Deterministic Networking (DetNet) services are expected to be integrated with VPN technologies. Such deployment scenarios include mobile backhauls and TSN islands inter-connections. This document describes an overall VPN framework that provides deterministic transport services (called deterministic VPN), specifies corresponding control and data plane protocols that are required to support the framework, and initially summarizes potential extensions of existing protocols to enable deterministic VPNs.

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 September 9, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
Deterministic Networking (DetNet) aims to provide bounded latency transport as well as low data loss rate for specific data flows over layer-3 networks [arch]. Potential use cases include electrical utilities, building automation systems, and industrial machine to machine [use-case]. From the perspective of real-world deployment, DetNet services are expected to be integrated with VPN technologies, e.g., MPLS/IP VPN, E-VPN. In particular, one or more VPN instances of an ISP network are required to provide bounded latency and low data loss rate transmission services for the customers. Such deployment scenarios include mobile backhauls and TSN islands inter-connections.

This document presents an overall VPN framework that provides deterministic transport services (called deterministic VPN), specifies corresponding control and data plane protocols that are required to support the framework, and initially summarizes potential extensions of existing protocols to enable deterministic VPNs. Note that specific extensions of existing protocols will be defined by separated documents.
2. Deployment Scenarios

This section introduces deployment scenarios for the deterministic VPN.

2.1. Mobile Backhaul

In the last decade, IP/MPLS devices are continuously replacing traditional TDM-based devices in operators' mobile backhaul networks for the benefits of simplicity and high bandwidth utilization. However, best effort IP forwarding cannot provide deterministic transport services as TDM could, making it hard to satisfy user’s QoS requirements. DetNet is expected to fill up this gap. Simultaneously, layer-2 and layer-3 VPNs are also required in mobile backhaul networks in order to isolate different PDU sessions. Therefore, DetNet and VPN might be integrated in mobile backhaul networks.

The example in Figure 1 further illustrates such scenarios, where eNodeB and S-GW are connected by multiple IP routers (i.e., IP backhaul). In this case, a layer-3 or layer-2 deterministic VPN SHOULD be established between the eNodeB and the S-GW to carry the GTP-U encapsulation.

```
+------ GTP +------ +------ +------ GTP +------
|      |<------|      |      |<------|      |
|      |       |Router|       |Router|       |      |
+------       +------       +------       +------

<-----------------L2/L3 VPN---------------->

Figure 1
```

2.2. Inter-connection of TSN Islands

Another deployment scenario is using deterministic VPN to connect TSN islands. In particular, an enterprise may intend to connect its two (separately located) TSN networks by using an ISP network who can provide deterministic transport services. Since the ISP may provide the same service to different enterprises simultaneously, a layer-2 VPN SHOULD be established to isolate the traffic between different enterprises, as shown in Figure 2.
Figure 2

3. Deterministic VPN Framework

Figure 3 shows the overall framework of deterministic VPN, where CE1 and CE2 could be mobile network elements such as eNodeB, s-GW, or p-GW, or could be TSN switches of an enterprise network. PE1, P1, P2, and PE2 are ISP’s IP/MPLS (layer-3) devices who have specific scheduling and shaping capabilities in the data plane thus providing deterministic transport (or DetNet) services. This document assumes that the CQF-based mechanism described in [ldn] is running on PE1, P1, P2 and PE2’s data plane.

In this framework, a layer-2 or layer-3 VPN SHOULD be established between PE1 and PE2 to provide the deterministic transport service for CE1 and CE2. This requires that 1) data flows between CE1 and CE2 MUST be forwarded with bounded latency and low loss rate, and 2) the addresses as well as the traffic among CE1 and CE2 SHOULD be isolated from other CEs’. Note that although the overall framework is quite similar with existing VPN frameworks (e.g., IP/MPLS VPN and E-VPN), extensions of existing protocols are needed to support the deterministic transport, as will be discussed in the following sub-sections.
3.1. Control Plane Protocols

IGP: In the framework described above, IGP protocols such as IS-IS and OSPF SHOULD be used to advertise underlay reachability information. In the case where SR-MPLS and SRv6 encapsulations are chose for data plane tunnels, the IGP protocol SHOULD also advertise corresponding SIDs. To support deterministic VPN, corresponding information of deterministic transport, e.g., interface-level capability of scheduling and shaping, as well as available bandwidth SHOULD also be advertised by the IGP protocols [igp-te-ext].

MP-BGP: MP-BGP is used to advertise VPN reachability information in the framework, e.g., IP prefixes for layer-3 VPNs or MAC addresses for layer-2 VPNs, and corresponding VPN labels, e.g., MPLS labels or a SRv6 END.DX4 SIDs. To support deterministic VPN, MP-BGP SHOULD be extended to deliver related information for the deterministic transport services. Such extensions will be defined in separate documents.

RSVP-TE: RSVP-TE is used to reserve dedicated resources for the deterministic VPN flows. In the case where MPLS LSP is chose for the data plane encapsulation, RSVP-TE will also be used to allocate MPLS label(s) in each node along the forwarding path. To support deterministic VPN, RSVP-TE SHOULD be extended to carry relative information of the deterministic transport services. Such extensions will be defined in separate documents.
3.2. Data Plane Protocols

MPLS LSP Tunnel: If MPLS LSP tunnels are chosen to be the data plane encapsulations for deterministic VPN flows, a mechanism of multiple MPLS labels per LSP per node SHOULD be used to identify different CQF forwarding cycles, as per [ldn]. Such mechanism has been described in [mpls-cqf].

SR-MPLS Tunnel: Accordingly, a SR-MPLS based mechanism to indicate different forwarding cycles at the data plane will also be specified in a separate document.

SRv6 Tunnel: Corresponding SRv6 based mechanism will also be specified in a separate document.

4. IANA Considerations

TBD.

5. Security Considerations

TBD.

6. Acknowledgements

TBD.

7. Normative References


Authors’ Addresses

Zhe Chen
Huawei

Email: chenzhel7@huawei.com

Li Qiang
Huawei

Email: qiangli3@huawei.com