

IPv6 Performance and Diagnostic Metrics v2 (PDMv2) Destination Option

draft-elkins-ippm-encrypted-pdmv2-03

Nalini Elkins: Inside Products: nalini.elkins@insidestack.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

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

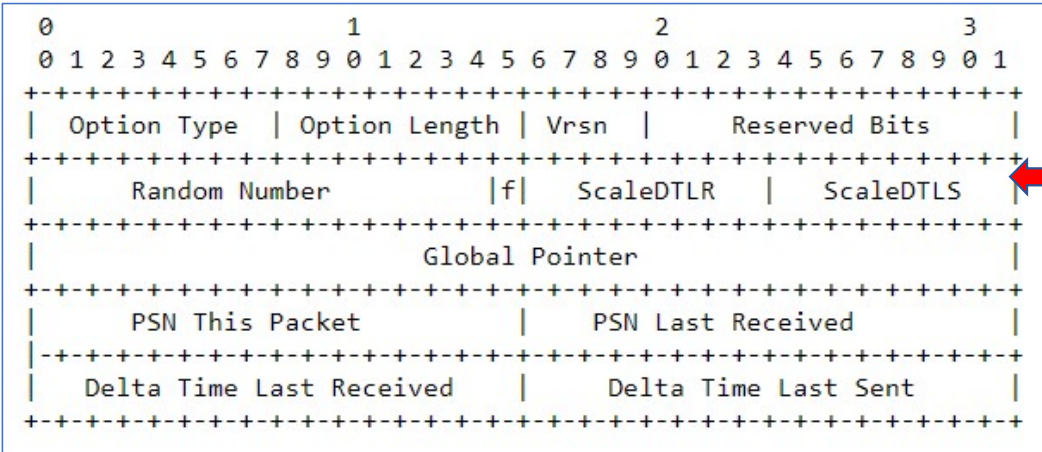
- SCALEDTLR: Scale for Delta Time Last Received
- SCALEDTLS: Scale for Delta Time Last Sent
- GLOBALPTR: Global Pointer
- PSNTP: Packet Sequence Number This Packet
- **PSNLR: Packet Sequence Number Last Received**
- DELTATLR: Delta Time Last Received
- DELTATLS: Delta Time Last Sent

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.

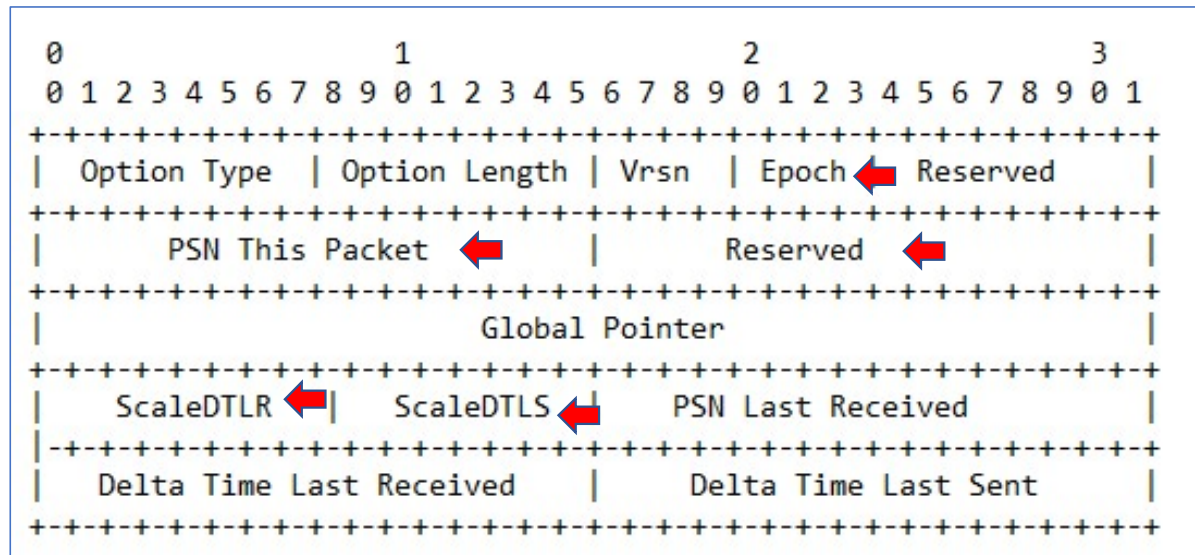
Proposal

- 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

- What do you think of this simplification?
- If WG agrees, then we will discuss with SECDIR to get their opinion
- If they agree, then we will revise the draft (describing PDMv2 flow only. No talk of Primary / Secondary.

Thoughts?

Offline Decryption

In offline decryption, the organization will have to obtain:

- Sender's key,
 - Ciphersuite,
 - metadata involved in decryption (nonce)
-
- Key and ciphersuite can be given via registration / other process. Out of scope of this draft
 - Nonce is in each packet

NalinionNewarkPingToCDNEdge.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ipv6.dst == 2001:19f0:5:3ce7:5400:4ff:fe31:1527

| No. | Time | Source | Destination | Next Header | Info |
|------|-----------|-------------------------------------|-------------------------------------|--------------------------------------|--|
| 5... | 58.923897 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=1, |
| 6... | 59.897937 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=2, |
| 6... | 60.968120 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=3, |
| 6... | 61.927963 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=4, |
| 6... | 62.897907 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=5, |
| 6... | 63.908317 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=6, |
| 6... | 64.361687 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | ICMPv6 | Neighbor Solicitation for 2001:19f0:5: |
| 6... | 64.977971 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=7, |
| 6... | 65.907922 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=8, |
| 6... | 66.927850 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | Destination Options for IPv6 | Echo (ping) request id=0x0002, seq=9, |
| 8... | 80.932002 | 2001:19f0:fc01:b::6464:c801 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | ICMPv6, Destination Options for IPv6 | Time Exceeded (hop limit exceeded in t |
| 9... | 85.938483 | 2001:19f0:fc01:b::6464:c801 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | ICMPv6, Destination Options for IPv6 | Time Exceeded (hop limit exceeded in t |
| 9... | 85.939296 | 2001:19f0:fc00::a40:5c5 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | ICMPv6, Destination Options for IPv6 | Time Exceeded (hop limit exceeded in t |
| 9... | 90.944369 | 2001:19f0:fc01:b::6464:c801 | 2001:19f0:5:3ce7:5400:4ff:fe31:1527 | ICMPv6, Destination Options for IPv6 | Time Exceeded (hop limit exceeded in t |

> Frame 598: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)

> Ethernet II, Src: fa:19:84:a9:af:ff (fa:19:84:a9:af:ff), Dst: 56:00:04:31:15:27 (56:00:04:31:15:27)

> Internet Protocol Version 6, Src: 2409:4071:6e9e:7a8f:e492:822b:3a0a:5ef5, Dst: 2001:19f0:5:3ce7:5400:4ff:fe31:1527

0110 = Version: 6

> 0010 1000 = Traffic Class: 0x28 (DSCP: AF11, ECN: Not-ECT)

.... 1100 0111 0111 0100 1011 = Flow Label: 0xc774b

Payload Length: 104

Next Header: Destination Options for IPv6 (60)

Seeing "PDM" in the wild! 1527 is our server. 5ef5 does not belong to us!