Internet Engineering Task Force (IETF)
Request for Comments: 9016
Category: Informational
ISSN: 2070-1721

B. Varga
J. Farkas
Ericsson
R. Cummings
National Instruments
Y. Jiang
Huawei
D. Fedyk
LabN Consulting

March 2021

Flow and Service Information Model for Deterministic Networking (DetNet)

Abstract

This document describes the flow and service information model for Deterministic Networking (DetNet). These models are defined for IP and MPLS DetNet data planes.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9016.

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 [RFC8655].

This document describes the DetNet flow and service information model. For reference, [RFC3444] describes the rationale behind information models in general. This document describes the flow and service information models for operators and users to understand DetNet services and for implementors as a guide to the functionality required by DetNet services.

The DetNet architecture treats 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 provides resource allocation (to ensure low loss, assured latency, and limited out-of-order delivery) and leverages traffic engineering mechanisms.

DetNet service utilizes IP or MPLS, and DetNet is currently defined for IP and MPLS networks, as shown in Figure 1, which is a reprint of Figure 2 from [RFC8938]. IEEE 802.1 Time-Sensitive Networking (TSN) utilizes Ethernet and is defined over Ethernet networks. A DetNet flow includes one or more application-level flow (App-flow) as payload. App-flows can be Ethernet, MPLS, or IP flows, which impacts which header fields are utilized to identify a flow. DetNet flows are identified by the DetNet encapsulation of App-flow(s) (e.g., MPLS labels, IP 6-tuples, etc.). In some scenarios, App-flow and DetNet flow look similar on the wire (e.g., Layer 3 (L3) App-flow over a DetNet IP network).

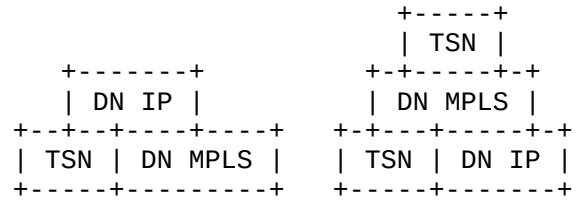


Figure 1: DetNet Service Examples as per Data Plane Framework

As shown in Figure 1 and as described in [RFC8938], a DetNet flow can be treated as an App-flow, e.g., at DetNet flow aggregation or in a sub-network that interconnects DetNet nodes.

The DetNet flow and service information model provided by this document contains both DetNet-flow- and App-flow-specific information in an integrated fashion.

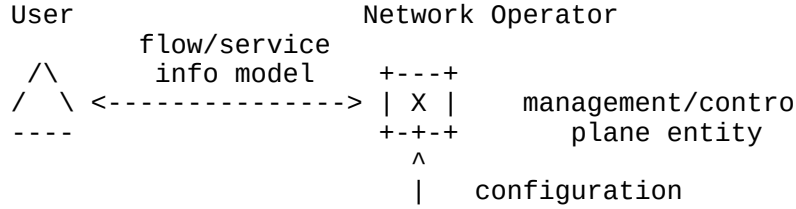
In a given network scenario, three information models can be distinguished:

* Flow information models that describe characteristics of data flows. These models describe, in detail, all relevant aspects of a flow that are needed to support the flow properly by the network between the source and the destination(s).

* Service information models that describe characteristics of services being provided for data flows over a network. These models can be treated as an information model that is network operator independent.

* Configuration information models that describe, in detail, the settings required on network nodes to provide proper service to a data flow.

Service and flow information models are used between the user and the network operator. Configuration information models are used between the management/control plane entity of the network and the network nodes. They are shown in Figure 2.



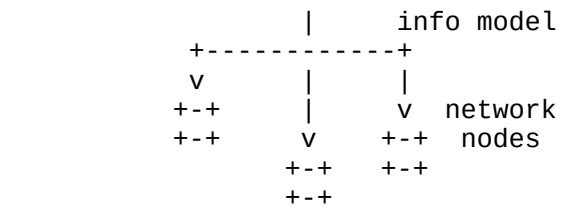


Figure 2: Usage of Information Models (Flow, Service, and Configuration)

The DetNet flow and service information model is based on [RFC8655] and the concept of the data model specified by [IEEE8021Qcc]. In addition to the TSN data model, [IEEE8021Qcc] also specifies configuration of TSN features (e.g., traffic scheduling specified by [IEEE8021Qbv]). The common architecture and flow information model allow configured features to be consistent in certain deployment scenarios, e.g., when the network that provides the DetNet service includes both L3 and L2 network segments.

1.1. Goals

As expressed in the DetNet WG Charter [IETFDetNet], the DetNet WG collaborates with IEEE 802.1 TSN in order to define a common architecture for both Layers 2 and 3. This is beneficial for several reasons, e.g., in order to simplify implementations and maintain consistency across diverse networks. The flow and service information models are also aligned for those reasons. Therefore, the DetNet flow and service information models described in this document are based on [IEEE8021Qcc], which is an amendment to [IEEE8021Q].

This document specifies flow and service information models only.

1.2. Non-Goals

This document does not specify flow data models or DetNet configuration. Therefore, the goals of this document differ from the goals of [IEEE8021Qcc], which also specifies the TSN data model and configuration of certain TSN features.

The DetNet-specific YANG data model is described in [DETNET-YANG].

2. Terminology

2.1. Terms Used in This Document

This document uses the terminology established in the DetNet architecture [RFC8655] and the DetNet data plane framework [RFC8938]. The reader is assumed to be familiar with these documents and any terminology defined therein. The DetNet <=> TSN dictionary of [RFC8655] is used to perform translation from [IEEE8021Qcc] to this document.

The following terminology is used in accordance with [RFC8655]:

App-flow: The payload (data) carried over a DetNet service.

DetNet flow: A sequence of packets that conform uniquely to a flow identifier and to which the DetNet service is to be provided. It includes any DetNet headers added to support the DetNet service and forwarding sub-layers.

The following terminology is introduced in this document:

Source: Reference point for an App-flow, where the flow starts.

Destination	Reference point for an App-flow, where the flow terminates.
DN Ingress	Reference point for the start of a DetNet flow. Networking technology-specific encapsulation may be added here to the served App-flow(s).
DN Egress	Reference point for the end of a DetNet flow. Networking technology-specific encapsulation may be removed here from the served App-flow(s).

2.2. Abbreviations

The following abbreviations are used in this document:

DetNet	Deterministic Networking
DN	DetNet
MPLS	Multiprotocol Label Switching
PSN	Packet Switched Network
TSN	Time-Sensitive Networking

2.3. Naming Conventions

The following naming conventions were used for naming information model components in this document. It is recommended that extensions of the model use the same conventions.

* Descriptive names are used.

* Names start with uppercase letters.

* Composed names use capital letters for the first letter of each component. All other letters are lowercase, even for abbreviations. Exceptions are made for abbreviations containing a mixture of lowercase and capital letters, such as IPv6. Example composed names are SourceMacAddress and DestinationIPv6Address.

3. DetNet Domain and Its Modeling

3.1. DetNet Service Overview

The DetNet service can be defined as a service that provides a capability to carry a unicast or a multicast data flow for an application with constrained requirements on network performance, e.g., low packet loss rate and/or latency.

Figures 5 and 8 in [RFC8655] show the DetNet service-related reference points and main components.

3.2. Reference Points Used in Modeling

From a service-design perspective, a fundamental question is the location of the service/flow endpoints, i.e., where the service/flow starts and ends.

App-flow-specific reference points are the source (where it starts) and the destination (where it terminates). Similarly, a DetNet flow has reference points termed "DN Ingress" (where a DetNet flow starts) and "DN Egress" (where a DetNet flow ends). These reference points may coexist in the same node (e.g., in a DetNet IP end system). DN Ingress and DN Egress reference points are intermediate reference

points for a served App-flow.

In this document, all reference points are assumed to be packet-based reference points. A DN Ingress may add and a DN Egress may remove networking technology-specific encapsulation to/from the served App-flow(s) (e.g., MPLS label(s), UDP, and IP headers).

3.3. Information Elements

The DetNet flow information model and the service information model rely on three groups of information elements:

App-flow-related parameters: These describe the App-flow characteristics (e.g., identification, encapsulation, traffic specification, endpoints, status, etc.) and the App-flow service expectations (e.g., delay, loss, etc.).

DetNet flow-related parameters: These describe the DetNet flow characteristics (e.g., identification, format, traffic specification, endpoints, rank, etc.).

DetNet service-related parameters: These describe the expected service characteristics (e.g., delivery type, connectivity delay/loss, status, rank, etc.).

In the information model, a DetNet flow contains one or more (aggregated) App-flows (N:1 mapping). During DetNet aggregation, the aggregated DetNet flows are treated simply as App-flows and the aggregate is the DetNet flow, which provides N:1 mapping. Similarly, there is an aggregated many-to-one relationship for the DetNet flow(s) to the DetNet service.

4. App-Flow-Related Parameters

When DetNet service is required by time-/loss-sensitive application(s) running on an end system during communication with its peer(s), the resulting data exchange has various requirements on delay and/or loss parameters.

4.1. App-Flow Characteristics

App-flow characteristics are described by the following parameters:

FlowID: a unique (management) identifier of the App-flow, which can be used to define the N:1 mapping of App-flows to a DetNet flow

FlowType: set by the encapsulation format of the flow, which can be Ethernet (TSN), MPLS, or IP

DataFlowSpecification: a flow descriptor, defining which packets belongs to a flow, using specific packet header fields, such as src-addr, dst-addr, label, VLAN-ID, etc.

TrafficSpecification: a flow descriptor, defining traffic parameters, such as packet size, transmission time interval, and maximum packets per time interval

FlowEndpoints: delineates the start and end reference points of the App-flow by pointing to the source interface/node and destination interface(s)/node(s)

FlowStatus: indicates the status of the App-flow with respect to the establishment of the flow by the connected network, e.g., ready, failed, etc.

FlowRank: indicates the rank of this flow relative to other flows in the connected network

> | Note: When defining the N:1 mapping of App-flows to a DetNet flow, the App-flows must have the same FlowType and different DataFlowSpecification parameters.

4.2. App-Flow Requirements

App-flow requirements are described by the following parameters:

FlowRequirements: defines the attributes of the App-flow regarding bandwidth, latency, latency variation, loss, and misordering tolerance

FlowBiDir: defines the data path requirement of the App-flow whether it must share the same data path and physical path for both directions through the network, e.g., to provide congruent paths in the two directions

5. DetNet Flow-Related Parameters

The data model specified by [IEEE8021Qcc] describes data flows using TSN service as periodic flows with fixed packet size (i.e., Constant Bitrate (CBR) flows) or with variable packet size. The same concept is applied for flows using DetNet service.

Latency and loss parameters are correlated because the effect of late delivery can result in data loss for an application. However, not all applications require hard limits on both latency and loss. For example, some real-time applications allow graceful degradation if loss happens (e.g., sample-based data processing and media distribution). Some other applications may require high-bandwidth connections that make use of packet replication techniques that are economically challenging or even impossible. Some applications may not tolerate loss but are not delay sensitive (e.g., bufferless sensors). Time- or loss-sensitive applications may have somewhat special requirements, especially for loss (e.g., no loss over two consecutive communication cycles, very low outage time, etc.).

DetNet flows have the following attributes:

a. DnFlowID (Section 5.1)
b. DnPayloadType (Section 5.2)
c. DnFlowFormat (Section 5.3)
d. DnFlowSpecification (Section 5.4)
e. DnTrafficSpecification (Section 5.5)
f. DnFlowEndpoints (Section 5.6)
g. DnFlowRank (Section 5.7)
h. DnFlowStatus (Section 5.8)

DetNet flows have the following requirement attributes:

a. DnFlowRequirements (Section 5.9)
b. DnFlowBiDir (Section 5.10)

Flow attributes are described in the following sections.

5.1. Management ID of the DetNet Flow

A unique (management) identifier is needed for each DetNet flow within the DetNet domain. It is specified by DnFlowID. It can be used to define the N:1 mapping of DetNet flows to a DetNet service.

5.2. Payload Type of the DetNet Flow

The DnPayloadType attribute is set according to the encapsulated App-flow format. The attribute can be Ethernet, MPLS, or IP.

5.3. Format of the DetNet Flow

The DnFlowFormat attribute is set according to the DetNet PSN technology. The attribute can be MPLS or IP.

5.4. Identification and Specification of DetNet Flows

Identification options for DetNet flows at the Ingress/Egress and within the DetNet domain are specified as follows; see Section 5.4.1 for DetNet MPLS flows and Section 5.4.2 for DetNet IP flows.

5.4.1. DetNet MPLS Flow Identification and Specification

The identification of DetNet MPLS flows within the DetNet domain is based on the MPLS context in the service information model. The attributes are specific to the MPLS forwarding paradigm within the DetNet domain [RFC8964]. DetNet MPLS flows can be identified and specified by the following attributes:

a. SLabel
b. FLabelStack

5.4.2. DetNet IP Flow Identification and Specification

DetNet IP flows can be identified and specified by the following attributes [RFC8939]:

a. SourceIpAddress
b. DestinationIpAddress
c. IPv6FlowLabel
d. Dscp
e. Protocol
f. SourcePort
g. DestinationPort
h. IPSecSpi

The IP 6-tuple that is used for DetNet IP flow identification consists of items a, b, d, e, f, and g. Items c and h are additional attributes that can be used for DetNet flow identification in addition to the 6-tuple. The 6-tuple and use of wild cards for these attributes are specified in [RFC8939].

5.5. Traffic Specification of the DetNet Flow

The DnTrafficSpecification attributes specify how the DN Ingress transmits packets for the DetNet flow. This is effectively the promise/request of the DN Ingress to the network. The network uses this traffic specification to allocate resources and adjust queue parameters in network nodes.

TrafficSpecification has the following attributes:

a. Interval: the period of time in which the traffic specification is specified

b. MaxPacketsPerInterval: the maximum number of packets that the Ingress will transmit in one Interval

c. MaxPayloadSize: the maximum payload size that the Ingress will transmit

d. MinPayloadSize: the minimum payload size that the Ingress will transmit

e. MinPacketsPerInterval: the minimum number of packets that the Ingress will transmit in one Interval

These attributes can be used to describe any type of traffic (e.g., CBR, Variable Bitrate (VBR), etc.) and can be used during resource allocation to represent worst-case scenarios. Intervals are specified as an integer number of nanoseconds. PayloadSizes are specified in octets.

Flows exceeding the traffic specification (i.e., having more traffic than defined by the maximum attributes) may receive a different network behavior than the DetNet network has been engineered for. Excess traffic due to malicious or malfunctioning devices can be prevented or mitigated (e.g., through the use of existing mechanisms, such as policing and shaping).

When MinPayloadSize and MinPacketsPerInterval parameters are used, all packets less than the MinPayloadSize will be counted as being of the size MinPayloadSize during packet processing when packet size matters, e.g., when policing; all flows having less than MinPacketsPerInterval will be counted as having MinPacketsPerInterval when the number of packets per interval matters, e.g., during resource reservation. However, flows having less than MinPacketsPerInterval may result in a different network behavior than the DetNet network has been engineered for. MinPayloadSize and MinPacketsPerInterval parameters, for example, may be used when engineering the latency bounds of a DetNet flow when Packet Ordering Function (POF) is applied to the given DetNet flow.

Further optional attributes can be considered to achieve more efficient resource allocation. Such optional attributes might be worth for flows with soft requirements (i.e., the flow is only loss sensitive or only delay sensitive but not both delay and loss sensitive). Possible options about how to extend DnTrafficSpecification attributes is for further discussion.

5.6. Endpoints of the DetNet Flow

The DnFlowEndpoints attribute defines the start and end reference points of the DetNet flow by pointing to the ingress interface/node and egress interface(s)/node(s). Depending on the network scenario, it defines an interface or a node. Interface can be defined, for example, if the App-flow is a TSN Stream, and it is received over a well-defined User-to-Network Interface (UNI). For example, for App-flows with MPLS encapsulation, defining an ingress node is more common when a per-platform label space is used.

5.7. Rank of the DetNet Flow

The DnFlowRank attribute provides the rank of this flow relative to other flows in the DetNet domain. Rank (range: 0-255) is used by the DetNet domain to decide which flows can and cannot exist when network resources reach their limit. Rank is used to help to determine which flows can be bumped (i.e., removed from node configuration thereby releasing its resources) if, for example, a port of a node becomes oversubscribed (e.g., due to network reconfiguration). DnFlowRank value 0 is the highest priority.

5.8. Status of the DetNet Flow

The DnFlowStatus attribute provides the status of the DetNet flow with respect to the establishment of the flow by the DetNet domain.

DnFlowStatus includes the following attributes:

a. DnIngressStatus is an enumeration for the status of the flow's Ingress reference point:

   None: No Ingress.
   Ready: Ingress is ready.
   Failed: Ingress failed.
   OutOfService: Administratively blocked.

b. DnEgressStatus is an enumeration for the status of the flow's Egress reference points:

   None: No Egress.
   Ready: All Egresses are ready.
   PartialFailed: One or more Egress is ready, and one or more Egress failed. The DetNet flow can be used if the Ingress is Ready.
   Failed: All Egresses failed.
   OutOfService: All Egresses are administratively blocked.

c. FailureCode is a nonzero code that specifies the error if the DetNet flow encounters a failure (e.g., packet replication and elimination is requested but not possible or DnIngressStatus is Failed, DnEgressStatus is Failed, or DnEgressStatus is PartialFailed).

Defining FailureCodes for DetNet is out of scope for this document. Table 46-1 of [IEEE8021Qcc] describes TSN failure codes.

5.9. Requirements of the DetNet Flow

The DnFlowRequirements attribute specifies requirements to ensure the service level desired for the DetNet flow.

DnFlowRequirements includes the following attributes:

a. MinBandwidth (Section 5.9.1)
b. MaxLatency (Section 5.9.2)
c. MaxLatencyVariation (Section 5.9.3)
d. MaxLoss (Section 5.9.4)
e. MaxConsecutiveLossTolerance (Section 5.9.5)
f. MaxMisordering (Section 5.9.6)

5.9.1. Minimum Bandwidth of the DetNet Flow

MinBandwidth is the minimum bandwidth that has to be guaranteed for the DetNet flow. MinBandwidth is specified in octets per second.

5.9.2. Maximum Latency of the DetNet Flow

MaxLatency is the maximum latency from Ingress to Egress(es) for a single packet of the DetNet flow. MaxLatency is specified as an integer number of nanoseconds.

5.9.3. Maximum Latency Variation of the DetNet Flow

MaxLatencyVariation is the difference between the minimum and the maximum end-to-end, one-way latency. MaxLatencyVariation is specified as an integer number of nanoseconds.

5.9.4. Maximum Loss of the DetNet Flow

MaxLoss defines the maximum Packet Loss Rate (PLR) requirement for the DetNet flow between the Ingress and Egress(es) and the loss measurement interval.

5.9.5. Maximum Consecutive Loss of the DetNet Flow

Some applications have special loss requirements, such as MaxConsecutiveLossTolerance. The maximum consecutive loss tolerance parameter describes the maximum number of consecutive packets whose loss can be tolerated. The maximum consecutive loss tolerance can be measured, for example, based on sequence number.

5.9.6. Maximum Misordering Tolerance of the DetNet Flow

MaxMisordering describes the tolerable maximum number of packets that can be received out of order. The value zero for the maximum allowed misordering indicates that in-order delivery is required; misordering cannot be tolerated.

The maximum allowed misordering can be measured, for example, based on sequence numbers. When a packet arrives at the egress after a packet with a higher sequence number, the difference between the sequence number values cannot be bigger than "MaxMisordering + 1".

5.10. BiDir Requirement of the DetNet Flow

The DnFlowBiDir attribute defines the requirement that the flow and the corresponding reverse direction flow must share the same path (links and nodes) through the routed or switch network in the DetNet domain, e.g., to provide congruent paths in the two directions that share fate and path characteristics.

6. DetNet Service-Related Parameters

The DetNet service has the following attributes:

a. DnServiceID (Section 6.1)
b. DnServiceDeliveryType (Section 6.2)
c. DnServiceDeliveryProfile (Section 6.3)
d. DNServiceConnectivity (Section 6.4)
e. DnServiceBiDir (Section 6.5)
f. DnServiceRank (Section 6.6)
g. DnServiceStatus (Section 6.7)

Service attributes are described in the following sections.

6.1. Management ID of the DetNet Service

The DnServiceId attribute is a unique (management) identifier for each DetNet service within the DetNet domain. It can be used to define the many-to-one mapping of DetNet flows to a DetNet service.

6.2. Delivery Type of the DetNet Service

The DnServiceDeliveryType attribute is set according to the payload of the served DetNet flow (i.e., the encapsulated App-flow format). The attribute can be Ethernet, MPLS, or IP.

6.3. Delivery Profile of the DetNet Service

The DnServiceDeliveryProfile attribute specifies the delivery profile to ensure proper serving of the DetNet flow.

DnServiceDeliveryProfile includes the following attributes:

a. MinBandwidth (Section 6.3.1)
b. MaxLatency (Section 6.3.2)
c. MaxLatencyVariation (Section 6.3.3)
d. MaxLoss (Section 6.3.4)
e. MaxConsecutiveLossTolerance (Section 6.3.5)
f. MaxMisordering (Section 6.3.6)

6.3.1. Minimum Bandwidth of the DetNet Service

MinBandwidth is the minimum bandwidth that has to be guaranteed for the DetNet service. MinBandwidth is specified in octets per second and excludes additional DetNet header (if any).

6.3.2. Maximum Latency of the DetNet Service

MaxLatency is the maximum latency from Ingress to Egress(es) for a single packet of the DetNet flow. MaxLatency is specified as an integer number of nanoseconds.

6.3.3. Maximum Latency Variation of the DetNet Service

MaxLatencyVariation is the difference between the minimum and the maximum end-to-end, one-way latency. MaxLatencyVariation is specified as an integer number of nanoseconds.

6.3.4. Maximum Loss of the DetNet Service

MaxLoss defines the maximum Packet Loss Rate (PLR) parameter for the DetNet service between the Ingress and Egress(es) of the DetNet domain.

6.3.5. Maximum Consecutive Loss of the DetNet Service

Some applications have a special loss requirement, such as MaxConsecutiveLossTolerance. The maximum consecutive loss tolerance parameter describes the maximum number of consecutive packets whose loss can be tolerated. The maximum consecutive loss tolerance can be measured, for example, based on sequence number.

6.3.6. Maximum Misordering Tolerance of the DetNet Service

MaxMisordering describes the tolerable maximum number of packets that can be received out of order. The maximum allowed misordering can be measured, for example, based on sequence number. The value zero for the maximum allowed misordering indicates that in-order delivery is required; misordering cannot be tolerated.

6.4. Connectivity Type of the DetNet Service

Two connectivity types are distinguished: point-to-point (p2p) and point-to-multipoint (p2mp). Connectivity type p2mp may be created by a forwarding function (e.g., p2mp LSP). (Note that from a service perspective, mp2mp connectivity can be treated as a superposition of p2mp connections.)

6.5. BiDir Requirement of the DetNet Service

The DnServiceBiDir attribute defines the requirement that the flow and the corresponding reverse direction flow must share the same path (links and nodes) through the routed or switch network in the DetNet domain, e.g., to provide congruent paths in the two directions that share fate and path characteristics.

6.6. Rank of the DetNet Service

The DnServiceRank attribute provides the rank of a service instance relative to other services in the DetNet domain. DnServiceRank (range: 0-255) is used by the network in case of network resource limitation scenarios. DnServiceRank value 0 is the highest priority.

6.7. Status of the DetNet Service

The DnServiceStatus information group includes elements that specify the status of the service-specific state of the DetNet domain. This information group informs the user whether or not the service is ready for use.

DnServiceStatus includes the following attributes:

a. DnServiceIngressStatus is an enumeration for the status of the service's Ingress:

   None: No Ingress.
   Ready: Ingress is ready.
   Failed: Ingress failed.
   OutOfService: Administratively blocked.

b. DnServiceEgressStatus is an enumeration for the status of the service's Egress:

   None: No Egress.
   Ready: All Egresses are ready.
   PartialFailed: One or more Egress is ready, and one or more Egress failed. The DetNet flow can be used if the Ingress is Ready.
   Failed: All Egresses failed.
   OutOfService: Administratively blocked.

c. DnServiceFailureCode is a nonzero code that specifies the error if the DetNet service encounters a failure (e.g., packet replication and elimination is requested but not possible or DnServiceIngressStatus is Failed, DnServiceEgressStatus is Failed, or DnServiceEgressStatus is PartialFailed).

Defining DnServiceFailureCodes for DetNet service is out of scope for this document. Table 46-1 of [IEEE8021Qcc] describes TSN failure codes.

7. Flow-Specific Operations

The DetNet flow information model relies on three high-level information groups:

DnIngress: The DnIngress information group includes elements that specify the source for a single DetNet flow. This information group is applied from the user of the DetNet service to the network.

DnEgress: The DnEgress information group includes elements that specify the destination for a single DetNet flow. This information group is applied from the user of the DetNet service to the network.

DnFlowStatus: The DnFlowStatus information group includes elements that specify the status of the flow in the network. This information group is applied from the network to the user of the DetNet service. This information group informs the user whether or not the DetNet flow is ready for use.

There are three possible operations for each DetNet flow with respect to its DetNet service at a DN Ingress or a DN Egress (similar to App-flows at a source or a destination):

Join: DN Ingress/DN Egress intends to join the flow.
Leave: DN Ingress/DN Egress intends to leave the flow.
Modify: DN Ingress/DN Egress intends to change the flow.

7.1. Join Operation

For the join operation, the DnFlowSpecification, DnFlowRank, DnFlowEndpoint, and DnTrafficSpecification are included within the DnIngress or DnEgress information groups. For the join operation, the DnServiceRequirements groups can be included.

7.2. Leave Operation

For the leave operation, the DnFlowSpecification and DnFlowEndpoint are included within the DnIngress or DnEgress information groups.

7.3. Modify Operation

For the modify operation, the DnFlowSpecification, DnFlowRank, DnFlowEndpoint, and DnTrafficSpecification are included within the DnIngress or DnEgress information group. For the join operation, the DnServiceRequirements groups can be included.

The Modify operation can be considered to address cases when a flow is slightly changed, e.g., only MaxPayloadSize (Section 5.5) has been changed. The advantage of having a Modify is that it allows initiation of a change of flow spec while leaving the current flow operating until the change is accepted. If there is no linkage between the Join and the Leave, then while figuring out whether the new flow spec can be supported, the controller entity has to assume that the resources committed to the current flow are in use. By using Modify, the controller entity knows that the resources supporting the current flow can be available for supporting the altered flow. Modify is considered to be an optional operation due to possible controller plane limitations.

8. Summary

This document describes the DetNet flow information model and the service information model for DetNet IP networks and DetNet MPLS networks. These models are used as input for creating the DetNet-specific YANG module.

9. IANA Considerations

This document has no IANA actions.

10. Security Considerations

The external interfaces of the DetNet domain need to be subject to appropriate confidentiality. Additionally, knowledge of which flows/services are provided to a customer or delivered by a network operator may supply information that can be used in a variety of security attacks. Security considerations for DetNet are described in detail in [DETNET-SECURITY]. General security considerations are described in [RFC8655]. This document discusses modeling the information, not how it is exchanged.

11. References

11.1. Normative References

[IEEE8021Qcc]
IEEE, "IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks -- Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements",
DOI 10.1109/IEEESTD.2018.8514112, IEEE 802.1Qcc-2018, October 2013,
<https://ieeexplore.ieee.org/document/8514112/>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[RFC8939] Varga, B., Ed., Farkas, J., Berger, L., Fedyk, D., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP", RFC 8939, DOI 10.17487/RFC8939, November 2020, <https://www.rfc-editor.org/info/rfc8939>.

[RFC8964] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., Bryant, S., and J. Korhonen, "Deterministic Networking (DetNet) Data Plane: MPLS", RFC 8964, DOI 10.17487/RFC8964, January 2021, <https://www.rfc-editor.org/info/rfc8964>.

11.2. Informative References

[DETNET-SECURITY] Grossman, E., Mizrahi, T., and A. J. Hacker, "Deterministic Networking (DetNet) Security Considerations", Work in Progress, Internet-Draft, draft-ietf-detnet-security-16, 2 March 2021, <https://tools.ietf.org/html/draft-ietf-detnet-security-16>.

[DETNET-YANG] Geng, X., Chen, M., Ryoo, Y., Fedyk, D., Rahman, R., and Z. Li, "Deterministic Networking (DetNet) YANG Model", Work in Progress, Internet-Draft, draft-ietf-detnet-yang-11, 19 February 2021, <https://tools.ietf.org/html/draft-ietf-detnet-yang-11>.

[IEEE8021Q] IEEE, "IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks", DOI 10.1109/IEEESTD.2018.8403927, IEEE 802.1Q-2018, July 2018, <https://ieeexplore.ieee.org/document/8403927>.

[IEEE8021Qbv] IEEE, "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic", DOI 10.1109/IEEESTD.2016.8613095, IEEE 802.1Qbv-2015, March 2016, <https://ieeexplore.ieee.org/document/8613095>.

[IETFDetNet] IETF, "Deterministic Networking (detnet)", <https://datatracker.ietf.org/wg/detnet/charter/>.

[RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between Information Models and Data Models", RFC 3444, DOI 10.17487/RFC3444, January 2003, <https://www.rfc-editor.org/info/rfc3444>.

[RFC8938] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane Framework", RFC 8938, DOI 10.17487/RFC8938, November 2020, <https://www.rfc-editor.org/info/rfc8938>.

Authors' Addresses

Balzs Varga
Ericsson
Budapest
Magyar Tudosok krt. 11.

1117
Hungary

Email: balazs.a.varga@ericsson.com

Jnos Farkas
Ericsson
Budapest
Magyar Tudosok krt. 11.
1117
Hungary

Email: janos.farkas@ericsson.com

Rodney Cummings
National Instruments
Bldg. C
11500 N. Mopac Expwy
Austin, TX 78759-3504
United States of America

Email: rodney.cummings@ni.com

Yuanlong Jiang
Huawei
Bantian, Longgang district
Shenzhen
518129
China

Email: jiangyuanlong@huawei.com

Don Fedyk
LabN Consulting, L.L.C.

Email: dfedyk@labn.net