IPv6 Extension Header (Performance and Diagnostic Metrics (PDM) Destination Option) draft-ietf-ippm-encrypted-pdmv2-01

IETF114

N. Elkins: Inside Products, Inc.

M. Ackermann: BCBS Michigan

A. Deshpande: NITK Surathkal

T. Pecorella, A. Rashid: University of Florence

Brief explanation of PDM

- RFC8250: IPv6 Performance and Diagnostic Metrics (PDM) Destination Option
- To assess performance problems, this document describes optional headers embedded in each packet that provide sequence numbers and timing information as a basis for measurements. Such measurements may be interpreted in real time or after the fact. This document specifies the Performance and Diagnostic Metrics (PDM) Destination Options header.

- PDMv2: encrypts PDM

Status

- Early SECDIR review
- Continuing work on implementation
- Testing of extension headers across the Internet

SECDIR Review

I'm saying the draft is not yet ready primarily because it's early, and there is a "TBD" in "5.3 Security Goals for Authentication". That said, I'm not sure there's much to add here beyond the communicating parties being mutually authenticated.

The security considerations section addresses authentication by stating, "the Authentication and Authorization of Clients and Servers is thus delegated to the respective Organizations." I would add that the selected encryption scheme (HPKE incorporating KEM, KDF, and AEAD) should cover this requirement.

I'll also mention that authentication is mentioned in 5.3 but seemingly ignored in the list of things PDMv3 DOH needs to consider (see the middle of page 12).

Otherwise, the security considerations section covers the relevant threat scenarios reasonably well, and the document seems to provide a methodology to provide delegated trust, as claimed.

Can IPv6 Extension Headers Be Used on the Internet?

- Controversy for many years
- A number of studies showing that IPv6 extension headers get dropped at very high percentage rates.
- Studies (by and large) sent “Test” IPv6 extension headers to Alexa top n sites
- If this is true, our work on our IPv6 Extension Header Destination Option Performance and Diagnostic Metrics (PDM) is really for naught

What we did

- Used a small hosting service (not one of the “brand-name” ones)
- Using real PDM data, in DOH EHs, on actual applications sessions (FTP, HTTP,etc)
- Locations throughout the world
- *Using a kernel patch in FreeBSD to install PDM*

1. PDM-Warsaw
2. PDM-Toronto
3. PDM-Seattle
4. PDM-Mumbai
5. PDM-Melbourne
6. PDM-Frankfurt

All machines are FreeBSD with a modification to the kernel to send PDM IPv6 Destination option with every packet

Tested large FTP: Toronto to Mumbai (with PDM)

- Connected to **2401:c080:2400:1179:5400:04ff:fe0f:804a.**
- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
- 220-You are user number 1 of 50 allowed.
- 220-Local time is now 15:12. Server port: 21.
- 220 You will be disconnected after 15 minutes of inactivity.
- 331 User PDMuser OK. Password required
- 230 OK. Current directory is /
- Remote system type is UNIX.
- Using binary mode to transfer files.

- 229 Extended Passive mode OK (|||3353|)
- 150-Accepted data connection
- 150 **27872.0 kbytes to download**
- 100% |**********| 27872 KiB 222.31 KiB/s 00:00 ETA
- 226-**File successfully transferred**
- 226 125.107 seconds (measured here), 222.78 Kbytes per second
- 28540928 bytes received in 02:05 (222.31 KiB/s)
- 221-Goodbye. You uploaded 0 and downloaded 27872 kbytes.
- 221 Logout.

FTPTorontoToMumbaiJustIPv6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

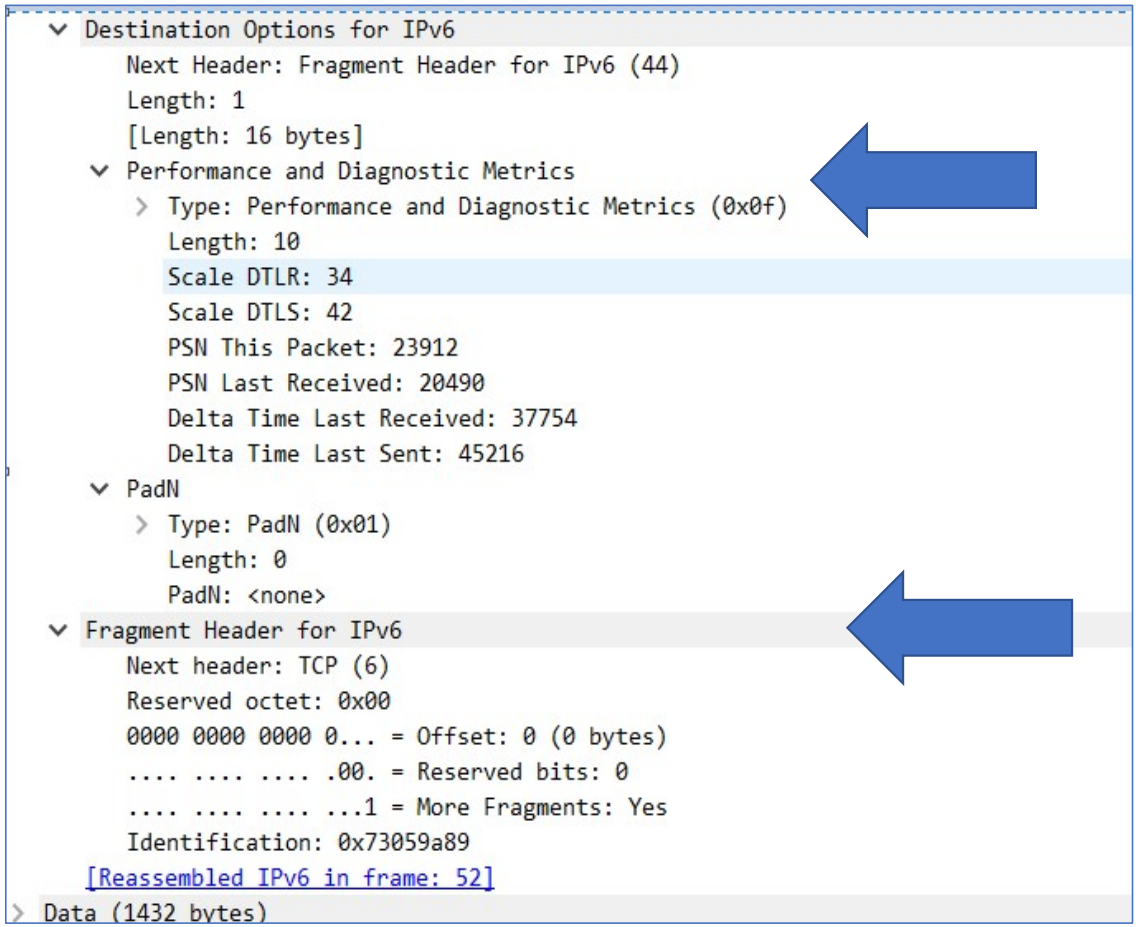
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	PSN This Packet	PSN Last Received	Info
41	3.056686	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	TCP	20490	23911	61272 → 53696 [ACK] Seq=1 Ack=1 Win=66240 L
42	3.056735	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	FTP	14105	12376	Request: RETR out.txt
43	3.253255	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490	IPv6 fragment (off=0 more=y ident=0x73059a8

```
Frame 41: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Ethernet II, Src: 56:00:04:0f:80:6d (56:00:04:0f:80:6d), Dst: 86:1f:85:c1:55:77 (86:1f:85:c1:55:77)
Internet Protocol Version 6, Src: 2001:19f0:b001:6ce:5400:4ff:fe0f:806d, Dst: 2401:c080:2400:1179:5400:4ff:fe0f:804a
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1100 1001 0100 0100 1110 = Flow Label: 0xc944e
    Payload Length: 48
    Next Header: Destination Options for IPv6 (60)
    Hop Limit: 64
    Source Address: 2001:19f0:b001:6ce:5400:4ff:fe0f:806d
    Destination Address: 2401:c080:2400:1179:5400:4ff:fe0f:804a
  v Destination Options for IPv6
      Next Header: TCP (6)
      Length: 1
      [Length: 16 bytes]
    v Performance and Diagnostic Metrics
      > Type: Performance and Diagnostic Metrics (0x0f)
        Length: 10
        Scale DTLR: 29
        Scale DTLS: 42
        PSN This Packet: 20490
        PSN Last Received: 23911
        Delta Time Last Received: 50924
        Delta Time Last Sent: 45220
    > PadN
Transmission Control Protocol, Src Port: 61272, Dst Port: 53696, Seq: 1, Ack: 1, Len: 0
```

PDM IPv6 Extension Header Destination Option

Showing both Extension Headers



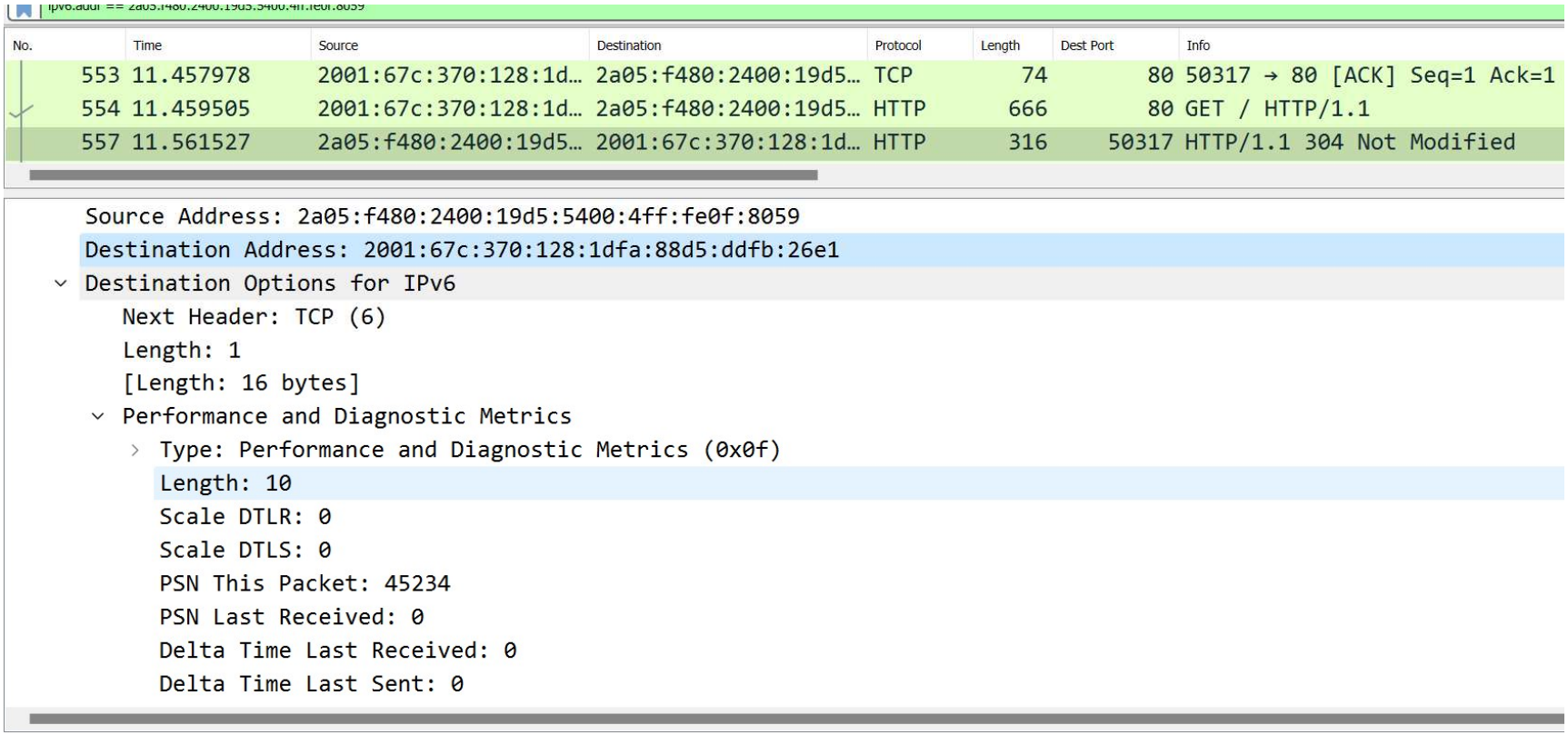
Bottom line

1. PDM-FTP Toronto to Warsaw - worked
2. PDM-FTP Toronto to Seattle - worked
3. PDM-FTP Toronto to Mumbai - worked
4. PDM-FTP Toronto to Melbourne - worked
5. PDM-FTP Toronto to Frankfurt - worked

Traces available for all to look at.

Come to the Hackathon (or HackDemo) if you want to see for yourself.

IETF Curl to Warsaw: Response



No.	Time	Source	Destination	Protocol	Length	Dest Port	Info
553	11.457978	2001:67c:370:128:1d…	2a05:f480:2400:19d5…	TCP	74	80	50317 → 80 [ACK] Seq=1 Ack=1
554	11.459505	2001:67c:370:128:1d…	2a05:f480:2400:19d5…	HTTP	666	80	GET / HTTP/1.1
557	11.561527	2a05:f480:2400:19d5…	2001:67c:370:128:1d…	HTTP	316	50317	HTTP/1.1 304 Not Modified

Next Time

- Continuing implementation
- Will have drafts at v6ops & IPPM on EH testing
- Working on EH BCP and other drafts
- Welcome collaborators

Questions?