Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 23 July 2026

N. Elkins
Inside Products, Inc.
M. Ackermann
BCBS Michigan
A. Deshpande
NITK Surathkal/Google
T. Pecorella
University of Florence
A. Rashid
Politecnico di Bari
L. Fedi
University of Florence

19 January 2026

IPv6 Performance and Diagnostic Metrics Version 2 (PDMv2) Destination Option

draft-ietf-ippm-encrypted-pdmv2-13

Abstract

RFC 8250 defines an IPv6 Destination Option that carries Performance and Diagnostic Metrics (PDM) such as sequence numbers and timing information. While useful for measurement and troubleshooting, clear-text PDM data may expose operational characteristics of endpoints and networks.

This document defines PDMv2, a revised version of PDM that introduces a registration-based security model. Instead of specifying cryptographic algorithms or inline key negotiation, PDMv2 relies on a prior registration process to authenticate entities, authorize participation, and establish shared secrets. These secrets are then used by endpoints and authorized analyzers to protect and interpret PDMv2 data according to local policy.

This document specifies the PDMv2 semantics, header structure, and operational model. Cryptographic algorithms, key derivation functions, and cipher negotiation are explicitly out of scope.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ameyand.github.io/PDMv2/draft-elkins-ippm-encrypted-pdmv2.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-ippm-encrypted-pdmv2/.

Discussion of this document takes place on the IP Performance Measurement Working Group mailing list (mailto:ippm@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ippm/. Subscribe at https://www.ietf.org/mailman/listinfo/ippm/.

Source for this draft and an issue tracker can be found at https://github.com/ameyand/PDMv2.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 July 2026.

Copyright Notice

Table of Contents

1. Introduction

The Performance and Diagnostic Metrics (PDM) Destination Option defined in RFC 8250 provides packet sequence numbers and timing information to support performance measurement and diagnostics. While effective, transmitting such information in clear text can reveal details about endpoint behavior, processing capability, and network characteristics.

PDMv2 enhances PDM by enabling secure operation through a registration-first architecture. Security-sensitive material is established out of band, prior to data transmission, and is not negotiated inline with PDMv2 traffic. This approach preserves the lightweight nature of PDM while avoiding tight coupling to transport-layer security protocols.

PDMv2 operates entirely at the IPv6 layer and applies uniformly to TCP, UDP, ICMP, QUIC, and other upper-layer protocols. Intermediate devices are not required to decrypt or interpret PDMv2 contents.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Design Goals

PDMv2 is designed with the following goals:

* Maintain compatibility with the operational model of RFC 8250

* Avoid inline cryptographic handshakes at the IP layer

* Support heterogeneous transport protocols and non-transport flows

* Enable offline analysis by authorized entities

* Integrate cleanly with existing authentication and authorization infrastructures

4. PDMv2 Foundational Principles

PDMv2 adheres to the following foundational principles:

1. Registration-First Security: All security context used by PDMv2 is established during a prior registration phase. No cryptographic negotiation occurs during PDMv2 packet exchange.

2. IP-Layer Independence: PDMv2 security does not depend on TCP, TLS, QUIC, or any specific transport protocol.

3. Minimal On-Path Impact: Routers and intermediate nodes forward PDMv2 packets without decryption or inspection.

4. Offline Decryption and Analysis: PDMv2 data MAY be collected and analyzed after transmission. Real-time interpretation is optional and deployment-specific.

5. Separation of Specification Scope: This document defines protocol behavior and data formats, not cryptographic algorithms.

6. Explicit Authorization: Only registered and authorized entities may emit, receive, or analyze protected PDMv2 data.

5. Registration Framework Overview

PDMv2 relies on an external registration system to establish trust and shared context between participating entities.

5.1. Registration Objectives

A registration system used with PDMv2 MUST:

* Authenticate participating entities
* Authorize PDMv2 usage
* Establish one or more shared secrets or credentials
* Enable analyzers to interpret PDMv2 data
* Support revocation and lifecycle management

5.2. Registration Participants

The following logical roles are assumed:

* Client : An endpoint that initiates communication and emits PDMv2 data
* Server : An endpoint that receives communication and emits PDMv2 data
* Authentication Server (AS) : A trusted entity that performs authentication and authorization
* Analyzer : An authorized entity that interprets collected PDMv2 data

An implementation MAY combine roles within a single system.

5.3. Registration Transport

The registration exchange MUST be protected by a secure channel. The choice of transport and security protocol is out of scope for this document.

6. PDMv2 Destination Options

6.1. Use of IPv6 Destination Options

PDMv2 is carried as an IPv6 Destination Option within the Destination Options Header as defined in RFC 8200. Processing rules from RFC 8250 continue to apply unless explicitly updated by this document.

6.2. Metrics

PDMv2 supports the following metrics:

* Packet Sequence Number (This Packet)
* Packet Sequence Number (Last Received)
* Delta Time Last Received
* Delta Time Last Sent
* Global Pointer

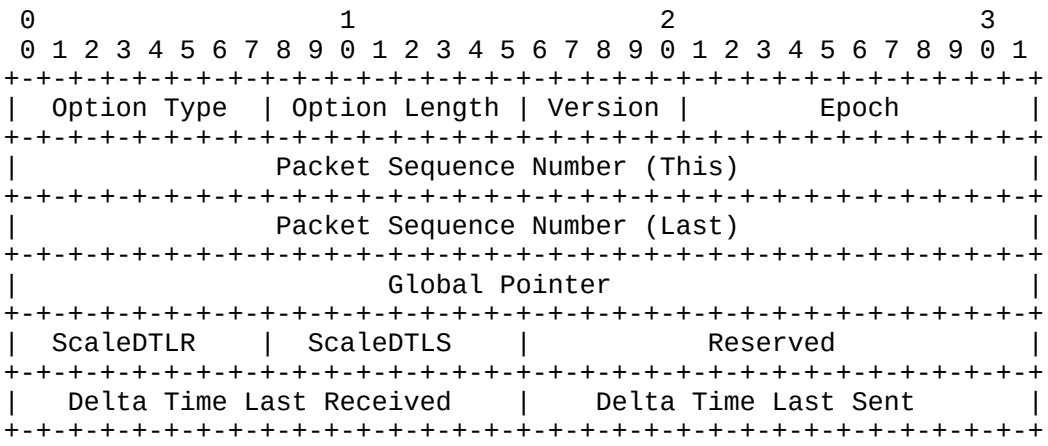
These metrics have the same semantics as in RFC 8250, with the addition of the Global Pointer.

6.3. Global Pointer

The Global Pointer provides a coarse indicator of packet transmission activity by an endpoint. Separate counters are maintained for link-local and global unicast source addresses.

7. PDMv2 Header Format

PDMv2 uses a single header format. Whether metric contents are protected or unprotected is determined by local policy and registration context.



Option Type

0x0F

8-bit unsigned integer. The Option Type is adopted from RFC 8250 [RFC8250].

Option Length

0x22: Unencrypted PDM

0x22: Encrypted PDM

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields.

Version Number

0x2

4-bit unsigned number.

Epoch

12-bit unsigned number.

Epoch field is used to indicate the valid SessionTemporaryKey.

Packet Sequence Number This Packet (PSNTP)

32-bit unsigned number.

This field is initialized at a random number and is incremented sequentially for each packet of the 5-tuple.

This field + Epoch are used in the Encrypted PDMv2 as the encryption nonce. The nonce MUST NOT be reused in different sessions.

Packet Sequence Number Last Received (PSNLR)

32-bit unsigned number.

This field is the PSNTP of the last received packet on the 5-tuple.

Global Pointer

32-bit unsigned number.

Global Pointer is initialized to 1 for the different source address types and incremented sequentially for each packet with the corresponding source address type.

This field stores the Global Pointer type corresponding to the SADDR type of the packet.

Scale Delta Time Last Received (SCALEDTLR)

8-bit unsigned number.

This is the scaling value for the Delta Time Last Sent (DELTATLS) field.

Scale Delta Time Last Sent (SCALEDTLS)

8-bit unsigned number.

This is the scaling value for the Delta Time Last Sent (DELTATLS) field.

Reserved Bits

16-bits.

Reserved bits for future use. They MUST be set to zero on transmission and ignored on receipt per [RFC3552].

Delta Time Last Received (DELTATLR)

16-bit unsigned integer.

The value is set according to the scale in SCALEDTLR.

Delta Time Last Received = (send time packet n - receive time packet (n - 1))

Delta Time Last Sent (DELTATLS)

16-bit unsigned integer.

The value is set according to the scale in SCALEDTLS.

Delta Time Last Sent = (receive time packet n - send time packet (n - 1))

8. Operational Model

8.1. Registration Phase

Prior to sending PDMv2 data:

* The endpoint authenticates to an Authentication Server
* Authorization for PDMv2 usage is evaluated
* Shared secret(s) or credentials are provisioned

8.2. Measurement Phase

* Endpoints send PDMv2 headers according to local policy
* No cryptographic negotiation occurs on the wire
* Intermediate devices forward packets unchanged

8.3. Analysis Phase

* Authorized analyzers access collected data
* Interpretation uses registration-derived context

9. Security Considerations

PDMv2 reduces exposure of sensitive operational metadata by ensuring that only registered and authorized entities can meaningfully interpret measurement data.

This document intentionally does not specify cryptographic mechanisms. Security strength therefore depends on the chosen registration system, its authentication methods, and its key management practices.

Implementations SHOULD support:

* Forward Secracy

* Logging of anomalous PDMv2 behavior

10. Privacy Considerations

PDMv2 metrics may reveal traffic patterns or operational characteristics. Registration-based authorization limits access to such data to approved entities. Deployments SHOULD consider enabling PDMv2 on multiple flows to reduce metadata distinguishability.

11. IANA Considerations

This document requests the allocation of a new IPv6 Destination Options Header Option Type from the "Destination Options and Hop-by-Hop Options" registry maintained by the Internet Assigned Numbers Authority.

The requested allocation is for the Performance and Diagnostic Metrics Version 2 (PDMv2) option. This option is distinct from and independent of the Performance and Diagnostic Metrics option defined in RFC 8250.

12. Contributors

The authors wish to thank NITK Surathkal for their support and assistance in coding and review. In particular Dr. Mohit Tahiliani and Abhishek Kumar (now with Google). Thanks also to Priyanka Sinha for her comments. Thanks to the India Internet Engineering Society (iiesoc.in), in particular Dhruv Dhody, for his comments and for providing the funding for servers needed for protocol development. Thanks to Balajinaidu V, Amogh Umesh, and Chinmaya Sharma of NITK for developing the PDMv2 implementation for testing.

13. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/rfc/rfc3552>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8250] Elkins, N., Hamilton, R., and M. Ackermann, "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option", RFC 8250, DOI 10.17487/RFC8250, September 2017, <https://www.rfc-editor.org/rfc/rfc8250>.

Appendix A. Example: RADIUS / EAP-Based Registration

This appendix illustrates one possible registration mechanism that satisfies the requirements defined in Section 4. Other mechanisms may be used.

A.1. Overview

This appendix describes an example registration system for PDMv2 based on RADIUS with Extensible Authentication Protocol (EAP). This approach has been implemented and validated in a prototype environment and demonstrates that a shared master secret can be established prior to PDMv2 operation without introducing inline cryptographic negotiation at the IP layer.

RADIUS and EAP are widely deployed for Authentication, Authorization, and Accounting (AAA) in enterprise, service provider, and federated environments (e.g., eduroam). Their use here is illustrative and leverages existing infrastructure and operational experience.

A.2. Participants

The following entities participate in this example:

* PDMv2 Endpoint

A Client or Server that will emit or receive PDMv2 data.

* Authentication Server (AS)

A RADIUS server that performs authentication and authorization using EAP.

* Analyzer

An authorized entity that may interpret or decrypt collected PDMv2 data using registration-derived context.

An implementation MAY combine multiple roles within a single system.

A.3. Registration Flow (Example)

A typical registration flow proceeds as follows:

* Secure Channel Establishment The PDMv2 endpoint establishes a secure exchange with the Authentication Server. In many deployments this occurs implicitly as part of an EAP method protected by TLS (e.g., EAP-TLS or PEAP).

* Endpoint Authentication The endpoint authenticates using credentials appropriate to the deployment, such as certificates, credentials, tokens, or federated identity.

* Authorization Decision The Authentication Server determines whether the endpoint is authorized to:

  - Send PDMv2 data

  - Receive PDMv2 data

  - Participate in specific measurement domains

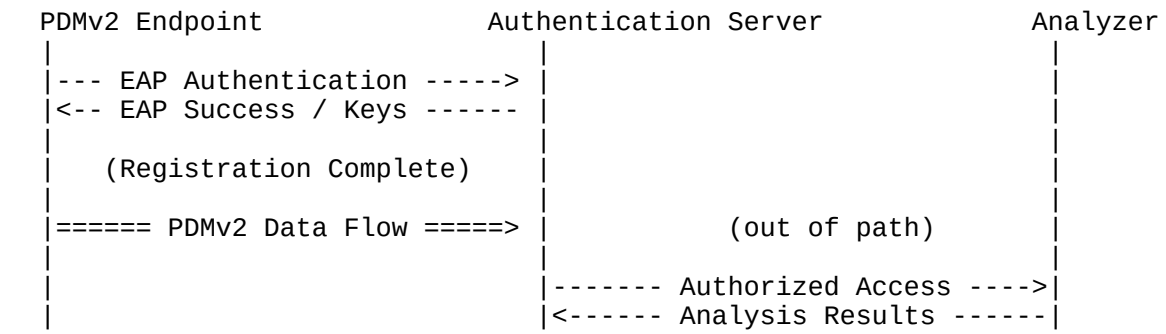
* Master Secret Establishment Upon successful authentication, EAP produces keying material (e.g., a Master Session Key). This keying material is made available to the endpoint and retained by the Authentication Server according to local policy.

* Provisioning of Context The endpoint associates the received master secret with local PDMv2 policy, such as permitted peers, scope, and lifetime.

* Analyzer Enablement (Optional) If offline analysis is required, the Authentication Server provisions appropriate authorization or keying context to approved analyzers.

A.4. Registration Flow (Illustrative ASCII Diagram)

The following diagram illustrates the example flow. It is provided for clarity only and does not define protocol behavior.



A.5. Use with PDMv2 Traffic

After registration:

* PDMv2 packets are sent without any inline authentication or negotiation.

* Endpoints locally derive any session-specific context needed to protect or interpret PDMv2 metrics.

* Intermediate routers forward packets without modification or inspection.

* Analyzers use registration-derived context to interpret collected data.

The registration system is not involved in the PDMv2 data path.

A.6. Key Lifecycle Considerations

In this example, the RADIUS/EAP infrastructure can support:

* Periodic re-registration to refresh secrets

* Revocation of authorization by disabling credentials

* Federation across administrative domains

* Separation of endpoint and analyzer privileges

Specific key derivation, transformation, or protection mechanisms are implementation-specific and intentionally outside the scope of this document.

A.7. Example Deployment: Federated Environments (eduroam-Style)

In federated environments such as global research and education networks, RADIUS is commonly deployed in a hierarchical or proxy-based architecture. An endpoint authenticates using credentials issued by its home organization, while authorization decisions may be enforced by visited or intermediate domains.

This model maps naturally to PDMv2 registration:

* Endpoints authenticate using existing institutional credentials
* Authorization for PDMv2 usage can be scoped by domain, role, or policy
* Registration secrets are derived without requiring bilateral agreements between all participating domains

This example demonstrates that PDMv2 registration can scale across organizational and administrative boundaries.

A.8. Why TLS Session Keys Are Not Reused (Informative)

It may appear attractive to reuse TLS session keys for protecting PDMv2 metrics. However, this approach is not suitable for PDMv2 for several reasons:

* Layering : PDMv2 operates at the IPv6 layer, while TLS is bound to transport-layer protocols such as TCP or QUIC.
* Protocol Coverage : PDMv2 applies equally to UDP, ICMP, and other non-TLS-capable protocols.
* Multiplicity of Flows : A single endpoint may emit PDMv2 data for multiple concurrent flows that do not share a common TLS session.
* Analyzer Access : Offline analyzers may require access to PDMv2 data without participating in live TLS sessions.
* Operational Simplicity : Registration decouples security establishment from traffic patterns and avoids inline negotiation complexity.

For these reasons, PDMv2 adopts a registration-based security model rather than reusing transport-layer session keys.

A.9. Summary

This appendix demonstrates that a RADIUS/EAP-based registration system can satisfy the PDMv2 registration requirements defined in this document. The example shows that secure, scalable, and federated registration can be achieved using existing AAA infrastructure, without constraining PDMv2 to a specific authentication or cryptographic technology.

Appendix B. Change Log

Note to RFC Editor: if this document does not obsolete an existing RFC, please remove this appendix before publication as an RFC.

Appendix C. Open Issues

Note to RFC Editor: please remove this appendix before publication as an RFC.

Authors' Addresses

Nalini Elkins
Inside Products, Inc.
United States
Email: nalini.elkins@insidethestack.com

Michael Ackermann
BCBS Michigan
United States
Email: mackermann@bcbsm.com

Ameya Deshpande
NITK Surathkal/Google
India
Email: ameyanrd@gmail.com

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

Adnan Rashid
Politecnico di Bari
Italy

Email: adnan.rashid@poliba.it

Lorenzo Fedi
University of Florence
Italy
Email: lorenzo.fedi3@edu.unifi.it