IETF
Internet-Draft
Intended status: Standards Track
Expires: 22 March 2026

Amogh. Kerigond
18 September 2025

Connectionless Packet Timestamp Forwarding (CPTF)
draft-kerigond-cptf-00

Abstract

This document specifies a protocol extension for connectionless packet transmission, enabling forwarding devices such as routers and switches to insert per-hop arrival timestamps directly into packets during transit. The extension allows receivers and monitoring systems to reconstruct the precise timing and location of delays throughout a packet’s network path, improving performance diagnostics for protocols such as UDP, ICMP, multicast, and broadcast.

Note

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79 and is intended for the IETF standards track.

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 22 March 2026.

Copyright Notice

Table of Contents

1. Introduction

Connectionless protocols such as UDP, ICMP, multicast, and broadcast are widely used for streaming, diagnostics, IoT, and control-plane functions. These packets traverse multiple network hops without explicit state; existing standards do not provide a means for intermediate devices to record their transit times. Lack of per-hop transit information impedes the ability to pinpoint delays, diagnose jitter, and perform fine-grained network analysis.

This document defines a Timestamp Forwarding Option for selected packet types, enabling hop-by-hop timestamp insertion and subsequent analysis.

2. Terminology

CPTF: Connectionless Packet Timestamp Forwarding

TFO: Timestamp Forwarding Option

Node Identifier: The device’s unique address (IP or MAC)

Timestamp: 64-bit value in milliseconds since Unix epoch

3. Problem Statement

Packet delay is typically only observable at endpoints. Operators cannot precisely identify which network hop induces delay or jitter, especially for connectionless flows. Traceroute and similar active probes require custom traffic and do not reflect normal traffic conditions. IoT and real-time services are particularly affected.

4. Protocol Overview

CPTF introduces a header option for eligible packets. Each CPTF-capable forwarding node appends or inserts its timestamp as the packet is received or forwarded. At the destination, these timestamps reveal per-hop transit delays for individual packets.

5. Timestamp Forwarding Option

5.1. IPv4 Option Structure

The CPTF IPv4 Option format:

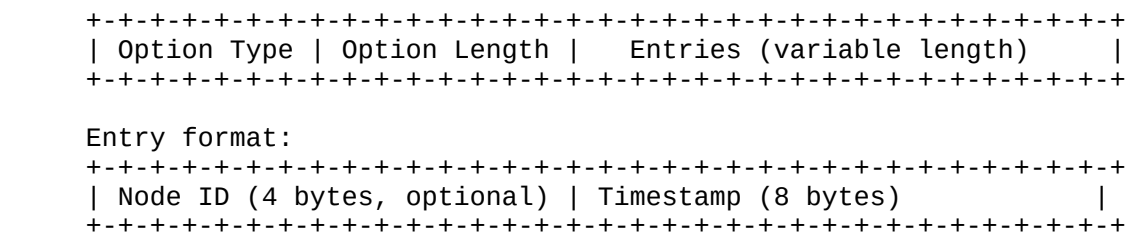

Figure 1

Multiple entries are appended in arrival order.

5.2. IPv6 Option Structure

The CPTF destination option is carried in the IPv6 Destination Options header.

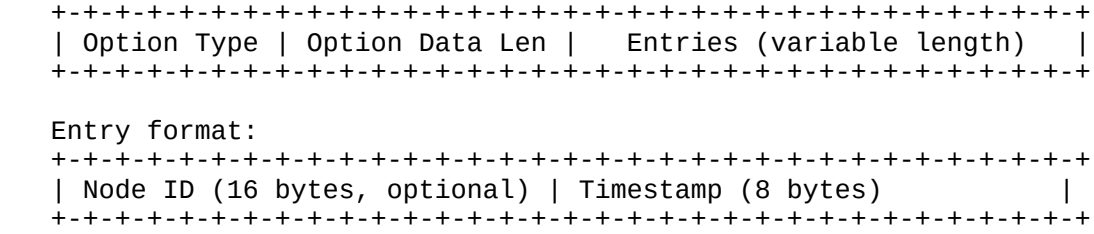

Figure 2

5.3. UDP Extension Structure

For UDP extensions, CPTF may be placed in the UDP payload or in an extension header.

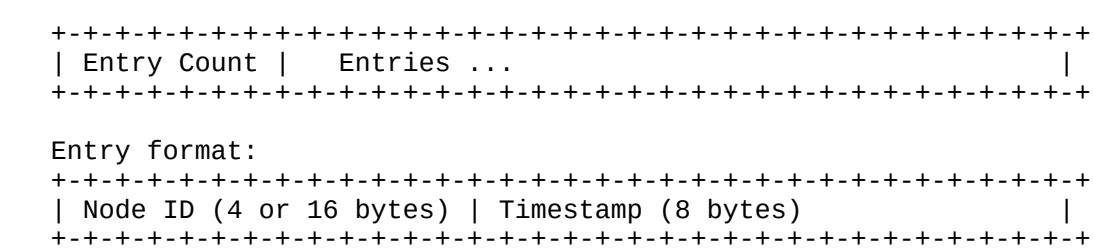

Figure 3

5.4. Processing Rules

Sender MAY initialize CPTF header and insert its timestamp.

Each CPTF-capable device SHOULD check for available entry slots and insert its Node ID and current time.

If all entry slots are full, no further timestamps are added.

Devices MUST NOT overwrite earlier timestamps.

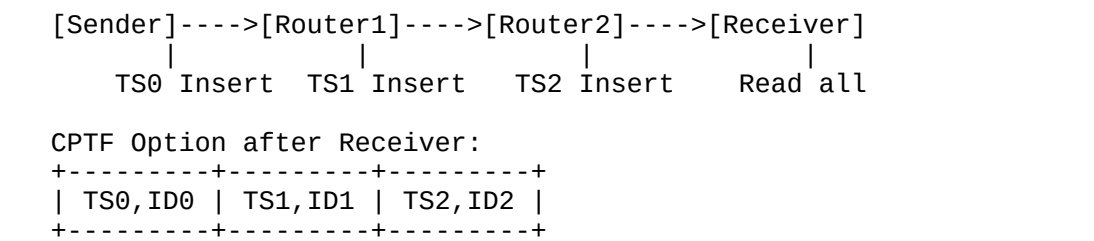

Figure 4

6. Operational Scenarios

UDP Video Streaming: Packets from a camera traverse routers, each adding CPTF info. The server can analyze delays per hop for each packet received.

ICMP Diagnostics: Echo Request and Reply packets accumulate CPTF data, allowing the initiator to determine where latency/jitter occurred without special probes.

IoT Mesh Broadcast: CPTF helps diagnose congested mesh segments by collecting hop timing.

7. Security Considerations

CPTF fields may reveal topology and timing to observers. Usage SHOULD be limited by network policy. Entry limits and rate controls are RECOMMENDED to avoid resource exhaustion. CPTF-enabled devices MAY restrict Node ID exposure.

8. IANA Considerations

This memo requests assignment of: CPTF IPv4 Option Number, CPTF IPv6 Destination Option Type, CPTF UDP Extension Option Code, CPTF ICMP Extension Option Code.

9. References

RFC791: Internet Protocol

RFC792: Internet Control Message Protocol

RFC2460: Internet Protocol, Version 6 (IPv6) Specification

RFC768: User Datagram Protocol

Appendix A. Acknowledgments

The author wishes to thank the networking and diagnostics communities for inspiring work that motivated CPTF.

Appendix B. Author’s Address

Amoghasidd Kerigond

Email: amogh.kerigond@gmail.com

Author’s Address

Amoghasidd Kerigond
Email: amogh.kerigond@gmail.com