# IPv6 Performance and Diagnostic Metrics v2 (PDMv2) Destination Option

draft-elkins-ippm-encrypted-pdmv2-04

Nalini Elkins: Inside Products: nalini.elkins@insidethestack.com

Michael Ackermann: BCBS Michigan: mackermann@bcbsm.com

Ameya Deshpande: NITK, Surathkal: ameyanrd@gmail.com

Tommaso Pecorella: University of Florence: tommaso.pecorella@unifi.it

Adnan Rashid: Politecnico di Bari : adnan.rashid@poliba.it

# Agenda

- We have done the simplification discussed in IETF116.
- If WG agrees, then we will discuss with SECDIR to get a review.

# The fields in PDMv2 : S-S

- SCALEDTLR: Scale for Delta Time Last Received
- SCALEDTLS: Scale for Delta Time Last Sent
- GLOBALPTR: Global Pointer
- PSNTP: Packet Sequence Number This Packet
- PSNLR: Packet Sequence Number Last Received
- DELTATLR: Delta Time Last Received
- DELTATLS: Delta Time Last Sent

# Only ONE needs to be decrypted by other end

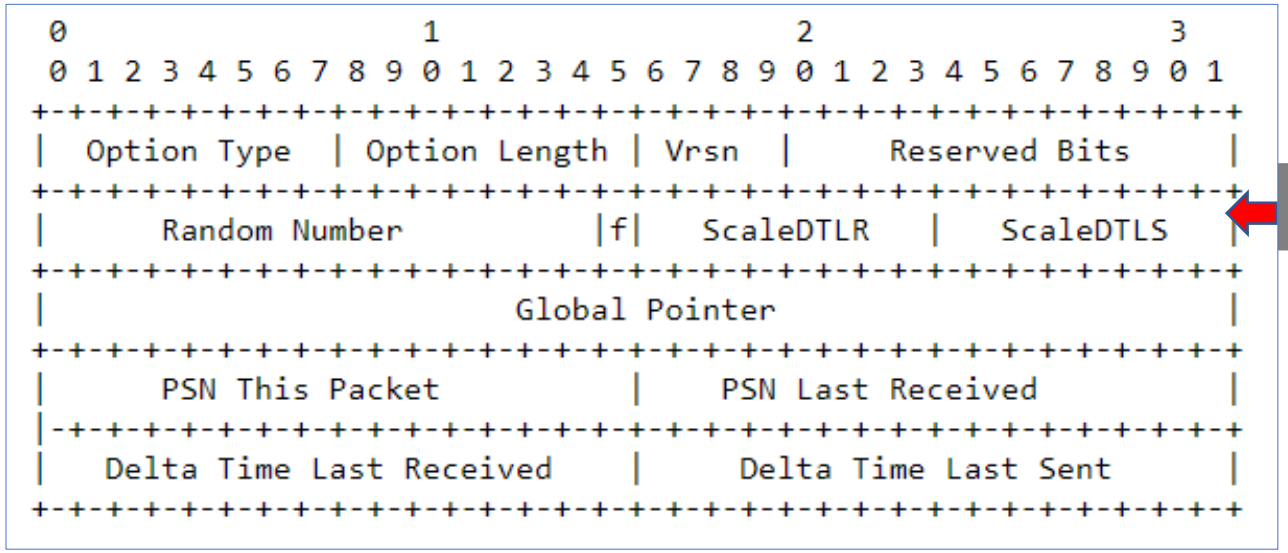
- SCALEDTLR: Scale for Delta Time Last Received
- SCALEDTLS: Scale for Delta Time Last Sent
- GLOBALPTR: Global Pointer
- PSNTP: Packet Sequence Number This Packet
- **PSNLR: Packet Sequence Number Last Received**
- DELTATLR: Delta Time Last Received
- DELTATLS: Delta Time Last Sent

**The PSNLR field is the PSNTP of the last packet received from the other side.**

**That is the ONLY reason that the other end (client or server, needs to decrypt the packet at all.**

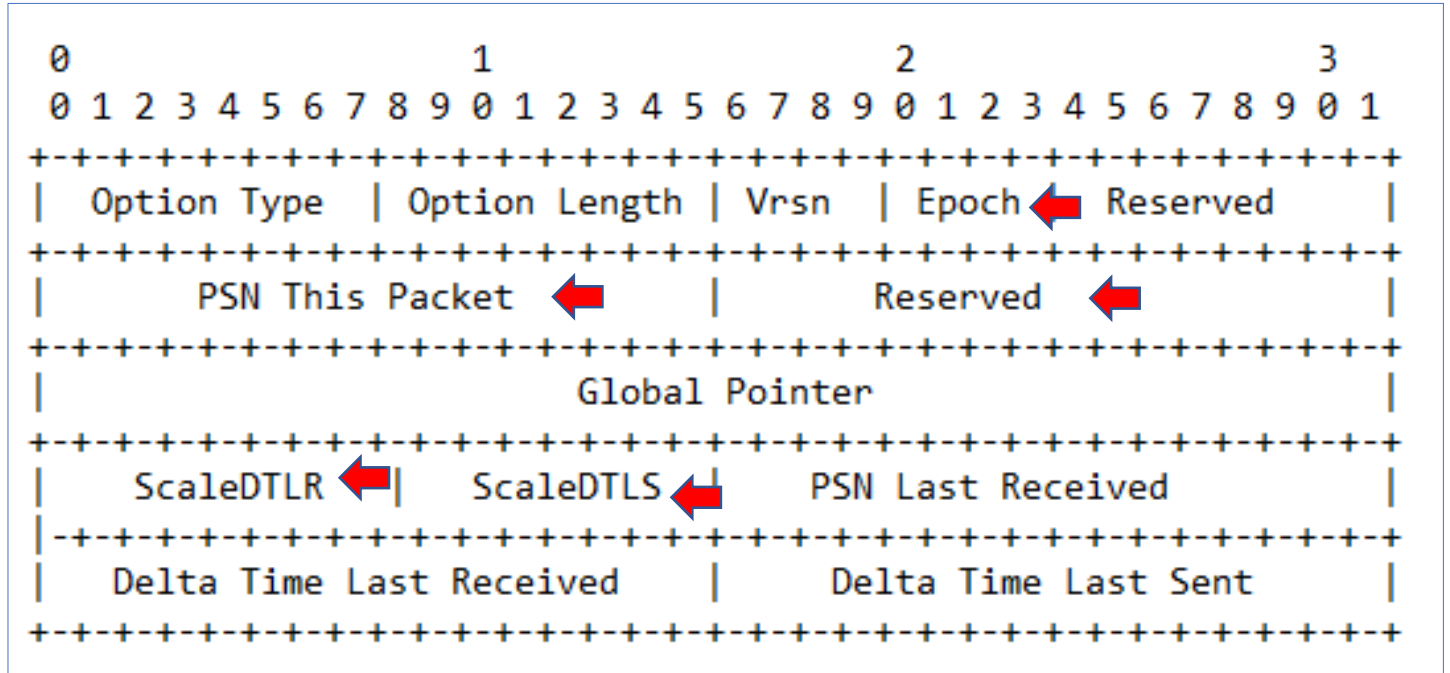
# Proposal

- Pass PSNTP in the clear
  - Other side does not ever need to decrypt
  - PSNTP becomes the "nonce" that is required for the encryption
  - Add “Epoch” field for roll-over of PSNTP counter
  - Greatly reduces response time and complexity of implementation
- Analysis of data is done offline (out of scope)
- Topology of Primary Server / Primary Client was needed because of key exchange. (Need to do real-time decryption.  So other side needs the key.) Now not needed!




PDMv2 Current Packet Layout

PDMv2 Proposed Packet Layout



# Question for WG

- Shall we will discuss with SECDIR to get a review.

Thoughts?