DetNet
Internet-Draft
Intended status: Standards Track
Expires: January 1, 2019

J. Korhonen, Ed.

B. Varga, Ed.
Ericsson

June 30, 2018

# DetNet IP Data Plane Encapsulation
# draft-ietf-detnet-dp-sol-ip-00

## Abstract

This document specifies Deterministic Networking data plane operation for IP encapsulated user data.

## Status of This Memo



## Copyright Notice

Table of Contents



## 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 header information is used to support flow identification and DetNet service delivery. 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.

The DetNet Architecture decomposes the DetNet related data plane functions into two layers: a service layer and a transport layer. The service layer is used to provide DetNet service protection and reordering. The transport layer is used to provides congestion protection (low loss, assured latency, and limited reordering). As no DetNet specific headers are added to support IP DetNet flows, only the transport layer functions are supported using the IP DetNet 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.

This document provides an overview of the DetNet IP data plane in Section 3, considerations that apply to providing DetNet services via the DetNet IP data plane in Section 4 and Section 5. Section 6 provides the requirements for hosts and routers that support IP-based DetNet services. Finally, Section 7 provides rules for mapping IP-based DetNet flows to IEEE 802.1 TSN streams.

## 2. Terminology

### 2.1. Terms used in this document

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

### 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. |
| TE | Traffic Engineering. |
| TSN | Time-Sensitive Networking, TSN is a Task Group of the IEEE 802.1 Working Group. |

### 2.3. 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.

## 3. DetNet IP Data Plane Overview

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.

```
   IP  DetNet       Relay                        Relay       IP DetNet
   End System       Node                         Node        End System

   +---------+                                               +---------+
   |  Appl.  |<---------------- End to End Service ---------->|  Appl.  |
   +---------+    ...........                  ...........   +---------+
   | Service |<---: Service :-- DetNet flow ---: Service :-->| Service |
   +---------+    +---------+                  +---------+   +---------+
   |Transport|    |Transport|                  |Transport|   |Transport|
   +-------.-+    +-.-----.-+                  +-.-----.-+   +---.-----+
           :  Link  :      \       ,-----.      /     /  ,-----.  \
           +........+       +-----[  Sub  ]----+      +-[  Sub  ]-+
                                  [Network]             [Network]
                                   `-----'               `-----'

           |<-DN IP->|    |<----- DetNet IP ---->|      |<-DN IP->|
```

Figure 1: A Simple DetNet (DN) Enabled IP Network

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 transport 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 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 IP DetNet flows to TSN streams and TSN protection mechanisms is covered in Section 7.

```
   IP  DetNet       Relay          Transit       Relay       IP DetNet
   End System       Node            Node         Node        End System

   +---------+                                               +---------+
   |  Appl.  |<--------------- End to End Service ---------->|  Appl.  |
   +---------+    .....-----+                 +-----.....   +---------+
   | Service |<---: Service |-- DetNet flow ---| Service :-->| Service |
   +---------+    +---------+   +---------+    +---------+   +---------+
   |Transport|    |Trp| |Trp|   |Transport|    |Trp| |Trp|   |Transport|
   +-------.-+    +-.-+ +-.-+   +---.---.-+    +-.-+ +-.-+   +---.-----+
           :  Link  :    /  ,-----.  \  :  Link  :    /  ,-----.  \
           +........+    +-[  Sub  ]-+  +........+    +-[  Sub  ]-+
                           [Network]                    [Network]
                            `-----'                      `-----'

           |<-DN IP->|   |<---- DetNet MPLS ---->|      |<-DN IP->|
```

Figure 2: DetNet (DN) IP Over MPLS Network

Figure 2 illustrates 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 [I-D.ietf-detnet-dp-sol-mpls] to map each DetNet flow to MPLS LSPs. While not shown, relay nodes can provide service layer functions such as PREOF over the MPLS transport layer, 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 [I-D.ietf-detnet-dp-sol-mpls] for details on the mapping of IP flows to MPLS as well as general support for DetNet services using MPLS.

```
   IP                Edge                            Edge         IP
   End System        Node                            Node         End System

   +---------+    +.........+                    +.........+   +---------+
   |  Appl.  |<---:Svc Proxy:-- E2E Service ---:Svc Proxy:-->|  Appl.  |
   +---------+    +---------+                    +---------+   +---------+
   |   IP    |    |IP | |Svc|<-- DetNet flow ->|Svc| |IP |   |   IP    |
   +---------+    +---+ +---+                    +---+ +---+   +---------+
   |Transport|    |Trp| |Trp|                    |Trp| |Trp|   |Transport|
   +-------.-+    +-.-+ +-.-+                    +-.-+ +-.-+   +---.-----+
           :  Link  :      \       ,-----.      /     /  ,-----.  \
           +........+       +-----[  Sub  ]---+      +-[  Sub  ]-+
                                  [Network]          [Network]
                                   `-----'            `-----'

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

Figure 3: Non-DetNet aware IP end systems with IP DetNet Domain

Figure 3 illustrates a 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 act as DetNet service proxies for the end applications by initiating and terminating DetNet service for the non-DetNet aware IP flows. The existing header information or an approach such as described in Section 4.7 can be used to support DetNet flow identification.

## 3.1. DetNet IP Flow Identification

DetNet IP flows are identified based on IP, both IPv4 [RFC0791] and IPv6 [RFC8200], header information. 6 header fields are used and this set of fields is commonly referred to as the IP header "6-tuple". The 6 fields include the IP source and destination address fields, the next level protocol or header field, the next level protocol (e.g. TCP or UDP) source and destination ports, and the IPv4 Type of Service or IPv6 Traffic Class field (i.e., DSCP). As part of single DetNet flow identification, any of the fields can be ignored (wildcarded), and bit masks, prefix based longest match, and ranges can also be used.

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.

### 3.2. DetNet Data Plane Requirements

Two major groups of scenarios can be distinguished which require flow identification during transport:

1. DetNet function related scenarios:

   Congestion protection and latency control:

      Usage 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: a reservation that maps a flow to a specific path, which also limits miss-ordering and jitter. The spreading of a single DetNet flow across multiple paths, e.g., via ECMP, also impacts ordering and end-to-end jitter, and as such use of multiple paths for support of a single DetNet flow is is out of scope this document.

   Service protection:

      Which in the case of this document translates to changing the explicit path after a failure is detected while maintaining the required DetNet service characteristics. Path changes, even in the case of failure recovery, can lead to the out of order delivery of data. Note: DetNet PREOF is not provided by the mechanisms defined in this document.

2. OAM function related scenarios:

   Troubleshooting:

      For example, identify misbehaving flows.

   Recognize flow(s) for analytics:

      For example, increase counters.

   Correlate events with flows:

      For example, volume above threshold.

## 4. DetNet IP Data Plane Considerations

This section provides informative considerations related to providing DetNet services via IP.

### 4.1. End-system specific considerations

Data-flows requiring DetNet service are generated and terminated on end systems. The specific protocols used by an end system are specific to an application. This said, DetNet's use of 6-tuple IP flow identification means that DetNet must be aware of not only the format of the IP header, but also of the next protocol carried within an IP packet.

When IP end systems are DetNet aware, no application-level or service-level proxy functions are needed inside the DetNet domain, so end systems peer with end systems using the same application encapsulation format (see Figure 4).

```
             +-----+
             |  X  |                               +-----+
             +-----+                               |  X  |
             |  IP |               _________       +-----+
             +-----+     ______   /        \       |  IP |
                    \   /     \__/          \___   +-----+
                     \ /                        \ /
                      0========= flow-1 =========0_
                      |                             \
                       \                             |
                       0========== flow-2 ==========0
                      / \                        __/ \
               +-----+   \__     DetNet domain  /     \
               |  X  |      \         __       /       +-----+
               +-----+       \_______/  \_____/        |  X  |
               |  IP |                                 +-----+
               +-----+                                 |  IP |
                                                       +-----+
```

Figure 4: End-systems and the DetNet domain

End systems need to ensure that DetNet service requirements are met when processing packets associated with a DetNet flow. When transporting packets, this generally means that packets are appropriately shaped on transmission and received appropriate traffic treatment on the connected sub-network, see Section 4.6 and Section 4.2.1 for more details. When receiving packets, this generally means that there are appropriate local node resources, e.g., buffers, to receive and process a DetNet flow packets.

### 4.2. DetNet domain specific considerations

As a general rule, DetNet domains need to be able to forward any DetNet flow identified by the IP 6-tuple. Doing otherwise would limit end system encapsulation format. From a practical standpoint this means that all nodes along the end-to-end path of a DetNet flows need to agree on what fields are used for flow identification, and the transport protocols (e.g., TCP/UDP/IPsec) which can be used to identify 6-tuple protocol ports.

[Editor's note: Update accordingly. BV to take a pass at update.]

From a connection type perspective three scenarios are identified:

1. Directly attached: end system is directly connected to an edge node.

2. Indirectly attached: end system is behind a (L2-TSN / L3-DetNet) sub-networks.

3. DN integrated: end system is part of the DetNet domain.

L3 end systems may use any of these connection types, however L2 end systems may use only the first two (directly or indirectly attached). DetNet domain MUST allow communication between any end-systems of the same type (L2-L2, L3-L3), independent of their connection type and DetNet capability. However, directly attached and indirectly attached end systems have no knowledge about the DetNet domain and its encapsulation format at all. See Figure 5 for L3 end system connection scenarios.

```
                                               ____+----+
                       +----+        _____    /    | ES3|
                       | ES1|____   /     \__/     +----+___
                       +----+    \ /                        \
                                  +                          |
                          ____     \                        _/
            +----+     __/    \     +__    DetNet domain   /
            | ES2|____/  L2/L3 |___/   \         __     __/
            +----+    \_______/         \_______/  \___/
```

Figure 5: Connection types of L3 end systems

### 4.2.1. 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 emilination 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.

```
                     +------+                         +------+
                     |  X   |                         |  X   |
                     +======+                         +------+
          End-system |  IP  |                         |  IP  |
                -----+------+-------+======+---     --+======+--
          DetNet                    |L2/SbN|          |L2/SbN|
                                    +------+          +------+
```

Figure 6: Encapsulation of DetNet Routing in simplified IP service L3 end-systems

Note: the DetNet Service Flow MUST be mapped to the link / sub-network specific resources using an underlying system specific means. This implies each DetNet aware node on path MUST look into the transported 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). 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.

[Editor's note: the service protection to be clarified further.]

## 4.3. 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 7). 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 IP DetNet Flows to MPLS is covered [I-D.ietf-detnet-dp-sol-mpls].  The mapping of IP DetNet Flows to IEEE 802.1 TSN is covered in Section 7.

```
                                   ______
                         _____    /      \__
            ____        /     \__/          \___    ______
+-----+   __/    +=======+                      +==+      \   +-----+
|src |__/  Seg1  )      |                        |  \  Seg3 \__| dst|
+-----+  \_______+      \        Segment-2       |   \+_____/  +-----+
                 \======+__                     _+===/
                           \         __      __/
                            \_______/  \___/
```

Figure 7: DetNet domains and multiple technology segments

## 4.4. OAM

[Editor's note: This section is TBD]

## 4.5. Class of Service

[Editor's note: this section is TBD]

Class and quality of service, i.e., CoS and QoS, are terms that are often used interchangeably and confused.  In the context of DetNet, CoS is used to refer to mechanisms that provide traffic forwarding treatment based on aggregate group basis and QoS is used to refer to mechanisms that provide traffic forwarding treatment based on a specific DetNet flow basis.  Examples of existing network level CoS mechanisms include DiffServ which is enabled by IP header differentiated services code point (DSCP) field [RFC2474] and MPLS label traffic class field [RFC5462], and at Layer-2, by IEEE 802.1p priority code point (PCP).

CoS for DetNet flows carried in PWs and MPLS is provided using the existing MPLS Differentiated Services (DiffServ) architecture [RFC3270]. Both E-LSP and L-LSP MPLS DiffServ modes MAY be used to support DetNet flows. The Traffic Class field (formerly the EXP field) of an MPLS label follows the definition of [RFC5462] and [RFC3270]. The Uniform, Pipe, and Short Pipe DiffServ tunneling and TTL processing models are described in [RFC3270] and [RFC3443] and MAY be used for MPLS LSPs supporting DetNet flows. MPLS ECN MAY also be used as defined in ECN [RFC5129] and updated by [RFC5462].

CoS for DetNet flows carried in IPv6 is provided using the standard differentiated services code point (DSCP) field [RFC2474] and related mechanisms. The 2-bit explicit congestion notification (ECN) [RFC3168] field MAY also be used.

One additional consideration for DetNet nodes which support CoS services is that they MUST ensure that the CoS service classes do not impact the congestion protection and latency control mechanisms used to provide DetNet QoS. This requirement is similar to requirement for MPLS LSRs to that CoS LSPs do not impact the resources allocated to TE LSPs via [RFC3473].

## 4.6. Quality of Service

[Editor's note: Keep this section. We should document the used technologies but the detailed discussion may go somewhere else. We should start having it here and then decide whether to move to some other document.]

Quality of Service (QoS) mechanisms for flow specific traffic treatment typically includes a guarantee/agreement for the service, and allocation of resources to support the service. Example QoS mechanisms include discrete resource allocation, admission control, flow identification and isolation, and sometimes path control, traffic protection, shaping, policing and remarking. Example protocols that support QoS control include Resource ReSerVation Protocol (RSVP) [RFC2205] (RSVP) and RSVP-TE [RFC3209] and [RFC3473]. The existing MPLS mechanisms defined to support CoS [RFC3270] can also be used to reserve resources for specific traffic classes.

In addition to explicit routes, and packet replication and elimination, DetNet provides zero congestion loss and bounded latency and jitter. As described in [I-D.ietf-detnet-architecture], there are different mechanisms that maybe used separately or in combination to deliver a zero congestion loss service. These mechanisms are provided by the either the MPLS or IP layers, and may be combined with the mechanisms defined by the underlying network layer such as 802.1TSN.

A baseline set of QoS capabilities for DetNet flows carried in PWs and MPLS can provided by MPLS with Traffic Engineering (MPLS-TE) [RFC3209] and [RFC3473]. TE LSPs can also support explicit routes (path pinning). Current service definitions for packet TE LSPs can be found in "Specification of the Controlled Load Quality of Service", [RFC2211], "Specification of Guaranteed Quality of Service", [RFC2212], and "Ethernet Traffic Parameters", [RFC6003]. Additional service definitions are expected in future documents to support the full range of DetNet services. In all cases, the existing label-based marking mechanisms defined for TE-LSPs and even E-LSPs are use to support the identification of flows requiring DetNet QoS.

QoS for DetNet service flows carried in IP MUST be provided locally by the DetNet-aware hosts and routers supporting DetNet flows. Such support will leverage the underlying network layer such as 802.1TSN. The traffic control mechanisms used to deliver QoS for IP encapsulated DetNet flows are expected to be defined in a future document. From an encapsulation perspective, the combination of the "6 tuple" i.e., the typical 5 tuple enhanced with the DSCP code, uniquely identifies a DetNet service flow.

Packets that are marked with a DetNet Class of Service value, but that have not been the subject of a completed reservation, can disrupt the QoS offered to properly reserved DetNet flows by using resources allocated to the reserved flows. Therefore, the network nodes of a DetNet network must:

- o Defend the DetNet QoS by discarding or remarking (to a non-DetNet CoS) packets received that are not the subject of a completed reservation.

- o Not use a DetNet reserved resource, e.g. a queue or shaper reserved for DetNet flows, for any packet that does not carry a DetNet Class of Service marker.

### 4.7. Cross-DetNet flow resource aggregation

[Editor's note: Aggregation is FFS. The addregation can be provided via encapsulation or header wildcards]

The ability to aggregate individual flows, and their associated resource control, into a larger aggregate is an important technique for improving scaling of control in the data, management and control planes. This document identifies the traffic identification related aspects of aggregation of DetNet flows. The resource control and management aspects of aggregation (including the queuing/shaping/ policing implications) will be covered in other documents. The data

plane implications of aggregation are independent for PW/MPLS and IP encapsulated DetNet flows.

DetNet flows transported via IP have more limited aggregation options, due to the available traffic flow identification fields of the IP solution. One available approach is to manage the resources associated with a DSCP identified traffic class and to map (remark) individually controlled DetNet flows onto that traffic class. This approach also requires that nodes support aggregation ensure that traffic from aggregated LSPs are placed (shaped/policed/enqueued) in a fashion that ensures the required DetNet service is preserved.

In both the MPLS and IP cases, additional details of the traffic control capabilities needed at a DetNet-aware node may be covered in the new service descriptions mentioned above or in separate future documents. Management and control plane mechanisms will also need to ensure that the service required on the aggregate flow (H-LSP or DSCP) are provided, which may include the discarding or remarking mentioned in the previous sections.

### 4.8. Time synchronization

While time synchronization can be important both from the perspective of operating the DetNet network itself and from the perspective of DetNet-based applications, time synchronization is outside the scope of this document. This said, a DetNet node can also support time synchronization or distribution mechanisms.

For example, [RFC8169] describes a method of recording the packet queuing time in an MPLS LSR on a packet by per packet basis and forwarding this information to the egress edge system. This allows compensation for any variable packet queuing delay to be applied at the packet receiver. Other mechanisms for IP networks are defined based on IEEE Standard 1588 [IEEE1588], such as ITU-T [G.8275.1] and [G.8275.2].

A more detailed discussion of time synchronization is outside the scope of this document.

## 5. Management and control plane considerations

[Editor's note: This section needs to be different for MPLS and IP solutions. Most solutions are technology dependant.]

While management plane and control plane are traditionally considered separately, from the Data Plane perspective there is no practical difference based on the origin of flow provisioning information. This document therefore does not distinguish between information

provided by a control plane protocol, e.g., RSVP-TE [RFC3209] and [RFC3473], or by a network management mechanisms, e.g., RestConf [RFC8040] and YANG [RFC7950].

[Editor's note: This section is a work in progress. discuss here what kind of enhancements are needed for DetNet and specifically for PREOF and DetNet zero congest loss and latency control. Need to cover both traffic control (queuing) and connection control (control plane).]

## 5.1. Explicit routes

[Editor's note: this is TBD.]

## 5.2. Service protection

[Editor's note: this is TBD.]

## 5.3. Congestion protection and latency control

[Editor's note: this is TBD.]

## 5.4. Flow aggregation control

[Editor's note: this is TBD.]

## 5.5. Bidirectional traffic

[Editor's note: This is managed at the management plane or controller level.]

Some DetNet applications generate bidirectional traffic. While the DetNet data plane must support bidirectional DetNet flows, there are no special bidirectional features with respect to the data plane other than need for the two directions take the same paths. That is to say that bidirectional DetNet flows are solely represented at the management and control plane levels, without specific support or knowledge within the DetNet data plane. Fate sharing and associated vs co-routed bidirectional flows can be managed at the control level. Note, that there is no stated requirement for bidirectional DetNet flows to be supported using the same 6-tuple in each direction. Control mechanisms will need to support such bidirectional flows but such mechanisms are out of scope of this document. An example control plane solution for MPLS can be found in [RFC7551].

## 6. DetNet IP Encapsulation Procedures

[Editor's note: RFC2119 conformance language goes here Need to support flow identification Based on 4 IP header fields {ip addrs, dscp, nct protocol} need to support port identification for TCP/UDP, IPsec spi (?), what else? Service proxies -- basically same from data plane, different from management map to local resources]

### 6.1. Multi-Path Considerations

[Note: talk about implications of ECMP/LAG/parallel links -- perhaps just say support for such is not covered in the document.]

## 7. Mapping IP DetNet Flows to IEEE 802.1 TSN

[Editor's note: This section is TBD - it covers how IP DetNet flows operate over an IEEE 802.1 TSN sub-network. BV to take a pass at filling in this section]

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 IPv6 encapsulations.

### 7.1. TSN Stream ID Mapping

[Editor's Note: This section covers the data plane aspects of mapping an IP DetNet flow to one or more TSN Stream-IDs.]

### 7.2. TSN Usage of FRER

[Core point] TSN Streams support 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 the FRER is not modified by the use of DetNe and follows IEEE 802.1CB [IEEE8021CB].

### 7.3. 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.]

## 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. Contributors

RFC7322 limits the number of authors listed on the front page of a draft to a maximum of 5, far fewer than the 20 individuals below who made important contributions to this draft. The editor wishes to thank and acknowledge each of the following authors for contributing text to this draft. See also Section 11.

Loa Andersson
Huawei
Email: loa@pi.nu

Yuanlong Jiang
Huawei
Email: jiangyuanlong@huawei.com

Norman Finn
Huawei
3101 Rio Way
Spring Valley, CA 91977
USA
Email: norman.finn@mail01.huawei.com

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

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain
Email: cjbc@it.uc3m.es

Tal Mizrahi
Marvell
6 Hamada st.
Yokneam
Israel
Email: talmi@marvell.com

Lou Berger
LabN Consulting, L.L.C.
Email: lberger@labn.net

## 11. Acknowledgements

The author(s) ACK and NACK.

The following people were part of the DetNet Data Plane Solution Design Team:

Jouni Korhonen

Janos Farkas

Norman Finn

Balazs Varga

Loa Andersson

Tal Mizrahi

David Mozes

Yuanlong Jiang

Carlos J. Bernardos

The DetNet chairs serving during the DetNet Data Plane Solution Design Team:

Lou Berger

Pat Thaler

Thanks for Stewart Bryant for his extensive review of the previous versions of the document.

## 12. References

### 12.1. Normative references

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[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/info/rfc2119>.

[RFC2211] Wroclawski, J., "Specification of the Controlled-Load Network Element Service", RFC 2211, DOI 10.17487/RFC2211, September 1997, <https://www.rfc-editor.org/info/rfc2211>.

[RFC2212] Shenker, S., Partridge, C., and R. Guerin, "Specification of Guaranteed Quality of Service", RFC 2212, DOI 10.17487/RFC2212, September 1997, <https://www.rfc-editor.org/info/rfc2212>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <https://www.rfc-editor.org/info/rfc3168>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC3270] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", RFC 3270, DOI 10.17487/RFC3270, May 2002, <https://www.rfc-editor.org/info/rfc3270>.

[RFC3443] Agarwal, P. and B. Akyol, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks", RFC 3443, DOI 10.17487/RFC3443, January 2003, <https://www.rfc-editor.org/info/rfc3443>.

[RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, DOI 10.17487/RFC3473, January 2003, <https://www.rfc-editor.org/info/rfc3473>.

[RFC5129] Davie, B., Briscoe, B., and J. Tay, "Explicit Congestion Marking in MPLS", RFC 5129, DOI 10.17487/RFC5129, January 2008, <https://www.rfc-editor.org/info/rfc5129>.

[RFC5462] Andersson, L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, DOI 10.17487/RFC5462, February 2009, <https://www.rfc-editor.org/info/rfc5462>.

[RFC6003] Papadimitriou, D., "Ethernet Traffic Parameters", RFC 6003, DOI 10.17487/RFC6003, October 2010, <https://www.rfc-editor.org/info/rfc6003>.

[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/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

## 12.2. Informative references

[G.8275.1] International Telecommunication Union, "Precision time protocol telecom profile for phase/time synchronization with full timing support from the network", ITU-T G.8275.1/Y.1369.1 G.8275.1, June 2016, <https://www.itu.int/rec/T-REC-G.8275.1/en>.

[G.8275.2] International Telecommunication Union, "Precision time protocol telecom profile for phase/time synchronization with partial timing support from the network", ITU-T G.8275.2/Y.1369.2 G.8275.2, June 2016, <https://www.itu.int/rec/T-REC-G.8275.2/en>.

[I-D.ietf-detnet-architecture] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", draft-ietf-detnet-architecture-05 (work in progress), May 2018.

[I-D.ietf-detnet-dp-sol-mpls] Korhonen, J., Varga, B., "DetNet MPLS Data Plane Encapsulation", 2018.

[I-D.ietf-detnet-security] Mizrahi, T., Grossman, E., Hacker, A., Das, S., Dowdell, J., Austad, H., Stanton, K., and N. Finn, "Deterministic Networking (DetNet) Security Considerations", draft-ietf-detnet-security-02 (work in progress), April 2018.

[IEEE1588] IEEE, "IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems Version 2", 2008.

[IEEE8021CB]
Finn, N., "Draft Standard for Local and metropolitan area networks - Seamless Redundancy", IEEE P802.1CB /D2.1 P802.1CB, December 2015, <http://www.ieee802.org/1/files/private/cb-drafts/d2/802-1CB-d2-1.pdf>.

[IEEE8021Q]
IEEE 802.1, "Standard for Local and metropolitan area networks--Bridges and Bridged Networks (IEEE Std 802.1Q-2014)", 2014, <http://standards.ieee.org/about/get/>.

[RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, DOI 10.17487/RFC2205, September 1997, <https://www.rfc-editor.org/info/rfc2205>.

[RFC3670] Moore, B., Durham, D., Strassner, J., Westerinen, A., and W. Weiss, "Information Model for Describing Network Device QoS Datapath Mechanisms", RFC 3670, DOI 10.17487/RFC3670, January 2004, <https://www.rfc-editor.org/info/rfc3670>.

[RFC7551] Zhang, F., Ed., Jing, R., and R. Gandhi, Ed., "RSVP-TE Extensions for Associated Bidirectional Label Switched Paths (LSPs)", RFC 7551, DOI 10.17487/RFC7551, May 2015, <https://www.rfc-editor.org/info/rfc7551>.

[RFC7657] Black, D., Ed. and P. Jones, "Differentiated Services (Diffserv) and Real-Time Communication", RFC 7657, DOI 10.17487/RFC7657, November 2015, <https://www.rfc-editor.org/info/rfc7657>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8169] Mirsky, G., Ruffini, S., Gray, E., Drake, J., Bryant, S., and A. Vainshtein, "Residence Time Measurement in MPLS Networks", RFC 8169, DOI 10.17487/RFC8169, May 2017, <https://www.rfc-editor.org/info/rfc8169>.

## Appendix A. Example of DetNet data plane operation

[Editor's note: Add a simplified example of DetNet data plane and how labels etc work in the case of MPLS-based PSN and utilizing PREOF. The figure is subject to change depending on the further DT decisions on the label handling..]

## Appendix B. Example of pinned paths using IPv6

TBD.

Authors' Addresses

Jouni Korhonen (editor)

Email: jouni.nospam@gmail.com

Balazs Varga (editor)
Ericsson
Magyar Tudosok krt. 11.
Budapest 1117
Hungary

Email: balazs.a.varga@ericsson.com