DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking (TSN)
draft-ietf-detnet-ip-over-tsn-00

Abstract

This document specifies the Deterministic Networking IP data plane when operating over a TSN network.

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

Deterministic Networking (DetNet) is a service that can be offered by a network to DetNet flows. DetNet provides these flows extremely low packet loss rates and assured maximum end-to-end delivery latency. General background and concepts of DetNet can be found in the DetNet Architecture [I-D.ietf-detnet-architecture].

This document specifies the DetNet data plane operation for IP hosts and routers that provide DetNet service to IP encapsulated data. No DetNet specific encapsulation is defined to support IP flows, rather existing IP and higher layer protocol header information is used to support flow identification and DetNet service delivery.

The DetNet Architecture decomposes the DetNet related data plane functions into two sub-layers: a service sub-layer and a forwarding sub-layer. The service sub-layer is used to provide DetNet service protection and reordering. The forwarding sub-layer is used to
provides congestion protection (low loss, assured latency, and limited reordering). As no DetNet specific headers are added to support DetNet IP flows, only the forwarding sub-layer functions are supported using the DetNet IP defined by this document. Service protection can be provided on a per sub-net basis using technologies such as MPLS [I-D.ietf-detnet-dp-sol-mpls] and IEEE802.1 TSN.

2. Terminology

[Editor’s note: Needs clean up.]

2.1. Terms Used In This Document

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

2.2. Abbreviations

The following abbreviations used in this document:

- **CE**  Customer Edge equipment.
- **CoS**  Class of Service.
- **DetNet**  Deterministic Networking.
- **DF**  DetNet Flow.
- **L2**  Layer-2.
- **L3**  Layer-3.
- **LSP**  Label-switched path.
- **MPLS**  Multiprotocol Label Switching.
- **OAM**  Operations, Administration, and Maintenance.
- **PE**  Provider Edge.
- **PREOF**  Packet Replication, Ordering and Elimination Function.
- **PSN**  Packet Switched Network.
- **PW**  Pseudowire.
- **QoS**  Quality of Service.
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. DetNet IP Data Plane Overview

[Editor’s note: simplify this section and highlight DetNet IP over subnets scenario being the focus in the remaining part of the document.]

This document describes how IP is used by DetNet nodes, i.e., hosts and routers, to identify DetNet flows and provide a DetNet service. From a data plane perspective, an end-to-end IP model is followed. As mentioned above, existing IP and higher layer protocol header information is used to support flow identification and DetNet service delivery.

DetNet uses "6-tuple" based flow identification, where "6-tuple" refers to information carried in IP and higher layer protocol headers. General background on the use of IP headers, and "5-tuples", to identify flows and support Quality of Service (QoS) can be found in [RFC3670]. [RFC7657] also provides useful background on the delivery differentiated services (DiffServ) and "6-tuple" based flow identification.

DetNet flow aggregation may be enabled via the use of wildcards, masks, prefixes and ranges. IP tunnels may also be used to support flow aggregation. In these cases, it is expected that DetNet aware intermediate nodes will provide DetNet service assurance on the aggregate through resource allocation and congestion control mechanisms.
Figure 1 illustrates a DetNet enabled IP network. The DetNet enabled end systems originate IP encapsulated traffic that is identified as DetNet flows, relay nodes understand the forwarding requirements of the DetNet flow and ensure that node, interface and sub-network resources are allocated to ensure DetNet service requirements. The dotted line around the Service component of the Relay Nodes indicates that the transit routers are DetNet service aware but do not perform any DetNet service sub-layer function, e.g., PREOF. IEEE 802.1 TSN is an example sub-network type which can provide support for DetNet flows and service. The mapping of DetNet IP flows to TSN streams and TSN protection mechanisms is covered in Section 6.

Note: The sub-network can represent a TSN, MPLS or IP network segment.
Figure 2 illustrates a variant of Figure 1, with an MPLS based DetNet network as a sub-network between the relay nodes. It shows a more complex DetNet enabled IP network where an IP flow is mapped to one or more PWs and MPLS (TE) LSPs. The end systems still originate IP encapsulated traffic that is identified as DetNet flows. The relay nodes follow procedures defined in RRR to map each DetNet flow to MPLS LSPs. While not shown, relay nodes can provide service sub-layer functions such as PREOF using DetNet over MPLS, and this is indicated by the solid line for the MPLS facing portion of the Service component. Note that the Transit node is MPLS (TE) LSP aware and performs switching based on MPLS labels, and need not have any specific knowledge of the DetNet service or the corresponding DetNet flow identification. See RRR for details on the mapping of IP flows to MPLS, and [I-D.ietf-detnet-dp-sol-mpls] for general support of DetNet services using MPLS.
Figure 3 illustrates another variant of Figure 1 where the end systems are not DetNet aware. In this case, edge nodes sit at the boundary of the DetNet domain and provide DetNet service proxies for the end applications by initiating and terminating DetNet service for the application’s IP flows. The existing header information or an approach used for aggregation can be used to support DetNet flow identification.

Non-DetNet and DetNet IP packets are identical on the wire. From data plane perspective, the only difference is that there is flow-associated DetNet information on each DetNet node that defines the flow related characteristics and required forwarding behavior. As shown above, edge nodes provide a Service Proxy function that "associates" one or more IP flows with the appropriate DetNet flow-specific information and ensures that the receives the proper traffic treatment within the domain.

Note: The operation of IEEE802.1 TSN end systems over DetNet enabled IP networks is not described in this document. While TSN flows could be encapsulated in IP packets by an IP End System or DetNet Edge Node in order to produce DetNet IP flows, the details of such are out of scope of this document.

5. DetNet IP Data Plane Considerations

[Editor’s note: Sort out what data plane considerations are relevant for sub-net scenarios.]
5.1. DetNet Routers

Within a DetNet domain, the DetNet enabled IP Routers interconnect links and sub-networks to support end-to-end delivery of DetNet flows. From a DetNet architecture perspective, these routers are DetNet relays, as they must be DetNet service aware. Such routers identify DetNet flows based on the IP 6-tuple, and ensure that the DetNet service required traffic treatment is provided both on the node and on any attached sub-network.

This solution provides DetNet functions end to end, but does so on a per link and sub-network basis. Congestion protection and latency control and the resource allocation (queuing, policing, shaping) are supported using the underlying link / sub net specific mechanisms. However, service protections (packet replication and packet elimination functions) are not provided at the DetNet layer end to end. But such service protection can be provided on a per underlying L2 link and sub-network basis.

![Diagram](image)

Figure 4: Encapsulation of DetNet Routing in simplified IP service L3 end-systems

The DetNet Service Flow is mapped to the link / sub-network specific resources using an underlying system specific means. This implies each DetNet aware node on path looks into the forwarded DetNet Service Flow packet and utilize e.g., a 5- (or 6-) tuple to find out the required mapping within a node.

As noted earlier, the Service Protection is done within each link / sub-network independently using the domain specific mechanisms (due the lack of a unified end to end sequencing information that would be available for intermediate nodes). Therefore, service protection (if any) cannot be provided end-to-end, only within sub-networks. This is shown for a three sub-network scenario in Figure 5, where each sub-network can provide service protection between its borders.
Figure 5: Replication and elimination in sub-networks for DetNet IP networks

If end to end service protection is desired that can be implemented, for example, by the DetNet end systems using Layer-4 (L4) transport protocols or application protocols. However, these are out of scope of this document.

5.2. Networks With Multiple Technology Segments

There are network scenarios, where the DetNet domain contains multiple technology segments (IEEE 802.1 TSN, MPLS) and all those segments are under the same administrative control (see Figure 6). Furthermore, DetNet nodes may be interconnected via TSN segments.

DetNet routers ensure that detnet service requirements are met per hop by allocating local resources, both receive and transmit, and by mapping the service requirements of each flow to appropriate sub-network mechanisms. Such mapping is sub-network technology specific. The mapping of DetNet IP Flows to MPLS is covered RRR. The mapping of IP DetNet Flows to IEEE 802.1 TSN is covered in Section 6.
6. Mapping DetNet IP Flows to IEEE 802.1 TSN

[Authors note: how do we handle control protocols such as ICMP, IPsec, etc.]

This section covers how DetNet IP flows operate over an IEEE 802.1 TSN sub-network. Figure 7 illustrates such a scenario, where two IP (DetNet) nodes are interconnected by a TSN sub-network. Node-1 is single homed and Node-2 is dual-homed. IP nodes can be (1) DetNet IP End System, (2) DetNet IP Edge or Relay node or (3) IP End System.

```
 IP (DetNet)          IP (DetNet)
  Node-1              Node-2

<--: Service :-- DetNet flow ----: Service :-->
         +----------+            +----------+
          |Forwarding|            |Forwarding|
             +--------.-+    <-TSN Str->    +-.-----.--+
                      \,-------.     /     /
                       \----[ TSN-Sub ]----+     /     /
                           [ Network ]----+-     /     /
                                \--------'     /     /
                                 \--------'     /

<----------------- DetNet IP ------------------>
```

Figure 7: DetNet (DN) Enabled IP Network over a TSN sub-network

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. Furthermore IEEE 802.1CB [IEEE8021CB] defines frame replication and elimination functions for reliability that should prove both compatible with and useful to, DetNet networks. All these functions have to identify flows those require TSN treatment.
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 may need additional marking, such as the priority field of an IEEE Std 802.1Q VLAN tag, to give the packet proper service.

TSN capabilities of the TSN sub-network are made available for IP (DetNet) flows via the protocol interworking function defined in IEEE 802.1CB [IEEE8021CB]. For example, applied on the TSN edge port connected to the IP (DetNet) node it can convert an ingress unicast IP (DetNet) flow to use a specific multicast destination MAC address and VLAN, in order to direct the packet through a specific path inside the bridged network. A similar interworking pair at the other end of the TSN sub-network would restore the packet to its original destination MAC address and VLAN.

Placement of TSN functions depends on the TSN capabilities of nodes. IP (DetNet) Nodes may or may not support TSN functions. For a given TSN Stream (i.e., DetNet flow) an IP (DetNet) node is treated as a Talker or a Listener inside the TSN sub-network.

6.1. TSN Stream ID Mapping

DetNet IP Flow and TSN Stream mapping is based on the active Stream Identification function, that operates at the frame level. IEEE 802.1CB [IEEE8021CB] defines an Active Destination MAC and VLAN Stream identification function, what can replace some Ethernet header fields namely (1) the destination MAC-address, (2) the VLAN-ID and (3) priority parameters with alternate values. Replacement is provided for the frame passed down the stack from the upper layers or up the stack from the lower layers.

Active Destination MAC and VLAN Stream identification can be used within a Talker to set flow identity or a Listener to recover the original addressing information. It can be used also in a TSN bridge that is providing translation as a proxy service for an End System. As a result IP (DetNet) flows can be mapped to use a particular (MAC-address, VLAN) pair to match the Stream in the TSN sub-network.

From the TSN sub-network perspective DetNet IP nodes without any TSN functions can be treated as TSN-unaware Talker or Listener. In such cases relay nodes in the TSN sub-network MUST modify the Ethernet encapsulation of the DetNet IP flow (e.g., MAC translation, VLAN-ID setting, Sequence number addition, etc.) to allow proper TSN specific handling of the flow inside the sub-network. This is illustrated in Figure 8.
IP (DetNet)
Node-1
<-------->

.............
<-:: Service ---> DetNet flow ------------------
| Forwarding |
| +----------+ +----------+
| L2        | L2 Relay with |---- TSN ----|
|           | TSN function | Stream    |
|++++++.+++++|++++.+++++++++++

TSN-unaware
Talker / TSN-Bridge
Listener    Relay
<-------- TSN sub-network -------

Figure 8: IP (DetNet) node without TSN functions

IP (DetNet) nodes being TSN-aware can be treated as a combination of a TSN-unaware Talker/Listener and a TSN-Relay, as shown in Figure 9. In such cases the IP (DetNet) node MUST provide the TSN sub-network specific Ethernet encapsulation over the link(s) towards the sub-network. An TSN-aware IP (DetNet) node MUST support the following TSN components:

1. For recognizing flows:
   * Stream Identification

2. For FRER used inside the TSN domain, additionally:
   * Sequencing function
   * Sequence encode/decode function

3. For FRER when the node is a replication or elimination point, additionally:
   * Stream splitting function
   * Individual recovery function

[Editor’s note: Should we added here requirements regarding IEEE 802.1Q C-VLAN component?]
A Stream identification component MUST be able to instantiate the following functions (1) Active Destination MAC and VLAN Stream identification function, (2) IP Stream identification function and (3) the related managed objects in Clause 9 of IEEE 802.1CB [IEEE8021CB]. IP Stream identification function provides a 6-tuple match.

The Sequence encode/decode function MUST support the Redundancy tag (R-TAG) format as per Clause 7.8 of IEEE 802.1CB [IEEE8021CB].

6.2. TSN Usage of FRER

TSN Streams supporting DetNet flows may use Frame Replication and Elimination for Redundancy (FRER) [802.1CB] based on the loss service requirements of the TSN Stream, which is derived from the DetNet service requirements of the DetNet mapped flow. The specific operation of FRER is not modified by the use of DetNet and follows IEEE 802.1CB [IEEE8021CB].

FRER function and the provided service recovery is available only within the TSN sub-network (as shown in Figure 5) as the Stream-ID and the TSN sequence number are not valid outside the sub-network. An IP (DetNet) node represents a L3 border and as such it terminates all related information elements encoded in the L2 frames.
6.3. Procedures

[Editor’s note: This section is TBD - covers required behavior of a TSN-aware DetNet node using a TSN underlay.]

This section provides DetNet IP data plane procedures to interwork with a TSN underlay sub-network when the IP (DetNet) node acts as a TSN-aware Talker or Listener (see Figure 9). These procedures have been divided into the following areas: flow identification, mapping of a DetNet flow to a TSN Stream and ensure proper TSN encapsulation.

Flow identification procedures are described in RRR. A TSN-aware IP (DetNet) node SHALL support the Stream Identification TSN components as per IEEE 802.1CB [IEEE8021CB].

Implementations of this document SHALL use management and control information to map a DetNet flow to a TSN Stream. N:1 mapping (aggregating DetNet flows in a single TSN Stream) SHALL be supported. The management or control function that provisions flow mapping SHALL ensure that adequate resources are allocated and configured to provide proper service requirements of the mapped flows.

For proper TSN encapsulation implementations of this document SHALL support active Stream Identification function as defined in chapter 6.6 in IEEE 802.1CB [IEEE8021CB].

A TSN-aware IP (DetNet) node SHALL support Ethernet encapsulation with Redundancy tag (R-TAG) as per chapter 7.8 in IEEE 802.1CB [IEEE8021CB].

Depending whether FRER functions are used in the TSN sub-network to serve the mapped TSN Stream, a TSN-aware IP (DetNet) node SHALL support Sequencing function and Sequence encode/decode function as per chapter 7.4 and 7.6 in IEEE 802.1CB [IEEE8021CB]. Furthermore when a TSN-aware IP (DetNet) node acting as a replication or elimination point for FRER it SHALL implement the Stream splitting function and the Individual recovery function as per chapter 7.7 and 7.5 in IEEE 802.1CB [IEEE8021CB].

7. Management and Control Implications

[Editor’s note: This section is TBD Covers Creation, mapping, removal of TSN Stream IDs, related parameters and, when needed, configuration of FRER. Supported by management/control plane.]

DetNet flow and TSN Stream mapping related information are required only for TSN-aware IP (DetNet) nodes. From the Data Plane
perspective there is no practical difference based on the origin of flow mapping related information (management plane or control plane).

TSN-aware DetNet IP nodes are member of both the DetNet domain and the TSN sub-network. Within the TSN sub-network the TSN-aware IP (DetNet) node has a TSN-aware Talker/Listener role, so TSN specific management and control plane functionalities must be implemented. There are many similarities in the management plane techniques used in DetNet and TSN, but that is not the case for the control plane protocols. For example, RSVP-TE and MSRP behaves differently. Therefore management and control plane design is an important aspect of scenarios, where mapping between DetNet and TSN is required.

In order to use a TSN sub-network between DetNet nodes, DetNet specific information must be converted to TSN sub-network specific ones. DetNet flow ID and flow related parameters/requirements must be converted to a TSN Stream ID and stream related parameters/requirements. Note that, as the TSN sub-network is just a portion of the end2end DetNet path (i.e., single hop from IP perspective), some parameters (e.g., delay) may differ significantly. Other parameters (like bandwidth) also may have to be tuned due to the L2 encapsulation used in the TSN sub-network.

In some case it may be challenging to determine some TSN Stream related information. For example on a TSN-aware IP (DetNet) node that acts as a Talker, it is quite obvious which DetNet node is the Listener of the mapped TSN stream (i.e., the IP Next-Hop). However it may be not trivial to locate the point/interface where that Listener is connected to the TSN sub-network. Such attributes may require interaction between control and management plane functions and between DetNet and TSN domains.

Mapping between DetNet flow identifiers and TSN Stream identifiers, if not provided explicitly, can be done by a TSN-aware IP (DetNet) node locally based on information provided for configuration of the TSN Stream identification functions (IP Stream identification and active Stream identification function).

Triggering the setup/modification of a TSN Stream in the TSN sub-network is an example where management and/or control plane interactions are required between the DetNet and TSN sub-network. TSN-unaware IP (DetNet) nodes make such a triggering even more complicated as they are fully unaware of the sub-network and run independently.

Configuration of TSN specific functions (e.g., FRER) inside the TSN sub-network is a TSN specific decision and may not be visible in the DetNet domain.
8. Security Considerations

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

9. IANA Considerations

TBD.

10. Acknowledgements

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

11. References

11.1. Normative references


Informative references


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