DetNet Data Plane: IEEE 802.1 Time Sensitive Networking over MPLS
draft-ietf-detnet-tsn-vpn-over-mpls-00

Abstract

This document specifies the Deterministic Networking data plane when
TSN networks interconnected over an MPLS Packet Switched Networks.

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 November 6, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(https://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
1. Introduction

[Editor’s note: Introduction to be made specific to TSN over DetNet scenario. Do we intend to cover both TSN over DetNet IP and TSN over DetNet MPLS? Or this document is limited to MPLS scenarios?]

2. Terminology

[Editor’s note: text to be review what is really needed here.]

2.1. Terms Used in This Document

This document uses the terminology established in the DetNet architecture [I-D.ietf-detnet-architecture], and the reader is assumed to be familiar with that document and its terminology.

The following terminology is introduced in this document:
F-Label  A Detnet "forwarding" label that identifies the LSP used to forward a DetNet flow across an MPLS PSN, e.g., a hop-by-hop label used between label switching routers (LSR).

S-Label  A DetNet "service" label that is used between DetNet nodes that implement also the DetNet service sub-layer functions. An S-Label is also used to identify a DetNet flow at DetNet service sub-layer.

d-CW     A DetNet Control Word (d-CW) is used for sequencing and identifying duplicate packets of a DetNet flow at the DetNet service sub-layer.

2.2. Abbreviations

[Editor’s note: text to be cleaned up].

The following abbreviations are used in this document:

AC         Attachment Circuit.
CE         Customer Edge equipment.
CoS        Class of Service.
CW         Control Word.
DetNet     Deterministic Networking.
DF         DetNet Flow.
DN-IWF     DetNet Inter-Working Function.
L2         Layer 2.
L2VPN      Layer 2 Virtual Private Network.
L3         Layer 3.
LSR        Label Switching Router.
MPLS       Multiprotocol Label Switching.
MPLS-TE    Multiprotocol Label Switching - Traffic Engineering.
MPLS-TP    Multiprotocol Label Switching - Transport Profile.
3. Requirements Language

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.

4. IEEE 802.1 TSN Over DetNet MPLS Data Plane Scenario

[Author’s note: review required on his part.]
Figure 1: A TSN over DetNet MPLS Enabled Network

Figure 1 shows IEEE 802.1 TSN end stations operating over a TSN aware DetNet service running over an MPLS network. DetNet Edge Nodes sit at the boundary of a DetNet domain. They are responsible for mapping non-DetNet aware L2 traffic to DetNet services. They also support the imposition and disposition of the required DetNet encapsulation. These are functionally similar to pseudowire (PW) Terminating Provider Edge (T-PE) nodes which use MPLS-TE LSPs. In this example they understand and support IEEE 802.1 TSN and are able to map TSN flows into DetNet flows. The specific of this operation are discussed later in this document.

Native TSN flow and DetNet MPLS flow differ not only by the additional MPLS specific encapsulation, but DetNet MPLS flows have on each DetNet node an associated DetNet specific data structure, what defines flow related characteristics and required forwarding functions. In this example, edge Nodes provide a service proxy function that "associates" the DetNet flows and native flows at the edge of the DetNet domain. This ensures that the DN Flow is properly served at the Edge node (and inside the domain).

Figure 2 illustrates how DetNet can provide services for IEEE 802.1TSN end systems, CE1 and CE2, over a DetNet enabled MPLS network. Edge nodes, E1 and E2, insert and remove required DetNet data plane encapsulation. The ‘X’ in the edge nodes and relay node, R1, represent a potential DetNet compound flow packet replication and elimination point. This conceptually parallels L2VPN services, and could leverage existing related solutions as discussed below.
5. DetNet MPLS Data Plane Considerations

[Editor’s note: Needs clean up, what is relevant for TSN over DetNet scenarios.].

This section provides informative considerations related to providing DetNet service to flows which are identified based on their header information. At a high level, the following are provided on a per flow basis:

Eliminating contention loss and jitter reduction:

Use of allocated resources (queuing, policing, shaping) to ensure that the congestion-related loss and latency/jitter requirements of a DetNet flow are met.

Explicit routes:

Use of a specific path for a flow. This limits misordering and bounds latency.

Service protection:

![Figure 2: IEEE 802.1 TSN Over DetNet](image)
Which in the case of this document primarily relates to replication and elimination. Changing the explicit path after a failure is detected in order to restore delivery of the required DetNet service characteristics is also possible. Path changes, even in the case of failure recovery, can lead to the out of order delivery of data.

Load sharing:

Generally, distributing packets of the same DetNet flow over multiple paths is not recommended. Such load sharing, e.g., via ECMP or UCMP, impacts ordering and possibly jitter.

Troubleshooting:

For example, to support identification of misbehaving flows.

Recognize flow(s) for analytics:

For example, increase counters.

Correlate events with flows:

For example, unexpected loss.

The DetNet data plane also allows for the aggregation of DetNet flows, e.g., via MPLS hierarchical LSPs, to improved scaling. When DetNet flows are aggregated, transit nodes provide service to the aggregate and not on a per-DetNet flow basis. In this case, nodes performing aggregation will ensure that per-flow service requirements are achieved.

5.1. End-System Specific Considerations

Data-flows requiring DetNet service are generated and terminated on end-systems. Encapsulation depends on application and its preferences. In a DetNet MPLS domain the DN functions use the d-CWs, S-Labels and F-Labels to provide DetNet services. However, an application may exchange further flow related parameters (e.g., time-stamp), which are not provided by DN functions.

Specifics related to non-MPLS DetNet end station behavior are outside the scope of this document. For example, details on support for DetNet IP data flows can be found in [I-D.ietf-detnet-dp-sol-ip]. This document is also useful for end stations that map IP flows to DetNet flows.
As a general rule, DetNet MPLS domains are capable of forwarding any DetNet MPLS flows and the DetNet domain does not mandate the end-system or edge system encapsulation format. Unless there is a proxy of some form present, end-systems peer with similar end-systems using the same application encapsulation format. For example, as shown in Figure 3, IP applications peer with IP applications and Ethernet L2VPN applications peer with Ethernet L2VPN applications.

Figure 3: End-Systems and The DetNet MPLS Domain

6. MPLS-Based DetNet Data Plane Solution

[Editor’s note: Needs clean up. Text should focus on Edge node related topics.]

6.1. DetNet Over MPLS Encapsulation Components

To carry DetNet over MPLS the following is required:

1. A method of identifying the MPLS payload type.


5. A suitable LSP to deliver the packet to the egress PE.


In this design an MPLS service label (the S-Label), similar to a pseudowire (PW) label [RFC3985], is used to identify both the DetNet flow identity and the payload MPLS payload type satisfying (1) and (2) in the list above. OAM traffic discrimination happens through the use of the Associated Channel method described in [RFC4385]. The DetNet sequence number is carried in the DetNet Control word which carries the Data/OAM discriminator. To simplify implementation and to maximize interoperability two sequence number sizes are supported: a 16 bit sequence number and a 28 bit sequence number. The 16 bit sequence number is needed to support some types of legacy clients. The 28 bit sequence number is used in situations where it is necessary ensure that in high speed networks the sequence number space does not wrap whilst packets are in flight.

The LSP used to forward the DetNet packet may be of any type (MPLS-LDP, MPLS-TE, MPLS-TP [RFC5921], or MPLS-SR [I-D.ietf-spring-segment-routing-mpls]). The LSP (F-Label) label and/or the S-Label may be used to indicate the queue processing as well as the forwarding parameters. Note that the possible use of Penultimate Hop Popping (PHP) means that the only label in a received label stack may be the S-Label.

6.2. TSN over MPLS Data Plane Encapsulation

6.2.1. Edge Node Processing

An edge node is responsible for matching ingress packets to the service they require and encapsulating them accordingly. An edge node may participate in the packet replication and duplication elimination.

The DetNet-aware forwarder selects the egress DetNet member flow segment based on the flow identification. The mapping of ingress DetNet member flow segment to egress DetNet member flow segment may be statically or dynamically configured. Additionally the DetNet-aware forwarder does duplicate frame elimination based on the flow identification and the sequence number combination. The packet replication is also done within the DetNet-aware forwarder. During elimination and the replication process the sequence number of the DetNet member flow MUST be preserved and copied to the egress DetNet member flow.

The internal design of a relay node is out of scope of this document. However the reader’s attention is drawn to the need to make any PREOF
state available to the packet processor(s) dealing with packets to which the PREOF functions must be applied, and to maintain that state is such as way that it is available to the packet processor operation on the next packet in the DetNet flow (which may be a duplicate, a late packet, or the next packet in sequence.

[Editor’s note: I think the rest of this section belongs in a new "802.1 TSN (island Interconnect) over DetNet MPLS" section.]

This may be done in the DetNet layer, or where the native service processing (NSP) ([RFC3985] is IEEE 802.1CB [IEEE8021CB] capable, the packet replication and duplicate elimination MAY entirely be done in the NSP, bypassing the DetNet flow encapsulation and logic entirely. This enables operating over unmodified implementations and deployments. The NSP approach works only between edge nodes and cannot make use of relay nodes.

The NSP approach is useful end to end tunnel and for for "island interconnect" scenarios. However, when there is a need to do PREOF in a middle of the network, such plain edge to edge operation is not sufficient.

The extended forwarder MAY copy the sequencing information from the native DetNet packet into the DetNet sequence number field and vice versa. If there is no existing sequencing information available in the native packet or the forwarder chose not to copy it from the native packet, then the extended forwarder MUST maintain a sequence number counter for each DetNet flow (indexed by the DetNet flow identification).

6.2.2. Layer 2 Addressing and QoS Considerations

[Editor’s NOTE: review and simplify this section if possible.]

The Time-Sensitive Networking (TSN) Task Group of the IEEE 802.1 Working Group have defined (and are defining) a number of amendments to IEEE 802.1Q [IEEE8021Q] that provide zero congestion loss and bounded latency in bridged networks. IEEE 802.1CB [IEEE8021CB] defines packet replication and elimination functions that should prove both compatible with and useful to, DetNet networks.

As is the case for DetNet, a Layer 2 network node such as a bridge may need to identify the specific DetNet flow to which a packet belongs in order to provide the TSN/DetNet QoS for that packet. It also will likely need a CoS marking, such as the priority field of an IEEE Std 802.1Q VLAN tag, to give the packet proper service.
Although the flow identification methods described in IEEE 802.1CB [IEEE8021CB] are flexible, and in fact, include IP 5-tuple identification methods, the baseline TSN standards assume that every Ethernet frame belonging to a TSN stream (i.e. DetNet flow) carries a multicast destination MAC address that is unique to that flow within the bridged network over which it is carried. Furthermore, IEEE 802.1CB [IEEE8021CB] describes three methods by which a packet sequence number can be encoded in an Ethernet frame.

Ensuring that the proper Ethernet VLAN tag priority and destination MAC address are used on a DetNet/TSN packet may require further clarification of the customary L2/L3 transformations carried out by routers and edge label switches. Edge nodes may also have to move sequence number fields among Layer 2, PW, and IP encapsulations.

7. Controller Plane (Management and Control) Considerations

[Editor’s note: requires considerations related to TSN over DetNet.].

8. Security Considerations

The security considerations of DetNet in general are discussed in [I-D.ietf-detnet-architecture] and [I-D.sdt-detnet-security]. Other security considerations will be added in a future version of this draft.

9. IANA Considerations

This document makes no IANA requests.

10. Acknowledgements

Thanks for Norman Finn and Lou Berger for their comments and contributions.

11. References

11.1. Normative References


11.2. Informative References


[I-D.ietf-detnet-flow-information-model]

[I-D.ietf-pce-pcep-extension-for-pce-controller]

[I-D.ietf-spring-segment-routing-mpls]

[I-D.sdt-detnet-security]

[IEEE1588]

[IEEE8021CB]

[IEEE8021Q]


Appendix A. Example of TSN over DetNet Data Plane Operation

[Editor’s note: Add a simplified example of DetNet data plane and how labels etc work in the case of TSN over DetNet MPLS and utilizing e.g., PREOF.]

Authors’ Addresses

Balazs Varga (editor)
Ericsson
Magyar Tudosok krt. 11.
Budapest 1117
Hungary
Email: balazs.a.varga@ericsson.com

Janos Farkas
Ericsson
Magyar Tudosok krt. 11.
Budapest 1117
Hungary
Email: janos.farkas@ericsson.com

Andrew G. Malis
Huawei Technologies
Email: agmalis@gmail.com

Stewart Bryant
Huawei Technologies
Email: stewart.bryant@gmail.com

Jouni Korhonen
Email: jouni.nospam@gmail.com