EVPN First Hop Security

IETF 121, Nov 2024
Dublin

https://datatracker.ietf.org/doc/html/draft-sajassi-bess-evpn-first-hop-security-03

Ali Sajassi (Cisco),
Lukas Krattiger (Cisco),
Krishna Ananthamurthy (Cisco),
Jorge Rabadan (Nokia)
Wen Lin (Juniper)

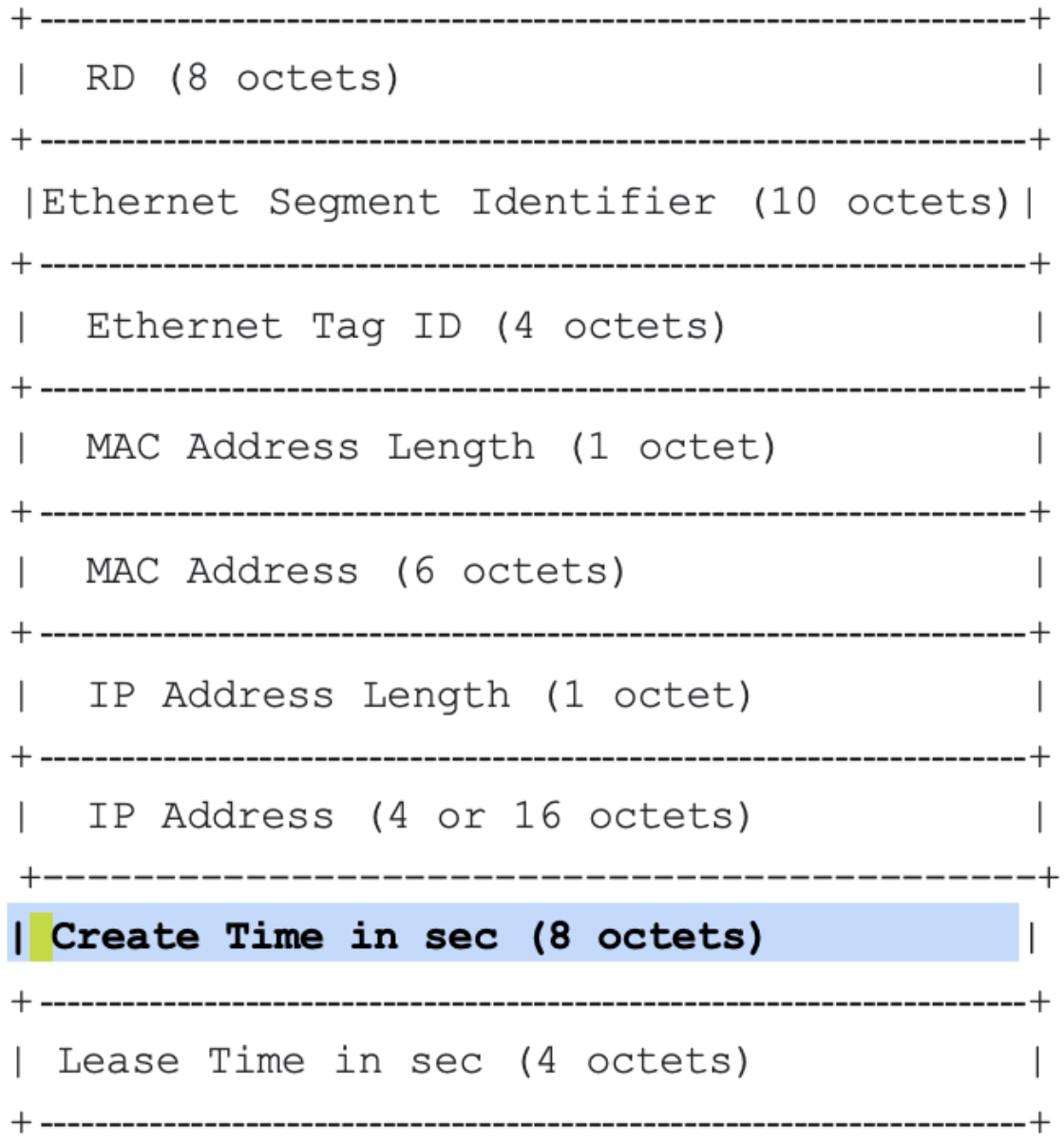
Recap

- Presented in IETF-116, IETF-117 & IETF-119
- Background:
  - DHCP Snoop Database
    - Stores valid IPv4/IPv6 MAC bindings by snooping DHCP messages
  - First Hop Security (FHS)
    - ARP Inspection, ND Inspection and IPv4/IPv6 Source Guard make use of DHCP bindings
  - FHS is widely deployed on access switches without standard based multihoming and host mobility

What is EVPN First Hop Security

- DHCP snoop database **sync between ES peers** for multihomed hosts.
- DHCP snoop database distribution with EVPN peers for mobility.
- Defines DHCP Sync Route.
- Address both bridge and IRB services.

DHCP Snoop Route Format



Next Step

- Draft is stable from last few IETFs
- Requesting WG adoption.

Thank You!