

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 9, 2020

X. Geng
Z. Li
M. Chen
Huawei
July 8, 2019

SRv6 for Deterministic Networking (DetNet)
draft-geng-spring-srv6-for-detnet-00

Abstract

Deterministic Networking provides service with low jitter, bounded latency and low loss rate, using technologies of explicit route, resource reservation and service protection. This document specifies how to implement Deterministic Networking (DetNet) in a SRv6 Network.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2020.

Copyright Notice

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

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	SRv6 for DetNet Overview	4
4.	Service Protection	5
4.1.	Service Protection Scenarios	6
4.2.	Data Plane Considerations	8
4.3.	Control Plane Considerations	8
4.4.	Functions for Service Protection	9
4.4.1.	End. B. Replication: Packet Replication Function	9
4.4.2.	End. B. Elimination: Packet Elimination Function	9
5.	Explicit Route	10
6.	IANA Considerations	10
7.	Security Considerations	10
8.	Acknowledgements	10
9.	Normative References	10
	Authors' Addresses	11

[1.](#) Introduction

With more and more applications running in the Internet, quality of the service gains more and more attention, especially for some new applications, for example Cloud VR, Cloud Game, HDV (high-definition video) and so on, SLA (Service Level Agreement), including jitter, delay and loss rate, influences the users' experience significantly. So SLA guarantee is an important issue which requires new technologies and solutions for the network.

Deterministic Networking (DetNet defined in [\[I-D.ietf-detnet-architecture\]](#)) provides a capability to carry specified data flows for real-time applications with extremely low data loss rates, low jitter and bounded latency within a network domain. Techniques used include: 1) providing explicit paths for DetNet flows that satisfies the SLA requirement from user and do not immediately change with the network topology; 2) reserving data plane resources for DetNet flows along the allocated path of the flow; 3) replicates DetNet flows into two or more copies and transport different copies through different path in parallel, called service protection.

Segment Routing(SR) leverages the source routing paradigm. An ingress node steers a packet through an ordered list of instructions, called "segments". SR can be applied over IPv6 data plane using Routing Extension Header(SRH, [\[I-D.ietf-6man-segment-routing-header\]](#)). A segment in Segment Routing is not limited to a routing/forwarding function. An SRv6 Segment can indicate functions that are executed locally in the node where they are defined.

[\[I-D.filsfils-spring-srv6-network-programming\]](#) describes some well-known functions and segments associated to them. SRH TLVs([\[I-D.ietf-6man-segment-routing-header\]](#)) also provides meta-data for segment processing. All these features make SRv6 suitable to carry DetNet flows, by defining new segments associated with DetNet functions and meta data for DetNet.

This document describes the concepts needed by implementing DetNet in an SRv6-based domain and provides considerations for any corresponding implementation.

Editor's note:

1. DetNet is limited in a controlled network domain, and it is not the only method to provide SLA guarantee. But it is a good start to discuss how to use SRv6 to have a SLA-guaranteed network service.
2. Resource Reservation will be added in future work.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

Terminologies for DetNet go along with the definition in [\[I-D.ietf-detnet-architecture\]](#) and [\[I-D.ietf-6man-segment-routing-header\]](#):

DetNet domain

The portion of a network that is DetNet aware. It includes end systems and DetNet nodes

DetNet edge node

An instance of a DetNet relay node that acts as a source and/ or destination at the DetNet service sub-layer. For example, it can include a DetNet service sub-layer proxy function for DetNet service protection (e.g., the addition or removal of packet

sequencing information) for one or more end systems, or starts or terminates resource allocation at the DetNet forwarding sub-layer, or aggregates DetNet services into new DetNet flows. It is analogous to a Label Edge Router (LER) or a Provider Edge (PE) router.

DetNet relay node

A DetNet node including a service sub-layer function that interconnects different DetNet forwarding sub-layer paths to provide service protection. A DetNet relay node participates in the DetNet service sub-layer. It typically incorporates DetNet forwarding sub-layer functions as well, in which case it is collocated with a transit node.

DetNet transit node

A DetNet node operating at the DetNet forwarding sub-layer, that utilizes link layer and/or network layer switching across multiple links and/or sub-networks to provide paths for DetNet service sub-layer functions. Typically provides resource allocation over those paths. An MPLS LSR is an example of a DetNet transit node.

End system

End systems of interest to this document are either sources or destinations of DetNet flows. An end system may or may not be DetNet forwarding sub-layer aware or DetNet service sub-layer aware.

DetNet service sub-layer

DetNet functionality is divided into two sub-layers. One of them is the DetNet service sub-layer, at which a DetNet service, e.g., service protection is provided.

DetNet forwarding sub-layer

DetNet functionality is divided into two sub-layers. One of them is the DetNet forwarding sub-layer, which optionally provides resource allocation for DetNet flows over paths provided by the underlying network.

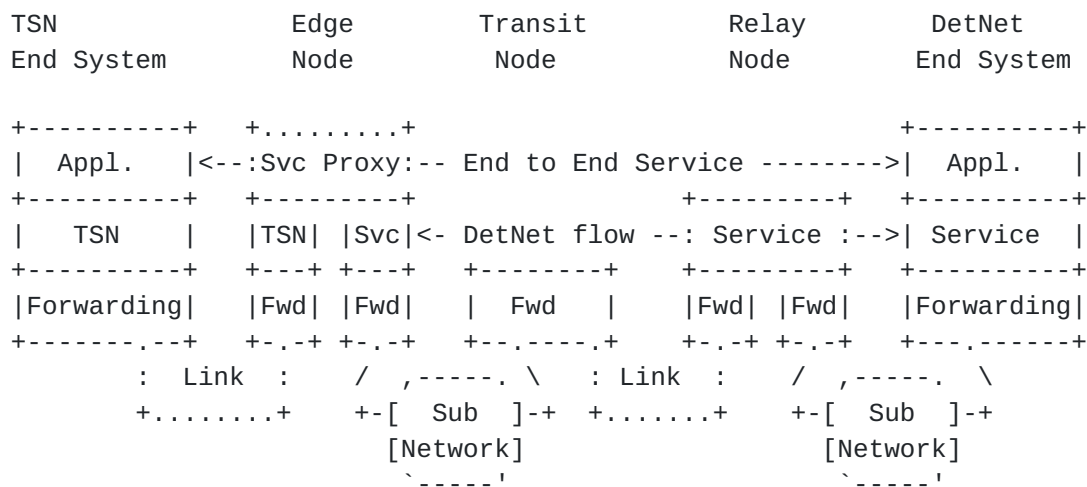
3. SRv6 for DetNet Overview

As mentioned above, there are mainly three technologies/functions defined in DetNet: Explicit Route, Resource Reservation and Service Protection. Explicit Route is the basic of the other two

technologies, and guarantees the path satisfies the SLA requirement from application. Resource Reservation protects DetNet flows from network congestion, which could reduce the end-to-end latency and congestion loss; Service Protection prevents DetNet flow from random media errors and equipment failures, which makes the loss rate extremely low.

In [[I-D.ietf-detnet-architecture](#)], DetNet functionality is implemented in two sub-layers in the protocol stack: the DetNet service sub-layer and the DetNet forwarding sub-layer. The DetNet service sub-layer provides DetNet service, e.g., service protection. The DetNet forwarding sub-layer supports DetNet service in the underlying network, by providing explicit routes and resource allocation to DetNet flows. There is no obvious protocol stack as MPLS, in SRv6 both service sub-layer and forwarding sub-layer are implemented through SRH.

The following picture shows that a general DetNet enabled network defined in [[I-D.ietf-detnet-architecture](#)] :

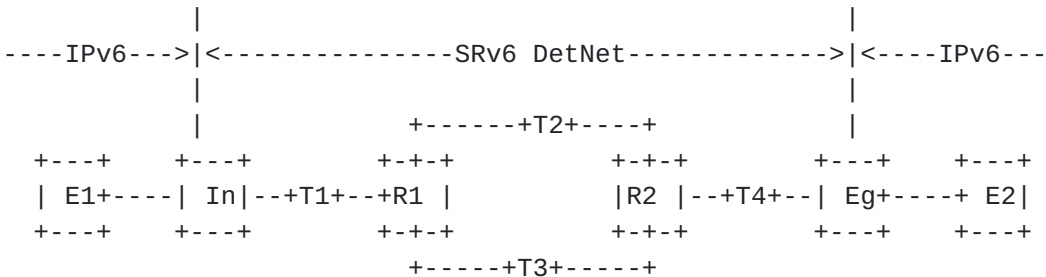


In SRv6 for DetNet, the outer IPv6 Header with the SRH is used for carrying DetNet flows. Explicit path is instantiated in the segment list of SRH, and other functions/arguments for service protection (packet replication, elimination and ordering, PREOF) and resource reservation (packet queuing and scheduling) are also defined in the specified SID. Meta data for DetNet could be instantiated in the Optional TLVs.

4. Service Protection

4.1. Service Protection Scenarios

The figure below shows that an IPv6 flow is sent out from the end station E1. The packet of the flow is encapsulated in an outer IPv6+SRH header as a DetNet SRv6 packet in the Ingress(In) and transported through an SRv6 DetNet domain. In the Egress(Eg), the outer IPv6 header+SRH of the packet is popped, and the packet is sent to the destination E2.



The DetNet packet processing is as follows:

Ingress:

Inserts the SRv6 Policy that will steer the packet from Ingress to the destination

The methods and mechanisms used for defining, instantiating and applying the policy are outside of this document. An example of policies are described in [[I-D.ietf-spring-segment-routing-policy](#)]

Flow Identification and Sequence Number are carried in the SRH.

Relay Node 1(Replication Node):

Replicates the payload and IPv6 Header with the SRH. This is a new function in the context of SRv6 Network Programming which will associate a given SID to a replication instruction in the node originating and advertising the SID. The replication instruction includes:

- * The removal of the existing IPv6+SRH header
- * The encapsulation into a new outer IPv6+SRH header. Each packet (the original and the duplicated) are encapsulated into respectively new outer IPv6+SRH headers.

Binding two different SRv6 Policies respectively to the original packet and the replicated packet, which can steer the packets from Relay Node 1 to Relay Node 2 through two tunnels.

Relay Node 2(Elimination Node):

Eliminates the redundant packets.

Binds a new SRv6 Policy to the survival packet, which steers the packet from Relay Node 2 to Egress.

Egress:

Decapsulates the outer Ipv6 header.

Sends the inner packet to the End Station 2.

The DetNet packet encapsulation is illustrated here below. It has to be noted that, in the example below, the R2 address is a SRH SID associated to a TBD function related to the packet replication the node R1 has to perform. The same (or reverse) apply to node R2 which is in charge of the discard of the duplicated packet. Here also a new function will have a new SID allocated to it and representing the delete of the duplication in R2.

End Station1 output packet: (E1,E2)

Ingress output packet: (In, T1)(R1,T1, SL=2)(E1,E2)

Transit Node1 output packet: (In, R1)(R1,T1,SL=1)(E1,E2)

Relay Node1 output packets : (R1, T2)(R2, T2, SL=2)(E1, E2),
(R1, T3)(R2, T3, SL=2)(E1, E2)

Transit Node2 output packet: (R1, R2)(R2, T2, SL=1)(E1, E2)

Transit Node3 output packet: (R1, R2)(R2, T3, SL=1)(E1, E2)

Relay Node2 output packet: (R2, T4)(Eg, T4, SL=2)(E1, E2)

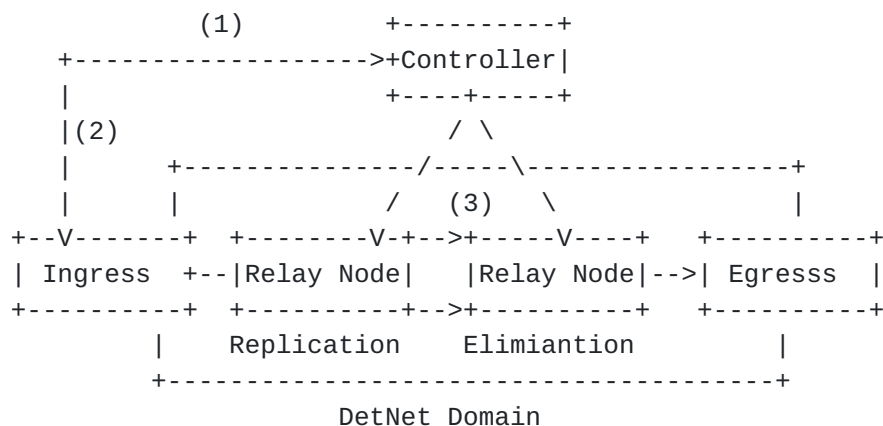
Transit Node4 output packet: (R2, Eg)(Eg, T4, SL=1)(E1, E2)

Egress out : (E1, E2)

4.2. Data Plane Considerations

Flow Identification and sequence number are necessary in the encapsulation of SRv6 for DetNet in order to support service protection. Replication nodes decide which DetNet flows are supposed to be replicated by identifying the flow with the flow identification. Elimination nodes decide whether a packet should be dropped because of redundancy by identifying the flow identification and sequence number.

4.3. Control Plane Considerations



1. Edge node->Controller: Sends a path computation requirement containing that service protection in order to have ultra-reliability through PCEP/BGP extensions.

2. Controller->Edge node: Computes a P2MP2P path, including replication nodes and elimination nodes. Between a pair of replication node and elimination node, there are more than one path, and if any equipment failure happens in one of them, the DetNet service is not interrupted. Send the path computation result to the edge node through PCEP/BGP extensions.

3. Controller->Relay Node : In a P2MP2P path, every pair of replication node and elimination node should be configured to identify different DetNet flows by the different flow identifications, and the rule of sequence number should be negotiated between relay nodes. After replication or elimination, the explicit path to the next relay is also required through BGP extensions or Netconf YANG.

4.4. Functions for Service Protection

New SRv6 Network Programming functions are defined as follows:

4.4.1. End. B. Replication: Packet Replication Function

1. IF NH=SRH & SL>0 THEN
2. extract the DetNet TLV values from the SRH
3. create two new outer IPv6+SRH headers: IPv6-SRH-1 and IPv6-SRH-2
Insert the policy-instructed segment lists in each newly created SRH (SRH-1 and SRH-2). Also, add the extracted DetNet TLVs into SRH-1 and SRH-2.
4. remove the incoming outer IPv6+SRH header.
5. create a duplication of the incoming packet.
6. encapsulate the original packet into the first outer IPv6+SRH header: (IPv6-SRH-1) (original packet)
7. encapsulate the duplicate packet into the second outer IPv6+SRH header: (IPv6-SRH-2) (duplicate packet)
8. set the IPv6 SA as the local address of this node.
9. set the IPv6 DA of IPv6-SRH-1 to the first segment of the SRv6 Policy in of SRH-1 segment list.
10. set the IPv6 DA of IPv6-SRH-2 to the first segment of the SRv6 Policy in of SRH-2 segment list.
11. ELSE
12. drop the packet

4.4.2. End. B. Elimination: Packet Elimination Function

1. IF NH=SRH & SL>0 & "the packet is not a redundant packet" THEN
2. do not decrement SL nor update the IPv6 DA with SRH[SL]
3. extract the value of DetNet TLVs from the SRH
4. create a new outer IPv6+SRH header

5. insert the policy-instructed segment lists in the newly created SRH and add the retrieved DetNet TLVs in the newly created SRH
6. remove the incoming outer IPv6+SRH header.
7. set the IPv6 DA to the first segment of the SRv6 Policy in the newly created SRH
8. ELSE
9. drop the packet

5. Explicit Route

SRv6 could support explicit route using segment list without extra extension. In DetNet, explicit route could be used with service protection or resource reservation. When explicit route works with service protection, a P2MP2P path is required to indicate the behavior of replication and elimination. When explicit route works with resource reservation, the explicit path indicates the nodes or links a DetNet flow goes through, and also indicates the resource allocated for the DetNet flow in the specified nodes or links.

6. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

7. Security Considerations

TBD

8. Acknowledgements

Thank you for valuable comments from James Guichard and Andrew Mails.

9. Normative References

[I-D.filsfils-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J.,
daniel.voyer@bell.ca, d., Matsushima, S., and Z. Li, "SRv6
Network Programming", [draft-filsfils-spring-srv6-network-programming-07](#) (work in progress), February 2019.

[I-D.ietf-6man-segment-routing-header]

Filsfils, C., Dukes, D., Previdi, S., Leddy, J., Matsushima, S., and d. daniel.voyer@bell.ca, "IPv6 Segment Routing Header (SRH)", [draft-ietf-6man-segment-routing-header-21](#) (work in progress), June 2019.

[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-dp-sol-mpls]

Korhonen, J. and B. Varga, "DetNet MPLS Data Plane Encapsulation", [draft-ietf-detnet-dp-sol-mpls-02](#) (work in progress), March 2019.

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

Filsfils, C., Sivabalan, S., daniel.voyer@bell.ca, d., bogdanov@google.com, b., and P. Mattes, "Segment Routing Policy Architecture", [draft-ietf-spring-segment-routing-policy-03](#) (work in progress), May 2019.

[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>>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", [RFC 8402](#), DOI 10.17487/RFC8402, July 2018, <<https://www.rfc-editor.org/info/rfc8402>>.

Authors' Addresses

Xuesong Geng
Huawei

Email: gengxuesong@huawei.com

Zhenbin Li
Huawei

Email: lizhenbin@huawei.com

Mach Chen
Huawei

Email: mach.chen@huawei.com