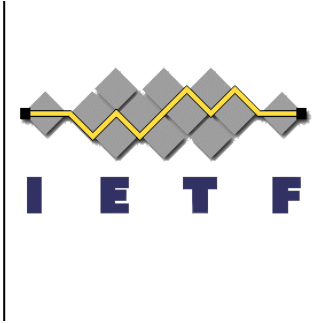
Section 3: interoperation

- There are operational issues with this, which need to be understood by the operator using the OAM capability.

- Such OAM capabilities may be usable only among consenting networks