DetNet
Internet-Draft
Intended status: Informational
Expires: March 15, 2020

B. Varga, Ed.
J. Farkas
Ericsson
L. Berger
D. Fedyk
LabN Consulting, L.L.C.
A. Malis
Independent
S. Bryant
Futurewei Technologies
J. Korhonen

September 12, 2019

DetNet Data Plane Framework
draft-ietf-detnet-data-plane-framework-02

Abstract

This document provides an overall framework for the Deterministic Networking data plane. It covers concepts and considerations that are generally common to any Deterministic Networking data plane specification.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Deterministic Networking (DetNet) provides a capability to carry specified unicast or multicast data flows for real-time applications with extremely low packet loss rates and assured maximum end-to-end

delivery latency. A description of the general background and concepts of DetNet can be found in [I-D.ietf-detnet-architecture].

This document describes the concepts needed by any DetNet data plane specification and provides considerations for any corresponding implementation. It covers the building blocks that provide the DetNet service, the DetNet service sub-layer and the DetNet forwarding sub-layer functions as described in the DetNet Architecture.

The DetNet Architecture models the DetNet related data plane functions decomposed 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 provide congestion protection (low loss, assured latency, and limited out-of-order delivery) and leverages Traffic Engineering mechanisms.

As part of the service sub-layer functions, this document describes typical DetNet node data plane operation. It describes the function and operation of the Packet Replication (PRF) Packet Elimination (PEF) and the Packet Ordering (POF) functions within the service sub-layer. It also describes the forwarding sub-layer that is used to eliminate (or reduce) contention loss and provide bounded latency for DetNet flows.

DetNet flows may be carried over network technologies that can provide the DetNet required service characteristics. For example, DetNet MPLS flows can be carried over IEEE 802.1 Time Sensitive Network (TSN) [IEEE802.1TSNTG] sub-networks. However, IEEE 802.1 TSN support is not required and some of the DetNet benefits can be gained by running over a data link layer that has not been specifically enhanced to support TSN.

Different traffic types, or application flows, can be mapped on top of DetNet. DetNet can optionally reuse header information provided by, or shared with, applications. An example of shared header fields can be found in [I-D.ietf-detnet-ip].

This document also covers concepts related to the controller plane and Operations, Administration, and Maintenance (OAM) functions related to the control plane. Data plane OAM specifics are out of scope for this docuement.

2. Terminology

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.

2.2. Abbreviations

The following abbreviations are used in this document:

CW	Control Word.
DetNet	Deterministic Networking.
GRE	Generic Routing Encapsulation.
IPSec	IP Security.
L2	Layer 2.
LSR	Label Switching Router.
MPLS	Multiprotocol Label Switching.
MPLS-TE	Multiprotocol Label Switching - Traffic Engineering.
OAM	Operations, Administration, and Maintenance.
PEF	Packet Elimination Function.
PRF	Packet Replication Function.
PREOF	Packet Replication, Elimination and Ordering Functions.
POF	Packet Ordering Function.
PSN	Packet Switched Network.
PW	PseudoWire.
QoS	Quality of Service.
TSN	Time-Sensitive Network.

3. DetNet Data Plane Overview

This document describes how application flows, or app-flows, are carried over DetNet networks. The DetNet Architecture, [I-D.ietf-detnet-architecture], models the DetNet related data plane functions decomposed into two sub-layers: a service sub-layer and a forwarding sub-layer.

Figure 1 reproduced from the [I-D.ietf-detnet-architecture],shows a logical DetNet service with the two sub-layers.

```
              |  packets going  |          ^  packets coming   ^
              v down the stack  v          |   up the stack    |
           +-----------------------+   +-----------------------+
           |        Source         |   |      Destination      |
           +-----------------------+   +-----------------------+
           |   Service sub-layer:  |   |   Service sub-layer:  |
           |   Packet sequencing   |   | Duplicate elimination |
           |    Flow replication   |   |     Flow merging      |
           |    Packet encoding    |   |    Packet decoding    |
           +-----------------------+   +-----------------------+
           | Forwarding sub-layer: |   | Forwarding sub-layer: |
           |  Resource allocation  |   |  Resource allocation  |
           |    Explicit routes    |   |    Explicit routes    |
           +-----------------------+   +-----------------------+
           |     Lower layers      |   |     Lower layers      |
           +-----------------------+   +-----------------------+
                       v                           ^
                        \_________________________/
```

Figure 1: DetNet data plane protocol stack

The DetNet forwarding sub-layer may be directly provided by the DetNet service sub-layer, for example by IP tunnels or MPLS. Alternatively, an overlay approach may be used in which the packet is natively carried between key nodes within the DetNet network (say between PREOF nodes) and a sub-layer is used to provide the information needed to reach the next hop in the overlay.

The forwarding sub-layer provides the quality underpin needed by the DetNet flow. It may do this directly through the use of queuing techniques and traffic engineering methods, or it may do this through the assistance of its underlying connectivity. For example it may call upon Ethernet TSN capabilities defined in IEEE 802.1 TSN [IEEE802.1TSNTG].

The service sub-layer provides additional support beyond the connectivity function of the forwarding sub-layer. An example of

this is Packet Replication, Elimination, and Ordering (PREOF) functions see Section 4.3.

The method of instantiating each of the layers is specific to the particular DetNet data plane method. There may be more than one approach that is applicable to a given bearer network type.

3.1. Data Plane Characteristics

There are two major characteristics to the data plane:

1. Data plane technology: The DetNet data plane is provided by the DetNet service and forwarding sub layers. The DetNet service sub-layer generally provides its functions for the DetNet application flows by using or applying existing standardized headers and/or encapsulations. The Detnet forwarding sub-layer may provide capabilities leveraging that same header or encapsulation technology e.g. Figure 2 or it may be achieved by other technologies e.g. Figure 3. DetNet is currently defined for operation over packet switched (IP) networks or label switched (MPLS) networks.

2. Encapsulation format: DetNet encodes specific flow attributes (namely flow identity and sequence number) in packets. For example, in DetNet IP, zero encapsulation may be used and no sequence number is available, and in DetNet MPLS, DetNet specific information may be added explicitly to the packets in the format of S-label and d-CW.

```
                          +-------+  +---------+
                          | DN IP |  | DN MPLS |
                          +-------+  +---------+
```

Figure 2: DetNet Services

```
                                             +-----+
                                             | TSN |
                        +--------+         +-+-----+-+
                        | DN IP  |         | DN MPLS |
                     +--+--+----+----+   +-+---+-----+-+
                     | TSN | DN MPLS |   | TSN | DN IP |
                     +-----+---------+   +-----+-------+
```

Figure 3: DetNet Service Examples

3.2. Encapsulation

The encapsulation of the DetNet flows allows them to be sent over a data plane technology other than their native type. Encapsulation is essential if, for example, it is required to send Ethernet TSN stream as a DetNet Application over a data plane such as MPLS. Figure 3 illustrates some relationships between the components.

The use of encapsulation is also required if additional information (meta-data) is needed by the DetNet data plane and there is either no ability to include it in the client data packet, or the specification of the client data plane does not permit the modification of the packet to include additional data. An example of such meta-data is the inclusion of a sequence number required by the PREOF function.

Encapsulation may also be used to carry or aggregate flows for equipment with limited DetNet capability.

3.3. DetNet Specific Metadata

The DetNet data plane can provide or carry meta-data:

1. Flow-ID

2. Sequence Number

Both of these metadata are required for DetNet service sub-layer specific functions (e.g., PREOF). DetNet forwarding sub-layer related functions require only Flow-ID.

Metadata can be a useful way of identifying packets that need to be treated as a flow or flow aggregate. It is also useful as a way of including a sequence number the packet for use by the PREOF function or as a place to carry OAM indications or OAM information to instrument DetNet data plane operation.

Explicit inclusion of metadata is possible through the use of IP options or IP extension headers. New IP options are almost impossible to get standardized or to deploy in an operational network and will not be discussed further in this text. IPv6 extensions headers are finding popularity in current IPv6 development work, particularly in connection with Segment Routing of IPv6 (SRv6) and IP OAM. The design of a new IPv6 extension header or the modification of an existing one is a technique available in the tool box of the DetNet IP data plane designer.

Explicit inclusion of metadata in an IP packet is also possible through the inclusion of an MPLS label stack and the MPLS DetNet Control Word using one of the methods for carrying MPLS over IP [I-D.ietf-detnet-mpls-over-udp-ip]. This is described in more detail in Section 3.6.4.

Implicit metadata in IP can be included through the use of the network programming paradigm [I-D.ietf-spring-srv6-network-programming] in which the suffix of an IPv6 address is used to encode additional information for use by the network of the receiving host.

Some MPLS examples of implicit metadata include the sequence number for use by the PREOF function, or even all the essential information being included into the DetNet over MPLS label stack (the DetNet Control Word and the DetNet Service label).

3.4. DetNet IP Data Plane

An IP data plane may operate natively or through the use of an encapsulation. Many types of IP encapsulation can satisfy DetNet requirements and it is anticipated that more than one encapsulation may be deployed for example GRE, IPSec etc.

One method of operating an IP DetNet data plane without encapsulation is to use "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 "6-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 "tuple" based flow identification. DetNet flow aggregation may be enabled via the use of wildcards, masks, prefixes and ranges. The operation of this method is described in detail in [I-D.ietf-detnet-ip].

The DetNet forwarding plane may use explicit route capabilities and traffic engineering capabilities to provide a forwarding sub-layer that is responsible for providing resource allocation and explicit

routes. It is possible to include such information in a native IP packet explicitly, or implicitly.

3.5. DetNet MPLS Data Plane

MPLS provides the ability to forward traffic over implicit and explicit paths to the point in the network where the next DetNet service sub-layer action needs to take place. It does this through the use of a stack of one or more labels with various forwarding semantics.

MPLS also provides the ability to identify a service instance that is used to process the packet through the use of a label that maps the packet to a service instance.

In cases where metadata is needed to process an MPLS encapsulated packet at the service sub-layer, a shim layer also called a control word (CW) [RFC4385] can be used. Although such CWs are frequently 32 bits long, there is no architectural constraint on its size of this structure, only the requirement that it is fully understood by all parties operating on it in the DetNet service sub-layer. The operation of this method is described in detail in [I-D.ietf-detnet-mpls].

3.6. Further DetNet Data Plane Considerations

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:

Reservation and Allocation of resources:

Reservation of resources can allocate resources to specific DetNet flows. This can eliminate packet contention and loss for DetNet traffic. This also can reduce jitter for the DetNet traffic. DetNet flows are assumed to behave with respect to the reserved traffic profile. If other traffic shares the link resources, the use of (queuing, policing, shaping) policies can be used to ensure that the allocation of resources reserved for DetNet is met. Queuing and shaping of DetNet traffic could be required to ensure that DetNet traffic does not exceed its reserved profile but this would impact the DetNet service characteristics.

Explicit routes:

Use of a specific path for a flow. This allows control of the network delay by steering the packet with the ability to influence

the physical path. Explicit routes complement reservation by ensuring that a consistent path can be associated with its resources for the duration of that path. Coupled with the traffic mechanism, this limits misordering and bounds latency. Explicit route computation can encompass a wide set of constraints and optimize the path for a certain characteristic e.g. highest bandwidth or lowest jitter. In these cases the "best" path for any set of characteristics may not be a shortest path. The selection of path can take into account multiple network metrics. Some of these metrics are measured and distributed by the routing system as traffic engineering metrics.

Service protection:

Use of multiple packet streams using multiple paths, for example 1+1 or 1:1 linear protection. For DetNet this primarily relates to packet replication and elimination capabilities. MPLS offers a number of protection schemes. MPLS hitless protection can be used to switch traffic to an already established path in order to restore delivery rapidly after a failure. Path changes, even in the case of failure recovery, can lead to the out of order delivery of data requiring packet ordering functions either within the DetNet service or at a high layer in the application traffic. Establishment of new paths after a failure is out of scope for DetNet services.

Network Coding:

Network Coding, not to be confused with network programming, comprises several techniques where multiple data flows are encoded. These resulting flows can then be sent on different paths. The encoding operation can combine flows and error recovery information. When the encoded flows are decoded and recombined the original flows can be recovered. Note that Network coding uses an alternative to packet by packet PREOF. Therefore, for certain network topologies and traffic loads, Network Coding can be used to improve a network's throughput, efficiency, latency, and scalability, as well as resilience to partition, attacks, and eavesdropping, as compared to traditional methods. DetNet could utilized Network coding as an alternative to other protection means. Network coding is often applied in wireless networks and is being explored for other network types.

Load sharing:

Use of packet by packet distribution of the same DetNet flow over multiple paths is not recommended except for the cases listed above where PREOF is utilized to improve protection of traffic and

maintain order. Packet by packet load sharing, e.g., via ECMP or UCMP, impacts ordering and possibly jitter.

Troubleshooting:

Since Detnet leverages many different forwarding sub-layers, those technologies also support a number of tools to troubleshoot connectivity for example, to support identification of misbehaving flows. At the service layer again there are existing mechanisms to troubleshoot or monitor flows. Many of these mechanisms exist for IP and MPLS networks. A client of a DetNet service can introduce any monitoring applications which can detect and monitor delay and loss.

Recognize flow(s) for analytics:

To a large degree this follows the logic in the previous section. Analytics can be inherited from the two sub-layers. At the DetNet service edge packet and bit counters e.g. sent, received, dropped, and out of sequence are maintained.

Correlate events with flows:

The provider of a DetNet service may allow other capabilities to monitor flows such as more detail loss statistics and time stamping of events. The details of these capabilities are currently out of scope for this document.

Several of these capabilities are expanded upon in more detail below.

3.6.1. Service Protection

Service protection allow DetNet services to increase reliability and maintain a DetNet Service Assurance in the case of network congestion or some failures. Detnet relies on the underlying technology capabilities for various protection schemes. Protection schemes enable partial or complete coverage of the network paths and active protection with combinations of PRF, PRE, and POF.

3.6.1.1. Linear Service Protection

An example DetNet MPLS network fragment and packet flow is illustrated in Figure 4.

```
            1      1.1       1.1      1.2.1    1.2.1      1.2.2
         CE1----EN1--------R1-------R2-------R3--------EN2-----CE2
                  \           1.2.1 /                   /
                   \1.2     /-----+                   /
                    +------R4------------------------+
                              1.2.2
```

Figure 4: Example Packet Flow in DetNet protected Network

In Figure 4 the numbers are used to identify the instance of a packet. Packet 1 is the original packet, and packets 1.1, and 1.2 are two first generation copies of packet 1. Packet 1.2.1 is a second generation copy of packet 1.2 etc. Note that these numbers never appear in the packet, and are not to be confused with sequence numbers, labels or any other identifier that appears in the packet. They simply indicate the generation number of the original packet so that its passage through the network fragment can be identified to the reader.

Customer Equipment CE1 sends a packet into the DetNet enabled network. This is packet (1). Edge Node EN1 encapsulates the packet as a DetNet Packet and sends it to Relay node R1 (packet 1.1). EN1 makes a copy of the packet (1.2), encapsulates it and sends this copy to Relay node R4.

Note that along the path from EN1 to R1 there may be zero or more nodes which, for clarity, are not shown. The same is true for any other path between two DetNet entities shown in Figure 4 .

Relay node R4 has been configured to send one copy of the packet to Relay Node R2 (packet 1.2.1) and one copy to Edge Node EN2 (packet 1.2.2).

R2 receives packet copy 1.2.1 before packet copy 1.1 arrives, and, having been configured to perform packet elimination on this DetNet flow, forwards packet 1.2.1 to Relay Node R3. Packet copy 1.1 is of no further use and so is discarded by R2.

Edge Node EN2 receives packet copy 1.2.2 from R4 before it receives packet copy 1.2.1 from R2 via relay Node R3. EN2 therefore strips any DetNet encapsulation from packet copy 1.2.2 and forwards the packet to CE2. When EN2 receives the later packet copy 1.2.1 this is discarded.

The above is of course illustrative of many network scenarios that can be configured.

This example also illustrates 1:1 protection scheme meaning there is traffic and path for each segment of the end to end path. Local DetNet relay nodes determine which packets are eliminated and which packets are forwarded. A 1+1 scheme where only one path is used for traffic at a time, could use the same topology. In this case there is no PRF function and traffic is switched upon detection of failure. An OAM scheme that monitors the paths detects the loss of path or traffic is required to initiate the switch. A POF may still be used in this case to prevent misordering of packets. In both cases the protection paths are established and maintained for the duration of the DetNet service.

3.6.1.2. Ring Service Protection

Ring protection may also be supported if the underlying technology supports it. Many of the same concepts apply however Rings are normally 1+1 protection for data efficiency reasons. [RFC8227] is an example of MPLS-TP data plane that supports Ring protection.

3.6.2. Aggregation Considerations

The DetNet data plane also allows for the aggregation of DetNet flows, to improved scaling by reducing the state per hop. How this is accomplished is data plane or control plane dependent. When DetNet flows are aggregated, transit nodes provide service to the aggregate and not on a per-DetNet flow basis. When aggregating DetNet flows the flows should be compatible i.e. the same or very similar QoS and CoS characteristics. In this case, nodes performing aggregation will ensure that per-flow service requirements are achieved.

If bandwidth reservations are used, the sum of the reservations should be the sum of all the individual reservations, in other words, the reservations should not create an over subscription of bandwidth reservation. If maximum delay bounds are used the system should ensure that the aggregate does not exceed the delay bounds of the individual flows.

DetNet encapsulation is a data plane mechanism that can be used to aggregate traffic. Encapsulation can either be in the same service type or in a different service type see Figure 3 for example. When an encapsulation is used the choice of reserving a maximum resource level and then tracking the services in the aggregated service or adjusting the aggregated resources as the services are added is implementation and technology specific.

DetNet flows at edges must be able to handle rejection to an aggregation group due to lack of resources as well as conditions where general requirements are not satisfied.

3.6.2.1. IP Aggregation

IP aggregation has both data plane and controller plane aspects. For the data plane flows may be aggregated for treatment based on shared characteristics such as 6-tuple. Alternatively, an IP encapsulation may be used to tunnel an aggregate number of DetNet Flows between relay nodes.

3.6.2.2. MPLS Aggregation

MPLS aggregation similarly has data plane and controller plane aspects. In the case of MPLS flows are often tunneled in a forwarding sub-layer and reservation is associated with that MPLS tunnel.

3.6.3. End-System Specific Considerations

Data-flows requiring DetNet service are generated and terminated on end-systems. Encapsulation depends on the application and its preferences. For example, 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.

As a general rule, DetNet domains are capable of forwarding any DetNet 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 5, IP applications peer with IP applications and Ethernet applications peer with Ethernet applications.

```
             +-----+
             |  X  |                               +-----+
             +-----+                               |  X  |
             | Eth |               ________        +-----+
             +-----+     _____    /        \       | Eth |
                    \   /     \__/          \___   +-----+
                     \ /                        \ /
                      0======== tunnel-1 ========0_
                      |                             \
                       \                             |
                       0========= tunnel-2 =========0
                      / \                        __/ \
               +-----+   \__ DetNet MPLS domain /     \
               |  X  |      \         __       /       +-----+
               +-----+       \_______/  \_____/        |  X  |
               |  IP |                                 +-----+
               +-----+                                 |  IP |
                                                       +-----+
```

Figure 5: End-Systems and The DetNet MPLS Domain

3.6.4. Sub-Network Considerations

Any of the DetNet service types may be transported by another DetNet service. MPLS nodes may interconnected by different sub-network technologies, which may include point-to-point links. Each of these sub-network technologies need to provide appropriate service to DetNet flows. In some cases, e.g., on dedicated point-to-point links or TDM technologies, all that is required is for a DetNet node to appropriately queue its output traffic. In other cases, DetNet nodes will need to map DetNet flows to the flow semantics (i.e., identifiers) and mechanisms used by an underlying sub-network technology. Figure 6 shows several examples of header formats that can be used to carry DetNet MPLS flows over different sub-network technologies. L2 represent a generic layer-2 encapsulation that might be used on a point-to-point link. TSN represents the encapsulation used on an IEEE 802.1 TSN network, as described in [I-D.ietf-detnet-mpls-over-tsn]. UDP/IP represents the encapsulation used on a DetNet IP PSN, as described in [I-D.ietf-detnet-mpls-over-udp-ip].

```
                              +------+  +------+  +------+
           App-Flow           |  X   |  |  X   |  |  X   |
                        +-----+======+--+======+--+======+-----+
           DetNet-MPLS        | d-CW |  | d-CW |  | d-CW |
                              +------+  +------+  +------+
                              |Labels|  |Labels|  |Labels|
                        +-----+======+--+======+--+======+-----+
           Sub-Network        |  L2  |  | TSN  |  | UDP  |
                              +------+  +------+  +------+
                                                  |  IP  |
                                                  +------+
                                                  |  L2  |
                                                  +------+
```

Figure 6: Example DetNet MPLS Sub-Network Formats

4. Controller Plane (Management and Control) Considerations

4.1. DetNet Controller Plane Requirements

While the definition of controller plane for DetNet is out of the scope of this document, there are particular considerations and requirements for such that result from the unique characteristics of the DetNet architecture [I-D.ietf-detnet-architecture] and data plane as defined herein.

The primary requirements of the DetNet controller plane are that it must be able to:

- Instantiate DetNet flows in a DetNet domain (which may include some or all of explicit path determination, link bandwidth reservations, restricting flows to IEEE 802.1 TSN links, node buffer and other resource reservations, specification of required queuing disciplines along the path, ability to manage bidirectional flows, etc.) as needed for a flow.

- In the case of MPLS, manage DetNet S-Label and F-Label allocation and distribution, where the DetNet MPLS encapsulation is in use see [I-D.ietf-detnet-mpls].

- Support DetNet flow aggregation.

- Advertise static and dynamic node and link resources such as capabilities and adjacencies to other network nodes (for dynamic signaling approaches) or to network controllers (for centralized approaches).

- Scale to handle the number of DetNet flows expected in a domain (which may require per-flow signaling or provisioning).

- Provision flow identification information at each of the nodes along the path. Flow identification may differ depending on the location in the network and the DetNet functionality (e.g. transit node vs. relay node).

These requirements, as stated earlier, could be satisfied using distributed control protocol signaling (such as RSVP-TE), centralized network management provisioning mechanisms (such as BGP, PCEP, YANG [I-D.ietf-detnet-flow-information-model], etc.) or hybrid combinations of the two, and could also make use of MPLS-based segment routing.

In the abstract, the results of either distributed signaling or centralized provisioning are equivalent from a DetNet data plane perspective - flows are instantiated, explicit routes are determined, resources are reserved, and packets are forwarded through the domain using the DetNet data plane.

However, from a practical and implementation standpoint, they are not equivalent at all. Some approaches are more scalable than others in terms of signaling load on the network. Some can take advantage of global tracking of resources in the DetNet domain for better overall network resource optimization. Some are more resilient than others if link, node, or management equipment failures occur. While a detailed analysis of the control plane alternatives is out of the scope of this document, the requirements from this document can be used as the basis of a later analysis of the alternatives.

4.2. Generic Controller Plane Considerations

This section covers control plane considerations that are independent of the data plane technology used for DetNet service delivery.

While management plane and control planes are traditionally considered separately, from the Data Plane perspective there is no practical difference based on the origin of flow provisioning information, and the DetNet architecture [I-D.ietf-detnet-architecture] refers to these collectively as the 'Controller Plane'. This document therefore does not distinguish between information provided by distributed control plane protocols, e.g., RSVP-TE [RFC3209] and [RFC3473], or by centralized network management mechanisms, e.g., RestConf [RFC8040], YANG [RFC7950], and the Path Computation Element Communication Protocol (PCEP) [I-D.ietf-pce-pcep-extension-for-pce-controller] or any combination

thereof. Specific considerations and requirements for the DetNet Controller Plane are discussed in Section 4.1.

Each respective data plane document also covers the control plane considerations for that technology. For example [I-D.ietf-detnet-ip] covers IP control plane normative considerations and [I-D.ietf-detnet-mpls] covers MPLS control plane normative considerations.

4.2.1. Flow Aggregation Control

Flow aggregation includes aggregation accomplished through the use of hierarchical LSPs in MPLS and tunnels, in the case of IP, MPLS and TSN, all of which aggregate multiple DetNet flows into a single new DetNet flow. Aggregation can also be grouping of IP flows that share 6-tuple attributes or flow identifiers at the DetNet sub-layer.

Control of aggregation involves a set of procedures listed here. Aggregation may use some or all of these capabilities and the order may vary:

- Traffic engineering resource collection and distribution:

  Available resources are tracked through control plane or management plane databases and distributed amongst controllers or nodes that can manage resources.

- Path computation and resource allocation:

  When DetNet services are provisioned or requested one or more paths meeting the requirements are selected and the resources verified and recorded.

- Resource assignment and data plane co-ordination:

  The assignment of resources along the path depends on the technology and it includes assignment of specific links and coordination of the queuing and other traffic management capabilities such as policing and shaping.

- Assigned Resource recording and updating:

  Depending on the specific technology the assigned resources are updated and distributed in the databases preventing over subscription.

4.2.2. Explicit Routes

Explicit routes are used to ensure that packets are routed through the resources that have been reserved for them, and hence provide the DetNet application with the required service. A requirement for the DetNet Controller Plane will be the ability to assign a particular identified DetNet IP flow to a path through the DetNet domain that has been assigned the required nodal resources. This provides the appropriate traffic treatment for the flow and also includes particular links as a part of the path that are able to support the DetNet flow. For example, by using IEEE 802.1 TSN links (as discussed in [I-D.ietf-detnet-mpls-over-tsn]) DetNet parameters can be maintained. Further considerations and requirements for the DetNet Controller Plane are discussed in Section 4.1.

Whether configuring, calculating and instantiating these routes is a single-stage or multi-stage process, or in a centralized or distributed manner, is out of scope of this document.

There are several approaches that could be used to provide explicit routes and resource allocation in the DetNet forwarding sub-layer. For example:

- The path could be explicitly set up by a controller which calculates the path and explicitly configures each node along that path with the appropriate forwarding and resource allocation information.

- The path could use a distributed control plane such as RSVP [RFC2205] or RSVP-TE [RFC3473] extended to support DetNet IP flows.

- The path could be implemented using IPv6-based segment routing when extended to support resource allocation.

See Section 4.1 for further discussion of these alternatives. In addition, [RFC2386] contains useful background information on QoS-based routing, and [RFC5575] discusses a specific mechanism used by BGP for traffic flow specification and policy-based routing.

4.2.3. Contention Loss and Jitter Reduction

As discussed in Section 1, this document does not specify the mechanisms needed to eliminate packet contention, packet loss or reduce jitter for DetNet flows at the DetNet forwarding sub-layer. The ability to manage node and link resources to be able to provide these functions is a necessary part of the DetNet controller plane. It is also necessary to be able to control the required queuing

mechanisms used to provide these functions along a flow's path through the network. See [I-D.ietf-detnet-ip] and Section 4.1 for further discussion of these requirements.

4.2.4. Bidirectional Traffic

DetNet applications typically generate bidirectional traffic. IP and MPLS typically treat each direction separately and do not force interdependence of each direction. MPLS has considered bidirectional traffic requirements and the MPLS definitions from [RFC5654] are useful to illustrate terms such as associated bidirectional flows and co-routed bidirectional flows. MPLS defines a point-to-point associated bidirectional LSP as consisting of two unidirectional point-to-point LSPs, one from A to B and the other from B to A, which are regarded as providing a single logical bidirectional forwarding path. This is analogous to standard IP routing. MPLS defines a point-to-point co-routed bidirectional LSP as an associated bidirectional LSP which satisfies the additional constraint that its two unidirectional component LSPs follow the same path (in terms of both nodes and links) in both directions. An important property of co-routed bidirectional LSPs is that their unidirectional component LSPs share fate. In both types of bidirectional LSPs, resource reservations may differ in each direction. The concepts of associated bidirectional flows and co-routed bidirectional flows can also be applied to DetNet IP flows.

While the DetNet IP data plane must support bidirectional DetNet flows, there are no special bidirectional features with respect to the data plane other than the need for the two directions of a co-routed bidirectional flow to take the same path. 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 or co-routed bidirectional flows, can be managed at the control level.

DetNet's use of PREOF may increase the complexity of using co-routing bidirectional flows, since if PREOF is used, then the replication points in one direction would have to match the elimination points in the other direction, and vice versa, and the optimal points for these functions in one direction may not match the optimal points in the other subsequent to the network and traffic constraints. Furthermore, due to the per packet service protection nature, bidirectional forwarding per packet may not be ensured. The first packet of received member flows is selected by the elimination function independently of which path it has taken through the network.

Control and management mechanisms need to support bidirectional flows, but the specification of such mechanisms are out of scope of this document. An example control plane solution for MPLS can be found in [RFC3473] , [RFC6387] and [RFC7551]. These requirements are included in Section 4.1.

4.3. Packet Replication, Elimination, and Ordering (PREOF)

The controller plane protocol solution required for managing the PREOF processing is outside the scope of this document. That said, it should be noted that the ability to determine, for a particular flow, optimal packet replication and elimination points in the DetNet domain requires explicit support. There may be capabilities that can be used, or extended, for example GMPLS end-to-end recovery [RFC4872] and GMPLS segment recovery [RFC4873].

5. Security Considerations

Security considerations for DetNet are described in detail in [I-D.ietf-detnet-security]. General security considerations are described in [I-D.ietf-detnet-architecture]. This section considers general security considerations applicable to all data planes.

Security aspects which are unique to DetNet are those whose aim is to provide the specific quality of service aspects of DetNet, which are primarily to deliver data flows with extremely low packet loss rates and bounded end-to-end delivery latency.

The primary considerations for the data plane is to maintain integrity of data and delivery of the associated DetNet service traversing the DetNet network. Application flows can be protected through whatever means is provided by the underlying technology. For example, encryption may be used, such as that provided by IPSec [RFC4301] for IP flows and/or by an underlying sub-net using MACSec [IEEE802.1AE-2018] for Ethernet (Layer-2) flows.

From a data plane perspective DetNet does not add or modify any header information.

At the management and control level DetNet flows are identified on a per-flow basis, which may provide controller plane attackers with additional information about the data flows (when compared to controller planes that do not include per-flow identification). This is an inherent property of DetNet which has security implications that should be considered when determining if DetNet is a suitable technology for any given use case.

To provide uninterrupted availability of the DetNet service, provisions can be made against DOS attacks and delay attacks. To protect against DOS attacks, excess traffic due to malicious or malfunctioning devices can be prevented or mitigated, for example through the use of existing mechanism such as policing and shaping applied at the input of a DetNet domain. To prevent DetNet packets from being delayed by an entity external to a DetNet domain, DetNet technology definition can allow for the mitigation of Man-In-The-Middle attacks, for example through use of authentication and authorization of devices within the DetNet domain.

6. IANA Considerations

This document makes no IANA requests.

7. Acknowledgements

The authors wish to thank Pat Thaler, Norman Finn, Loa Anderson, David Black, Rodney Cummings, Ethan Grossman, Tal Mizrahi, David Mozes, Craig Gunther, George Swallow, Yuanlong Jiang and Carlos J. Bernardos for their various contributions to this work.

8. References

8.1. Normative References

[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>.

[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>.

[RFC4385] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, DOI 10.17487/RFC4385, February 2006, <https://www.rfc-editor.org/info/rfc4385>.

8.2. Informative References

[I-D.ietf-detnet-architecture]
Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", draft-ietf-detnet-architecture-13 (work in progress), May 2019.

[I-D.ietf-detnet-flow-information-model]
Farkas, J., Varga, B., Cummings, R., Jiang, Y., and D. Fedyk, "DetNet Flow Information Model", draft-ietf-detnet-flow-information-model-05 (work in progress), September 2019.

[I-D.ietf-detnet-ip]
Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane: IP", draft-ietf-detnet-ip-01 (work in progress), July 2019.

[I-D.ietf-detnet-mpls]
Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane: MPLS", draft-ietf-detnet-mpls-01 (work in progress), July 2019.

[I-D.ietf-detnet-mpls-over-tsn]
Varga, B., Farkas, J., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane: MPLS over IEEE 802.1 Time Sensitive Networking (TSN)", draft-ietf-detnet-mpls-over-tsn-00 (work in progress), May 2019.

[I-D.ietf-detnet-mpls-over-udp-ip]
Varga, B., Farkas, J., Berger, L., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane: MPLS over UDP/IP", draft-ietf-detnet-mpls-over-udp-ip-01 (work in progress), July 2019.

[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-05 (work in progress), August 2019.

[I-D.ietf-pce-pcep-extension-for-pce-controller]
Zhao, Q., Li, Z., Negi, M., and C. Zhou, "PCEP Procedures and Protocol Extensions for Using PCE as a Central Controller (PCECC) of LSPs", draft-ietf-pce-pcep-extension-for-pce-controller-02 (work in progress), July 2019.

[I-D.ietf-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J., daniel.voyer@bell.ca, d., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-01 (work in progress), July 2019.

[IEEE802.1AE-2018]
IEEE Standards Association, "IEEE Std 802.1AE-2018 MAC Security (MACsec)", 2018, <https://ieeexplore.ieee.org/document/8585421>.

[IEEE802.1TSNTG]
IEEE Standards Association, "IEEE 802.1 Time-Sensitive Networking Task Group", <http://www.ieee802.org/1/tsn>.

[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>.

[RFC2386] Crawley, E., Nair, R., Rajagopalan, B., and H. Sandick, "A Framework for QoS-based Routing in the Internet", RFC 2386, DOI 10.17487/RFC2386, August 1998, <https://www.rfc-editor.org/info/rfc2386>.

[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>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4872] Lang, J., Ed., Rekhter, Y., Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, DOI 10.17487/RFC4872, May 2007, <https://www.rfc-editor.org/info/rfc4872>.

[RFC4873] Berger, L., Bryskin, I., Papadimitriou, D., and A. Farrel, "GMPLS Segment Recovery", RFC 4873, DOI 10.17487/RFC4873, May 2007, <https://www.rfc-editor.org/info/rfc4873>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <https://www.rfc-editor.org/info/rfc5575>.

[RFC5654] Niven-Jenkins, B., Ed., Brungard, D., Ed., Betts, M., Ed., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, DOI 10.17487/RFC5654, September 2009, <https://www.rfc-editor.org/info/rfc5654>.

[RFC6387] Takacs, A., Berger, L., Caviglia, D., Fedyk, D., and J. Meuric, "GMPLS Asymmetric Bandwidth Bidirectional Label Switched Paths (LSPs)", RFC 6387, DOI 10.17487/RFC6387, September 2011, <https://www.rfc-editor.org/info/rfc6387>.

[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>.

[RFC8227] Cheng, W., Wang, L., Li, H., van Helvoort, H., and J. Dong, "MPLS-TP Shared-Ring Protection (MSRP) Mechanism for Ring Topology", RFC 8227, DOI 10.17487/RFC8227, August 2017, <https://www.rfc-editor.org/info/rfc8227>.

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

Lou Berger
LabN Consulting, L.L.C.

Email: lberger@labn.net

Don Fedyk
LabN Consulting, L.L.C.

Email: dfedyk@labn.net

Andrew G. Malis
Independent

Email: agmalis@gmail.com

Stewart Bryant
Futurewei Technologies

Email: stewart.bryant@gmail.com

Jouni Korhonen

Email: jouni.nospam@gmail.com