



# IPv6 Segment Routing Security Considerations

draft-vyncke-6man-segment-routing-security-02

**Authors and contributors:**

Eric Vyncke ([evyncke@cisco.com](mailto:evyncke@cisco.com))

Stefano Previdi ([sprevidi@cisco.com](mailto:sprevidi@cisco.com))

David Lebrun ([david.lebrun@uclouvain.be](mailto:david.lebrun@uclouvain.be))

# Changes in -02

- Segment Routing Header (SRH) has changed in -06
  - Need to update text
- Reworded a lot of text
  - RFC 5095
  - Clearer on ‘within a single ISP network’
  - Not enabled by default
  - ICMP generation
  - BCP-38
  - Added David as co-author (thanks for HMAC fixes RFC 2104)

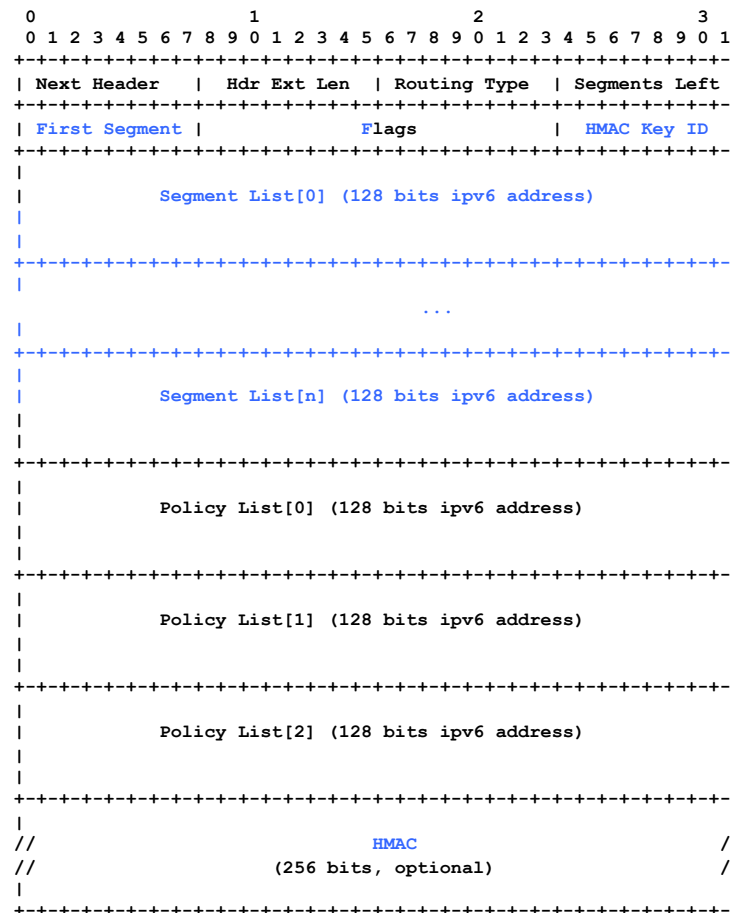
# What RFC 5095 Says

*“The severity of this threat is considered to be sufficient to warrant deprecation of RHO entirely. A side effect is that this also eliminates benign RHO use-cases; however, such applications may be facilitated by future Routing Header specifications.”*

```
J. Abley  
Afilias  
P. Savola  
CSC/FUNET  
G. Neville-Neil  
Neville-Neil Consulting  
  
December 2007  
  
Deprecation of Type 0 Routing Headers in IPv6  
RFC 5095
```

# SRH: HMAC Coverage

- **Source Address (not shown):** as it is immutable and to prevent SR service stealing
- **First Segment:** offset in the SRH, not including the first 8 octets and expressed in 16-octet units, pointing to the last element of the Segment List
- **Flags:**
  - bit-0: cleanup
  - bit-1: rerouted packet
  - bits 2 and 3: reserved
  - bits 4 to 15: policy flags
- **HMAC Key ID:**
- **Segment List[n]:** all segments



# Segment Routing Security

- Addresses concerns of RFC 5095
  - HMAC field to be used at ingress of a SR domain in order to validate/authorize the SRH
  - Inside SR domain, each node trust its brothers (RPL/RH-3 model)
- HMAC requires a shared secret (controller & SR-domain ingress routers)
  - Outside of current discussions
  - Pretty much similar to BGP session security or OSPFv3 security

# Questions?

Ask: Becoming a WG document?

SPRING are WG doc

Working implementation [S](#)

# Thanks!