IPv6 Performance and Diagnostic Metrics v2 (PDMv2) Destination Option

draft-elkins-ippm-encrypted-pdmv2-07

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

Comments from Last Call

- Comments that the current PDM sequence number and Epoch are not sufficient to monitor long-lasting or high speed connections. Counters may overflow very rapidly.

- We are using HPKE for encryption.

- We researched what HPKE recommends doing in this situation.

HPKE: RFC9180

5.2 Encryption and Decryption

HPKE allows multiple encryption operations to be done based on a given setup transaction. Since the public key operations involved in setup are typically more expensive than symmetric encryption or decryption, this allows applications to amortize the cost of the public key operations, reducing the overall overhead.

In order to avoid nonce reuse, however, this encryption must be stateful. Each of the setup procedures above produces a role-specific context object that stores the AEAD and secret export parameters. The AEAD parameters consist of:

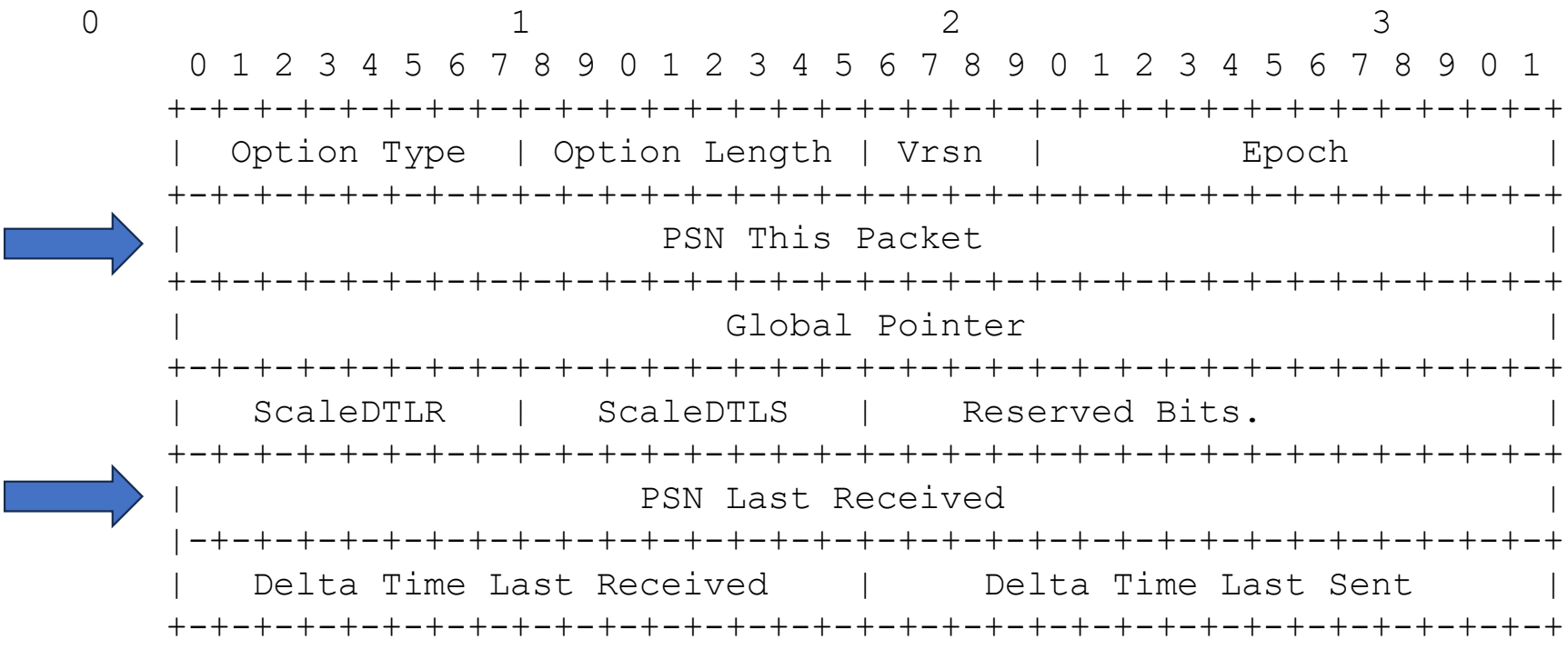
* The AEAD algorithm in use
* A secret key
* A base nonce base_nonce
* A sequence number (initially 0)

…

All these parameters except the AEAD sequence number are constant. The sequence number provides nonce uniqueness: The nonce used for each encryption or decryption operation is the result of XORing base_nonce with the current sequence number, encoded as a big-endian integer of the same length as base_nonce. Implementations MAY use a sequence number that is shorter than the nonce length (padding on the left with zero), but MUST raise an error if the sequence number overflows.

Revised Proposal for PDMv2

1. Increase the size of PSNTP (used as the sequence number for AEAD) from 16 bits to 32 bits



Revised Proposal for PDMv2

2. When PSNTP overflows, then increment Epoch and re-start PSNTP. When Epoch overflows, then stop collecting PDM data.

3. Then error message will be sent as per RFC9180:

* MessageLimitReachedError: Context AEAD sequence number overflow;

  Sections 4 and 5.2.