Stream:	Internet Engineering Task Force (IETF)
RFC:	9732
Category:	Informational
Published:	January 2025
ISSN:	2070-1721
Authors:	J. Dong	S. Bryant	Z. Li	T. Miyasaka	Y. Lee
---	---	---	---	---	---
	Huawei	*University of Surrey*	*China Mobile*	*KDDI Corporation*	*Samsung*

RFC 9732
A Framework for Network Resource Partition Based Enhanced Virtual Private Networks

Abstract

This document describes the framework for enhanced Virtual Private Networks (VPNs) that are Network Resource Partition (NRP) based in order to support the needs of applications with specific traffic performance requirements (e.g., low latency, bounded jitter). An NRP represents a subset of network resources and associated policies in the underlay network. NRP-based enhanced VPNs leverage the VPN and Traffic Engineering (TE) technologies and add characteristics that specific services require beyond those provided by conventional VPNs. Typically, an NRP-based enhanced VPN will be used to underpin network slicing, but it could also be of use in its own right providing enhanced connectivity services between customer sites. This document also provides an overview of relevant technologies in different network layers and identifies some areas for potential new work.

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/rfc9732.

Copyright Notice

Table of Contents

1. Introduction

Virtual Private Networks (VPNs) have served the industry well as a means of providing different groups of users with logically isolated connectivity over a common network. The common (base) network that is used to provide the VPNs is often referred to as the "underlay", and the VPN is often called an "overlay".

Customers of a network operator may request connectivity services with advanced characteristics, such as low-latency guarantees, bounded jitter, or isolation from other services or customers, so that changes in other services (e.g., changes in network load, or events such as congestion or outages) have no effect or only acceptable effects on the observed throughput or latency of the services delivered to the customer. These services are referred to as "enhanced VPNs", as they are similar to VPN services, providing the customer with the required connectivity, but they also provide enhanced characteristics.

This document describes a framework for delivering VPN services with enhanced characteristics, such as guaranteed resources, latency, jitter, etc. This list is not exhaustive. It is expected that other enhanced features may be added to VPN over time and that this framework will support these additions with necessary changes or enhancements in some network layers and network planes (data plane, control plane, and management plane).

The concept of network slicing has gained traction, driven largely by needs surfacing from 5G (see [NGMN-NS-Concept], [TS23501], and [TS28530]). According to [TS28530], a 5G end-to-end network slice consists of three major types of network segments: Radio Access Network (RAN), Transport Network (TN), and mobile Core Network (CN). The transport network provides the connectivity between different entities in RAN and CN segments of a 5G end-to-end network slice, with specific performance commitments.

[RFC9543] discusses the general framework, components, and interfaces for requesting and operating network slices using IETF technologies. These network slices may be referred to as "RFC 9543 Network Slices", but in this document (which is solely about IETF technologies), we simply use the term "network slice" to refer to this concept. A network slice service enables connectivity between a set of Service Demarcation Points (SDPs) with specific Service Level Objectives (SLOs) and Service Level Expectations (SLEs) over a common underlay network. A network slice can be realized as a logical network connecting a number of endpoints and is associated with a set of shared or dedicated network resources that are used to satisfy the SLO and SLE requirements. A network slice is considered to be one target use case of enhanced VPNs.

[RFC9543] also introduces the concept of Network Resource Partition (NRP), which is a subset of the buffer/queuing/scheduling resources and associated policies on each of a connected set of links in the underlay network. An NRP can be associated with a dedicated or shared network topology to select or specify the set of links and nodes involved.

The requirements of enhanced VPN services cannot simply be met by overlay networks: enhanced VPN services require tighter coordination and integration between the overlay and the underlay networks.

In the overlay network, the VPN has been defined as the network construct to provide the required connectivity for different services or customers. Multiple VPN flavors can be considered to create that construct [RFC4026]. In the underlay network, the NRP is used to represent a subset of the network resources and associated policies in the underlay network. An NRP can be associated with a dedicated or shared network topology to select or specify the set of links and nodes involved.

An enhanced VPN service can be realized by integrating a VPN in the overlay and an NRP in the underlay. This is called an "NRP-based enhanced VPN". In doing so, an enhanced VPN service can provide enhanced properties, such as guaranteed resources and assured or predictable performance. An enhanced VPN service may also involve a set of service functions (see Section 1.4 of [RFC7665] for the definition of service function). The techniques for delivering an NRP-based enhanced VPN can be used to instantiate a network slice service (as described in Section 6), and they can also be of use in general cases to provide enhanced connectivity services between customer sites or service endpoints.

This document describes a framework for using existing, modified, and potential new technologies as components to provide NRP-based enhanced VPN services. Specifically, this document provides:

- The functional requirements and service characteristics of an enhanced VPN service.
- The design of the data plane for NRP-based enhanced VPNs.
- The necessary control and management protocols in both the underlay and the overlay of enhanced VPNs.
- The mechanisms to achieve integration between the overlay network and the underlay network.
- The necessary Operation, Administration, and Management (OAM) methods to instrument an enhanced VPN to make sure that the required Service Level Agreement (SLA) between the customer and the network operator is met and to take any corrective action (such as switching traffic to an alternate path) to avoid SLA violation.

One possible layered network structure to achieve these objectives is shown in Section 4.1.

It is not envisaged that enhanced VPN services will replace conventional VPN services. VPN services will continue to be delivered using existing mechanisms and can coexist with enhanced VPN services. Whether enhanced VPN features are added to an active VPN service is deployment specific.

2. Terminology

In this document, the relationship of the four terms "VPN", "enhanced VPN", "NRP", and "Network Slice" are as follows:

- A Virtual Private Network (VPN) refers to the overlay network service that provides connectivity between different customer sites and that maintains traffic separation between different customers. Examples of technologies to provide VPN services are as follows: IPVPN [RFC2764], L2VPN [RFC4664], L3VPN [RFC4364], and EVPN [RFC7432].
- An enhanced VPN service is an evolution of the VPN service that makes additional service-specific commitments. An NRP-based enhanced VPN is made by integrating a VPN with a set of network resources allocated in the underlay network (i.e., an NRP).
- A Network Resource Partition (NRP), as defined in [RFC9543], is a subset of the buffer/queuing/scheduling resources and associated policies on each of a connected set of links in the underlay network. An NRP can be associated with a dedicated or shared network topology to select or specify the set of links and nodes involved. An NRP is designed to meet the network resources and performance characteristics required by the enhanced VPN services.
- A network slice service could be delivered by provisioning one or more NRP-based enhanced VPNs in the network. Other mechanisms for realizing network slices may exist but are not in the scope of this document.

The term "tenant" is used in this document to refer to a customer of the enhanced VPN services.

The following terms, defined in other documents, are also used in this document.

SLA: Service Level Agreement (see [RFC9543])

SLO: Service Level Objective (see [RFC9543])

SLE: Service Level Expectation (see [RFC9543])

ACTN: Abstraction and Control of TE Networks (see [RFC8453])

DetNet: Deterministic Networking (see [RFC8655])

FlexE: Flexible Ethernet (see [FLEXE])

TSN: Time-Sensitive Networking (see [TSN])

VN: Virtual Network (see [RFC8453])

3. Overview of the Requirements

This section provides an overview of the requirements of an enhanced VPN service.

3.1. Performance Guarantees

Performance guarantees are committed by network operators to their customers in relation to the services delivered to the customers. They are usually expressed in SLAs as a set of SLOs.

There are several kinds of performance guarantees, including guaranteed maximum packet loss, guaranteed maximum delay, and guaranteed delay variation. Note that these guarantees apply to conformance traffic; out-of-profile traffic will be handled according to a separate agreement with the customer (see, for example, Section 3.6 of [RFC7297]).

Guaranteed maximum packet loss is usually addressed by setting packet priorities, queue sizes, and discard policies. However, this becomes more difficult when the requirement is combined with latency requirements. The limiting case is zero congestion loss, and that is the goal of Deterministic Networking (DetNet) [RFC8655] and Time-Sensitive Networking (TSN) [TSN]. In modern optical networks, loss due to transmission errors already approaches zero, but there is the possibility of failure of the interface or the fiber itself. This type of fault can be addressed by some form of signal duplication and transmission over diverse paths.

Guaranteed maximum latency is required by a number of applications, particularly real-time control applications and some types of augmented reality and virtual reality (AR/VR) applications. DetNet techniques may be considered [RFC8655]; however, additional methods of enhancing the underlay to better support the delay guarantees may be needed. These methods will need to be integrated with the overall service provisioning mechanisms.

Guaranteed maximum delay variation is a performance guarantee that may also be needed. [RFC8578] calls up a number of cases that need this guarantee, for example, in electrical utilities. Time transfer is an example service that needs a performance guarantee, although it is in the nature of time that the service might be delivered by the underlay as a shared service and not provided through different enhanced VPNs. Alternatively, a dedicated enhanced VPN might be used to provide time transfer as a shared service.

This suggests that a spectrum of service guarantees needs to be considered when designing and deploying an enhanced VPN. For illustration purposes and without claiming to be exhaustive, four types of services are considered:

- Best effort
- Assured bandwidth
- Guaranteed latency
- Enhanced delivery

It is noted that some services may have mixed requirements from this list, e.g., both assured bandwidth and guaranteed latency can be required.

The best-effort service is the basic connectivity service that can be provided by current VPNs.

An assured bandwidth service is a connectivity service in which the bandwidth over some period of time is assured. This could be achieved either simply based on a best-effort service with over-capacity provisioning or based on MPLS TE Label Switching Paths (TE-LSPs) with bandwidth reservations. Depending on the technique used, however, the bandwidth is not necessarily assured at any instant. Providing assured bandwidth to VPNs, for example, by using per-VPN TE-LSPs, is not widely deployed at least partially due to scalability concerns. The more common approach of aggregating multiple VPNs onto common TE-LSPs results in shared bandwidth and so may reduce the assurance of bandwidth to any one service. Enhanced VPNs aim to provide a more scalable approach for such services.

A guaranteed latency service has an upper bound to edge-to-edge latency. Assuring the upper bound is sometimes more important than minimizing latency. There are several new technologies that provide some assistance with this performance guarantee:

- the IEEE TSN project [TSN] introduces the concept of scheduling of delay-sensitive and loss-sensitive packets.
- FlexE [FLEXE] is useful to help provide a guaranteed upper bound to latency.
- DetNet is of relevance in assuring an upper bound of end-to-end packet latency in the network layer.

The use of these technologies to deliver enhanced VPN services needs to be considered when a guaranteed latency service is required.

An enhanced delivery service is a connectivity service in which the underlay network (at Layer 3) needs to ensure to eliminate or minimize packet loss in the event of equipment or media failures. This may be achieved by delivering a copy of the packet through multiple paths. Such a mechanism may need to be used for enhanced VPN services.

3.2. Interaction Between Enhanced VPN Services

There is a fine distinction between how a customer requests limits on interaction between an enhanced VPN service and other services (whether they are other enhanced VPN services or any other network service) and how that is delivered by the service provider. This section examines the requirements and realization of limited interaction between an enhanced VPN service and other services.

3.2.1. Requirements on Traffic Isolation

"Traffic isolation" is a generic term that can be used to describe the requirements for separating the services of different customers or different service types in the network. In the context of network slicing, traffic isolation is defined as an SLE of the network slice service (Section 8.1 of [RFC9543]), which is one element of the SLA. A customer may care about disruption caused by other services, contamination by other traffic, or delivery of their traffic to the wrong destinations.

A customer may want to specify (and thus pay for) the traffic isolation provided by the service provider. Some customers (banking, for example) may have strict requirements on how their flows are handled when delivered over a shared network. Some professional services are used to relying on specific certifications and audits to ensure the compliancy of a network with traffic-isolation requirements and, specifically, to prevent data leaks.

With traffic isolation, a customer expects that the service traffic cannot be received by other customers in the same network. In [RFC4176], traffic isolation is mentioned as one of the requirements of VPN customers. Traffic isolation is also described in Section 3.8 of [RFC7297].

There can be different expectations of traffic isolation. For example, a customer may further request the protection of their traffic by requesting specific encryption schemes at the enhanced VPN access and also when transported between Provider Edge (PE) nodes.

An enhanced VPN service customer may request traffic isolation together with other operator-defined service characteristics. The exact details about the expected behavior need to be specified in the service request so that meaningful service assurance and fulfillment feedback can be exposed to the customers. It is out of the scope of this document to elaborate the service-modeling considerations.

3.2.2. Limited Interaction with Other Services

[RFC2211] describes the controlled-load service. In that document, the end-to-end behavior provided to an application by a series of network elements providing controlled-load service is described as closely approximating to the behavior visible to applications receiving best-effort service when those network elements are not carrying substantial traffic from other services.

Thus, a consumer of a controlled-load service may assume that:

- A very high percentage of transmitted packets will be successfully delivered by the network to the receiving end nodes.
- The transit delay experienced by a very high percentage of the delivered packets will not greatly exceed the minimum transmit delay experienced by any successfully delivered packet.

An enhanced VPN customer may request a controlled-load service in one of two ways:

1. It may configure a set of SLOs (for example, for delay and loss) such that the delivered enhanced VPN meets the behavioral objectives of the customer.
2. As described in [RFC2211], a customer may request the controlled-load service without reference to or specification of specific target values for control parameters such as delay or loss. Instead, acceptance of a request for controlled-load service is defined to imply a commitment by the network element to provide the requestor with service closely equivalent to that provided to uncontrolled (best-effort) traffic under lightly loaded conditions. This way of requesting the service is an SLE.

Limited interaction between enhanced VPN services does not cover service degradation due to non-interaction-related causes, such as link errors.

3.2.3. Realization of Limited Interaction with Enhanced VPN Services

A service provider may translate the requirements related to limited interaction into distinct engineering rules in its network. Honoring the service requirement may involve tweaking a set of QoS, TE, security, and planning tools, while traffic isolation will involve adequately configuring routing and authorization capabilities.

Concretely, there are many existing techniques that can be used to provide traffic isolation, such as IP and MPLS VPNs or other multi-tenant virtual network techniques. Controlled-load services may be realized as described in [RFC2211]. Other tools may include various forms of resource management and reservation techniques, such as network capacity planning, allocating dedicated network resources, traffic policing or shaping, prioritizing in using shared network resources, etc., so that a subset of bandwidth, buffers, and queueing resources can be available in the underlay network to support the enhanced VPN services.

To provide the required traffic isolation, or to reduce the interaction with other enhanced VPN services, network resources may need to be reserved in the data plane of the underlay network and dedicated to traffic from a specific enhanced VPN service or a specific group of enhanced VPN services. This may introduce scalability concerns both in the implementation (as each enhanced VPN may need to be tracked in the network) and in how many resources need to be reserved and how the services are mapped to the resources (Section 4.4). Thus, some trade-off needs to be considered to provide the traffic isolation and limited interaction between an enhanced VPN service and other services.

A dedicated physical network can be used to meet stricter SLO and SLE requests, at the cost of allocating resources on a long-term and end- to-end basis. On the other hand, where adequate traffic isolation and limited interaction can be achieved at the packet layer, this permits the resources to be shared amongst a group of services and only dedicated to a service on a temporary basis. By combining conventional VPNs with TE/QoS/security techniques, an enhanced VPN offers a variety of means to honor customer's requirements.

3.3. Integration with Network Resources and Service Functions

The way to achieve the characteristics demand of an enhanced VPN service (such as guaranteed or predictable performance) is by integrating the overlay VPN with a particular set of resources in the underlay network that are allocated to meet the service requirements. This needs to be done in a flexible and scalable way so that it can be widely deployed in operators' networks to support a good number of enhanced VPN services.

Taking mobile networks and, in particular, 5G into consideration, the integration of the network with service functions is likely a requirement. The IETF's work on Service Function Chaining (SFC) [RFC7665] provides a foundation for this. Service functions in the underlay network can be considered to be part of the enhanced VPN services, which means the service functions may need to be an integral part of the corresponding NRP. The details of the integration between service functions and enhanced VPNs are out of the scope of this document.

3.3.1. Abstraction

Integration of the overlay VPN and the underlay network resources and service functions does not always need to be a direct mapping. As described in [RFC7926], abstraction is the process of applying policy to a set of information about a traffic engineered (TE) network to produce selective information that represents the potential ability to connect across the network. The process of abstraction presents the connectivity graph in a way that is independent of the underlying network technologies, capabilities, and topology so that the graph can be used to plan and deliver network services in a uniform way.

With the approach of abstraction, an enhanced VPN may be built on top of an abstracted topology that represents the connectivity capabilities of the underlay TE-based network as described in the framework for Abstraction and Control of TE Networks (ACTN) [RFC8453] as discussed further in Section 5.5.

3.4. Dynamic Changes

Enhanced VPNs need to be created, modified, and removed from the network according to service demands (including scheduled requests). An enhanced VPN that requires limited interaction with other services (Section 3.2.2) must not be disrupted by the instantiation or modification of another enhanced VPN service. As discussed in Section 3.1 of [RFC4176], the assessment of traffic isolation is part of the management of a VPN service. Determining whether modification of an enhanced VPN can be disruptive to that enhanced VPN and whether the traffic in flight will be disrupted can be a difficult problem.

Dynamic changes both to the enhanced VPN and to the underlay network need to be managed to avoid disruption to services that are sensitive to changes in network performance.

In addition to managing the network without disruption during changes such as the inclusion of a new enhanced VPN service endpoint or a change to a link, enhanced VPN traffic might need to be moved because of changes to traffic patterns and volume. This means that during the lifetime of an enhanced VPN service, closed-loop optimization is needed so that the delivered service always matches the ordered service SLA.

The data plane aspects of this problem are discussed further in Sections 5.1, 5.2, and 5.3.

The control plane aspects of this problem are discussed further in Section 5.4.

The management plane aspects of this problem are discussed further in Section 5.5.

3.5. Customized Control

In many cases enhanced VPN services are delivered to customers without information about the underlying NRPs. However, in some cases, depending on the agreement between the operator and the customer, the customer may also be provided with some information about the underlying NRPs. Such information can be filtered or aggregated according to the operator's policy. This allows the customer of an enhanced VPN service to have some visibility and even

control over how the underlying topology and resources of the NRP are used. For example, the customer may be able to specify the path or path constraints within the NRP for specific traffic flows of their enhanced VPN service. Depending on the requirements, an enhanced VPN customer may have their own network controller, which may be provided with an interface to the control or management system run by the network operator. Note that such a control is within the scope of the customer's enhanced VPN service; any additional changes beyond this would require some intervention by the network operator.

A description of the control plane aspects of this problem are discussed further in Section 5.4. A description of the management plane aspects of this feature can be found in Section 5.5.

3.6. Applicability to Overlay Technologies

The concept of an enhanced VPN can be applied to any existing and future multi-tenancy overlay technologies including but not limited to:

- Layer 2 point-to-point (P2P) services, such as pseudowires (see [RFC3985])
- Layer 2 VPNs (see [RFC4664])
- Ethernet VPNs (see [RFC7209] and [RFC7432])
- Layer 3 VPNs (see [RFC4364] and [RFC2764])

Where such VPN service types need enhanced isolation and delivery characteristics, the technologies described in Section 5 can be used to tweak the underlay to provide the required enhanced performance.

3.7. Inter-Domain and Inter-Layer Network

In some scenarios, an enhanced VPN service may span multiple network domains. A domain is considered to be any collection of network elements under the responsibility of the same administrative entity, for example, an Autonomous System (AS). In some domains, the network operator may manage a multi-layered network, for example, a packet network over an optical network. When enhanced VPN services are provisioned in such network scenarios, the technologies used in different network planes (the data plane, control plane, and management plane) need to provide mechanisms to support multi-domain and multi-layer coordination and integration; this is to provide the required service characteristics for different enhanced VPN services and improve network efficiency and operational simplicity. The mechanisms for multi-domain VPNs (see [RFC4364]) may be reused, and some enhancement may be needed to meet the additional requirements of enhanced VPN services.

4. The Architecture of NRP-Based Enhanced VPNs

Multiple NRP-based enhanced VPN services can be provided by a common network infrastructure. Each NRP-based enhanced VPN service is provisioned with an overlay VPN and mapped to a corresponding NRP, which has a specific set of network resources and service functions allocated in the underlay to satisfy the needs of the customer. One NRP may support

one or more NRP-based enhanced VPN services. The integration between the overlay connectivity and the underlay resources ensures the required isolation between different enhanced VPN services and achieves the guaranteed performance for different customers.

The NRP-based enhanced VPN architecture needs to be designed with consideration given to:

- An enhanced data plane.
- A control plane to create enhanced VPNs and NRPs, making use of the data plane isolation and performance guarantee techniques.
- A management plane to manage enhanced VPN service life cycles.
- The OAM mechanisms for enhanced VPNs and the underlying NRPs.
- Telemetry mechanisms for enhanced VPNs and the underlying NRPs.

These topics are expanded below.

- The enhanced data plane provides:
  - The required packet-latency and jitter characteristics.
  - The required packet-loss characteristics.
  - The required resource-isolation capability, e.g., bandwidth guarantee.
  - The mechanism to associate a packet with the set of resources allocated to an NRP to which the enhanced VPN service packet is mapped.
- The control plane:
  - Collects information about the underlying network topology and network resources and exports this to network nodes and/or a centralized controller as required.
  - Creates NRPs with the network resource and topology properties needed by the enhanced VPN services.
  - Distributes the attributes of NRPs to network nodes that participate in the NRPs and/or a centralized controller.
  - Computes and sets up network paths in each NRP.
  - Maps enhanced VPN services to an appropriate NRP.
  - Determines the risk of SLA violation and takes appropriate avoidance/correction actions.
  - Considers the right balance of per-packet and per-node state according to the needs of the enhanced VPN services to scale to the required size.
- The management plane includes management interfaces, the Operations, Administration, and Maintenance (OAM) and telemetry mechanisms. More specifically, it provides:
  - An interface between the enhanced VPN service provider (e.g., the operator's network management system) and the enhanced VPN customer (e.g., an organization or service with an enhanced VPN requirement) such that the operation requests and the related parameters can be exchanged without the awareness of other enhanced VPN customers.
  - An interface between the enhanced VPN service provider and the enhanced VPN customers to expose the network capability information toward the customer.

- The service life-cycle management and operation of enhanced VPN services (e.g., creation, modification, assurance/monitoring, and decommissioning).
- The OAM tools to verify whether the underlay network resources (i.e., NRPs) are correctly allocated and operating properly.
- The OAM tools to verify the connectivity and monitor the performance of the enhanced VPN service.
- Telemetry of information in the underlay network for overall performance evaluation and the planning of the enhanced VPN services.
- Telemetry of information of enhanced VPN services for monitoring and analytics of the characteristics and SLA fulfillment of the enhanced VPN services.

4.1. Layered Architecture

The layered architecture of NRP-based enhanced VPNs is shown in Figure 1.

Underpinning everything is the physical network infrastructure layer, which provides the underlying resources used to provision the separate NRPs. This layer is responsible for the partitioning of link and/or node resources for different NRPs. Each subset of a link or node resource can be considered to be a virtual link or virtual node used to build the NRPs.

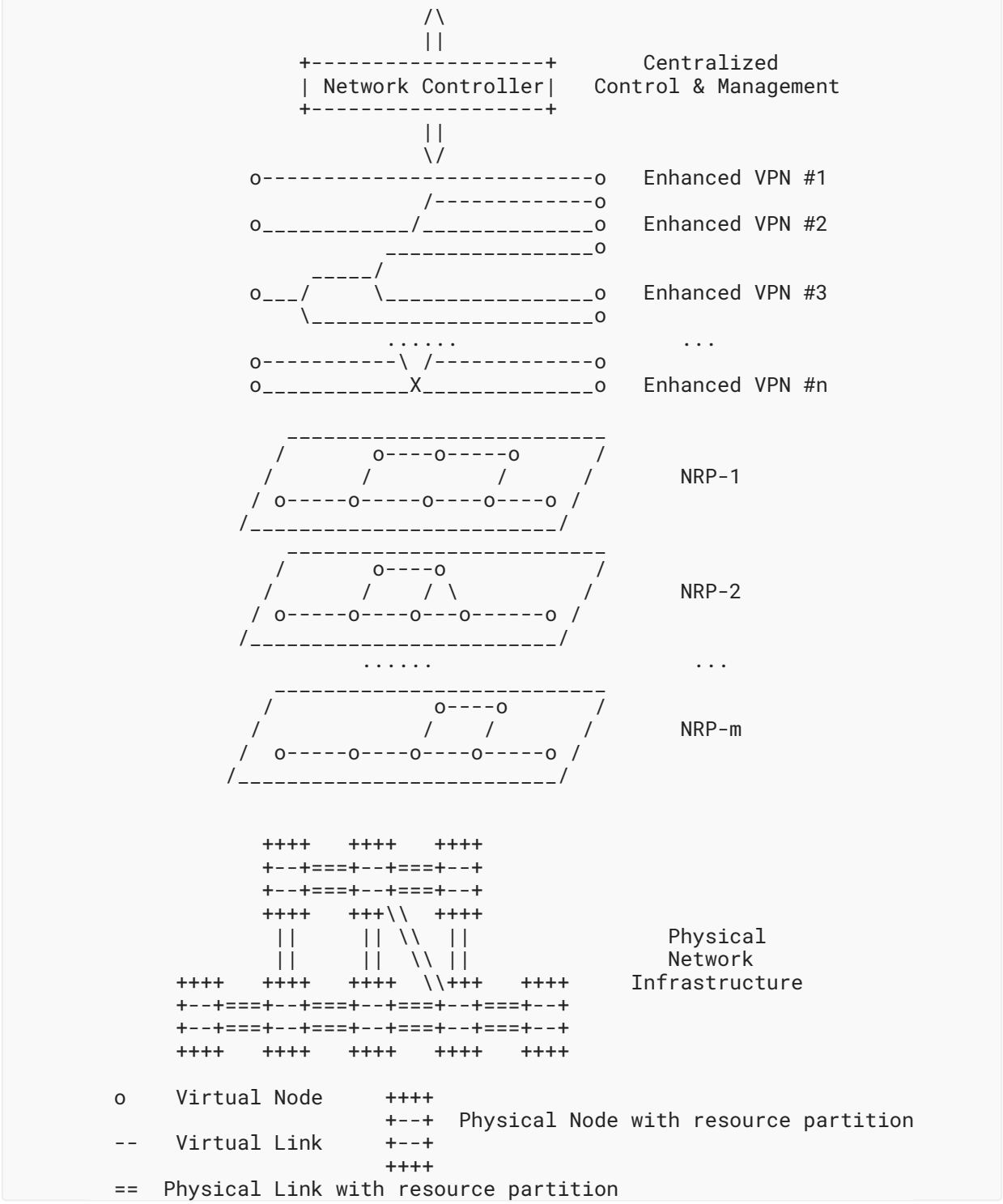

Figure 1: The Layered Architecture of Enhanced VPNs

Various components and techniques discussed in Section 5 can be used to enable resource partitioning of the physical network infrastructure, such as FlexE, TSN, dedicated queues, etc. These partitions may be physical or virtual so long as the SLA required by the higher layers is met.

Based on the set of network resource partitions provided by the physical network infrastructure, multiple NRPs can be created. Each of these NRPs:

- has a set of dedicated or shared network resources allocated from the physical underlay network, and
- can be associated with a customized logical network topology so as to meet the requirements of different enhanced VPN services or different groups of enhanced VPN services.

According to the associated logical network topology, each NRP needs to be instantiated on a set of network nodes and links that are involved in the logical topology. On each node or link, each NRP is associated with a set of local resources that are allocated for the processing of traffic in the NRP. The NRP provides the integration between the logical network topology and the required underlying network resources.

According to the service requirements of connectivity, performance, isolation, etc., enhanced VPN services can be mapped to the appropriate NRPs in the network. Different enhanced VPN services can be mapped to different NRPs; it is also possible that multiple enhanced VPN services are mapped to the same NRP. Thus, the NRP is an essential scaling technique as it has the potential of eliminating per-service per-path state from the network. In addition, when a group of enhanced VPN services is mapped to a single NRP, only the network state of the single NRP needs to be maintained in the network (see Section 4.4 for more information).

The network controller is responsible for creating an NRP, instructing the involved network nodes to allocate network resources to the NRP, and provisioning the enhanced VPN services on the NRP. A distributed control plane may be used for distributing the NRP resource and topology attributes among nodes in the NRP. Extensions to distributed control protocols (if any) are out of the scope of this document.

The process used to create NRPs and to allocate network resources for use by the NRPs needs to take a holistic view of the needs of all of the service provider's customers and to partition the resources accordingly. However, within an NRP, these resources can be managed via a dynamic control plane if required. This provides the required scalability and isolation with some flexibility.

4.2. Connectivity Types

At the VPN service level, the required connectivity for a Multipoint-to-Multipoint (MP2MP) VPN service is usually full or partial mesh. To support such VPN services, the corresponding NRP also needs to provide MP2MP connectivity among the endpoints.

Other service requirements may be expressed at different granularities, some of which can be applicable to the whole service while others may only be applicable to some pairs of endpoints. For example, when a particular level of performance guarantee is required, the point-to-point path through the underlying NRP of the enhanced VPN service may need to be specifically engineered to meet the required performance guarantee.

4.3. Application-Specific Data Types

Although a lot of the traffic that will be carried over enhanced VPN will likely be IP based, the design must be capable of carrying other traffic types, in particular Ethernet traffic. This is easily accomplished through various pseudowire (PW) techniques [RFC3985].

Where the underlay is MPLS, Ethernet traffic can be carried over an enhanced VPN encapsulated according to the method specified in [RFC4448]. Where the underlay is IP, L2 Tunneling Protocol - Version 3 (L2TPv3) [RFC3931] can be used with Ethernet traffic carried according to [RFC4719]. Encapsulations have been defined for most of the common L2 types for both PW over MPLS and for L2TPv3.

4.4. Scalable Service Mapping

VPNs are instantiated as overlays on top of an operator's network and offered as services to the operator's customers. An important feature of overlays is that they can deliver services without placing per-service state in the core of the underlay network.

An enhanced VPN may need to install some additional state within the network to achieve the features that they require. Solutions need to take the scale of such state into consideration, and deployment architectures should constrain the number of enhanced VPN services so that the additional state introduced to the network is acceptable and under control. It is expected that the number of enhanced VPN services will be small at the beginning: even in the future, the number of enhanced VPN services will be fewer than conventional VPNs because existing VPN techniques are good enough to meet the needs of most existing VPN-type services.

In general, it is not required that the state in the network be maintained in a 1:1 relationship with the enhanced VPN services. It will usually be possible to aggregate a set or group of enhanced VPN services so that they share the same NRP and the same set of network resources (much in the same way that current VPNs are aggregated over transport tunnels) so that collections of enhanced VPN services that require the same behavior from the network in terms of resource reservation, latency bounds, resiliency, etc. can be grouped together. This is an important feature to assist with the scaling characteristics of NRP-based enhanced VPN deployments.

[NRP-SCALABILITY] provides more details of scalability considerations for the NRPs used to instantiate NRPs, and Section 7 includes a greater discussion of scalability considerations.

5. Candidate Technologies

A VPN is created by applying a demultiplexing technique to the underlying network (the underlay) to distinguish the traffic of one VPN from that of another. The connections of a VPN are supported by a set of underlay paths. A path that travels by other than the shortest path through the underlay normally requires state to specify that path. The state of the paths could be applied to the underlay through the use of the RSVP-TE signaling protocol or directly through the use of a Software-Defined Networking (SDN) controller. Based on Segment Routing (SR), state could be maintained at the ingress node of the path and carried in the data packet. Other techniques may emerge as this problem is studied. This state gets harder to manage as the number of paths increases. Furthermore, as we increase the coupling between the underlay and the overlay to support the enhanced VPN service, this state is likely to increase further. Through the use of NRP, a subset of underlay network resources can be either dedicated for a particular enhanced VPN service or shared among a group of enhanced VPN services. A group of underlay paths can be established using the common set of network resources of the NRP.

This section describes the candidate technologies and examines them in the context of the different network planes that may be used together to build NRPs. Section 5.1 discusses the L2 packet-based or frame-based forwarding-plane mechanisms for resource partitioning. Section 5.2 discusses the corresponding encapsulation and forwarding mechanisms in the network layer. Non-packet data plane mechanisms are briefly discussed in Section 5.3. The control plane and management plane mechanisms are discussed in Sections 5.4 and 5.5, respectively.

5.1. Underlay Forwarding Resource Partitioning

Several candidate L2 packet-based or frame-based forwarding-plane mechanisms that can provide the required traffic isolation and performance guarantees are described in the following sections.

5.1.1. Flexible Ethernet

FlexE [FLEXE] provides the ability to multiplex channels over an Ethernet link to create point-to-point fixed-bandwidth connections in a way that provides separation between enhanced VPN services. FlexE also supports bonding links to create larger links out of multiple low-capacity links.

However, FlexE is only a link-level technology. When packets are received by the downstream node, they need to be processed in a way that preserves that traffic isolation in the downstream node. In turn, this requires a queuing and forwarding implementation that preserves the end-to-end separation of enhanced VPNs.

If different FlexE channels are used for different services, then no sharing is possible between the FlexE channels. Thus, it may be difficult to dynamically redistribute unused bandwidth to lower priority services in another FlexE channel. If one FlexE channel is used by one customer, the customer can use some methods to manage the relative priority of their own traffic in the FlexE channel.

5.1.2. Dedicated Queues

Diffserv-based queuing systems are described in [RFC2475] and [RFC4594]. This approach is not sufficient to provide separation of enhanced VPN services because Diffserv does not provide enough markers to differentiate between traffic of a large number of enhanced VPN services. Additionally, Diffserv does not offer the range of service classes that each enhanced VPN service needs to provide to its tenants. This problem is particularly acute with an MPLS underlay because MPLS only provides eight traffic classes.

In addition, Diffserv, as currently implemented, mainly provides per- hop priority-based scheduling, and it is difficult to use it to achieve quantitative resource reservation for different enhanced VPN services.

To address these problems and to reduce the potential interactions between enhanced VPN services, it would be necessary to steer traffic to dedicated input and output queues per enhanced VPN service or per group of enhanced VPN services: some routers have a large number of queues and sophisticated queuing systems that could support this while some routers may struggle to provide the granularity and level of separation required by the applications of an enhanced VPN.

5.1.3. Time-Sensitive Networking

[TSN] is an IEEE project to provide a method of carrying time-sensitive information over Ethernet. It introduces the concept of packet scheduling where a packet stream may be given a time slot guaranteeing that it will experience no queuing delay or increase in latency beyond a very small scheduling delay. The mechanisms defined in TSN can be used to meet the requirements of time-sensitive traffic flows of enhanced VPN service.

Ethernet can be emulated over a L3 network using an IP or MPLS pseudowire. However, a TSN Ethernet payload would be opaque to the underlay; thus, it would not be treated specifically as time-sensitive data. The preferred method of carrying TSN over a L3 network is through the use of deterministic networking as explained in Section 5.2.1.

5.2. Network Layer Encapsulation and Forwarding

This section considers the problem of enhanced VPN service differentiation and the representation of underlying network resources in the network layer. More specifically, it describes the possible data plane mechanisms to determine the network resources and the logical network topology or paths associated with an NRP.

5.2.1. Deterministic Networking (DetNet)

DetNet [RFC8655] is a technique being developed in the IETF to enhance the ability of L3 networks to deliver packets more reliably and with greater control over the delay. The design cannot use retransmission techniques such as TCP because that can exceed the delay tolerated by the applications. DetNet preemptively sends copies of the packet over various paths to minimize the chance of all copies of a packet being lost. It also seeks to set an upper bound on latency, but

the goal is not to minimize latency. DetNet can be realized over the IP data plane [RFC8939] or the MPLS data plane [RFC8964], and it may be used to provide deterministic paths for enhanced VPN services.

5.2.2. MPLS Traffic Engineering (MPLS-TE)

MPLS-TE (see [RFC2702] and [RFC3209]) introduces the concept of reserving end-to-end bandwidth for a TE-LSP, which can be used to provide a set of point-to-point resource-reserved paths across the underlay network to support VPN services. VPN traffic can be carried over dedicated TE-LSPs to provide guaranteed bandwidth for each specific connection in a VPN, and VPNs with similar behavior requirements may be multiplexed onto the same TE-LSPs. Some network operators have concerns about the scalability and management overhead of MPLS-TE system, especially with regard to those systems that use an active control plane, and this has lead them to consider other solutions for traffic engineering in their networks.

5.2.3. Segment Routing

Segment Routing (SR) [RFC8402] is a method that prepends instructions to packets at the headend of a path. These instructions are used to specify the nodes and links to be traversed, and they allow the packets to be routed on paths other than the shortest path. By encoding the state in the packet, per-path state is transitioned out of the network. SR can be instantiated using the MPLS data plane (SR-MPLS) (see [RFC8660]) or the IPv6 data plane (SRv6) (see [RFC8986]).

An SR traffic engineered path operates with the granularity of a link. Hints about priority are provided using the Traffic Class (TC) field in the packet header. However, to achieve the performance and isolation characteristics that are sought by enhanced VPN customers, it will be necessary to steer packets through specific virtual links and/or queues on the same link and direct them to use specific resources. With SR, it is possible to introduce such fine-grained packet steering by specifying the queues and the associated resources through an SR instruction list. One approach to do this is described in [RESOURCE-AWARE-SEGMENTS].

Note that the concept of a queue is a useful abstraction for different types of underlay mechanisms that may be used to provide enhanced isolation and performance support. How the queue satisfies the requirement is implementation specific and is transparent to the L3 data plane and control plane mechanisms used.

With Segment Routing, the SR instruction list could be used to build a P2P SR path. In addition, a group of SR Segment Identifiers (SIDs) could also be used to represent an MP2MP network. Thus, the SR-based mechanism could be used to provide both resource-reserved paths and NRPs for enhanced VPN services.

5.2.4. New Encapsulation Extensions

In contrast to reusing an existing data plane for enhanced VPN, another possible approach is to introduce new encapsulations or extensions to an existing data plane to allow dedicated identifiers for the underlay network resources of an enhanced VPN and the logical network topology or paths associated with an enhanced VPN. This may require more protocol work;

however, the potential benefits are that it can reduce the impact to existing network operation and improve the scalability of enhanced VPN. More details about the encapsulation extensions and the scalability concerns are described in [NRP-SCALABILITY].

5.3. Non-Packet Data Plane

Non-packet underlay data plane technologies, such as optical-based data planes, often have TE properties and behaviors. They meet many of the key requirements, particularly those for:

- bandwidth guarantees,
- traffic isolation (with physical isolation often being an integral part of the technology),
- highly predictable latency and jitter characteristics,
- measurable loss characteristics, and
- ease of identification of flows.

The cost is that the resources are allocated on a long-term and end-to-end basis. Such an arrangement means that the full cost of the resources has to be borne by the client to which the resources are allocated. When an NRP built with this data plane is used to support multiple enhanced VPN services, the cost could be distributed among such a group of services.

5.4. Control Plane

The control plane of NRP-based enhanced VPNs is likely to be based on a hybrid control mechanism that takes advantage of a logically centralized controller for on-demand provisioning and Global Concurrent Optimization (GCO) while still relying on a distributed control plane to provide scalability, high reliability, fast reaction, automatic failure recovery, etc. Extension to and optimization of the centralized and distributed control plane is needed to support the enhanced properties of an NRP-based enhanced VPN.

As described in Section 4, the enhanced VPN control plane needs to provide the following functions:

- Collection of information about the underlying network topology and network resources and exportation of this to network nodes and/or a centralized controller as required.
- Creation of NRPs with the network resource and topology properties needed by NRP-based enhanced VPN services.
- Distribution of the attributes of NRPs to network nodes that participate in the NRPs and/or the centralized controller.
- Mapping of enhanced VPN services to an appropriate NRP.
- Computation and set up of service paths in each NRP to meet enhanced VPN service requirements.

Underlying network topology and resource information can be collected using mechanisms based on the existing IGP and Border Gateway Protocol - Link State (BGP-LS) [RFC9552]. The creation of NRPs and the distribution of NRP attributes may need further control protocol

extensions. The computation of service paths based on the attributes and constraints of the NRP can be performed either by the headend node of the path or by a centralized Path Computation Element (PCE) [RFC4655].

Two candidate control plane mechanisms for path setup in the NRP are RSVP-TE and Segment Routing (SR).

- RSVP-TE, as described in [RFC3209], provides the signaling mechanism for establishing a TE-LSP in an MPLS network with end-to-end resource reservation. This can be seen as an approach of providing resource-reserved paths that could be used to bind the VPN to a specific set of network resources allocated within the underlay; however, there remain scalability concerns, as mentioned in Section 5.2.2.
- The SR control plane, as described in [RFC8665], [RFC8667], and [RFC9085], does not have the capability of signaling resource reservations along the path. On the other hand, the SR approach provides a potential way of binding the underlay network resource and the NRPs without requiring per-path state to be maintained in the network. A centralized controller can perform resource planning and reservation for NRPs, and it needs to instruct the network nodes to ensure that resources are correctly allocated for the NRP. The controller could provision the SR paths based on the mechanism in [RFC9256] to the headend nodes of the paths.

According to the service requirements for connectivity, performance, and isolation, one enhanced VPN service may be mapped to a dedicated NRP or a group of enhanced VPN services may be mapped to the same NRP. The mapping of enhanced VPN services to an NRP can be achieved using existing control mechanisms with possible extensions; it can be based on either the characteristics of the data packet or the attributes of the VPN service routes.

5.5. Management Plane

The management plane provides the interface between the enhanced VPN service provider and the customers for life-cycle management of the enhanced VPN service (i.e., creation, modification, assurance/monitoring, and decommissioning). It relies on a set of service data models for the description of the information and operations needed on the interface.

As an example, in the context of 5G end-to-end network slicing [TS28530], the management of the transport network segment of the 5G end-to-end network slice can be realized with the management plane of the enhanced VPN. The 3GPP management system may provide the connectivity and performance-related parameters as requirements to the management plane of the transport network. It may also require the transport network to expose the capabilities and status of the network slice. Thus, an interface between the enhanced VPN management plane and the 5G network slice management system, and relevant service data models are needed for the coordination of 5G end-to-end network slice management.

The management plane interface and data models for enhanced VPN services can be based on the service models described in Section 5.6.

It is important that the life-cycle management support in-place modification of enhanced VPN services. That is, it should be possible to add and remove endpoints, as well as to change the requested characteristics of the service that is delivered. The management system needs to be able to assess the revised enhanced VPN requests and determine whether they can be provided by the existing NRPs or whether changes must be made. It will also need to determine whether those changes to the NRP are possible. If not, then the customer's modification request may be rejected.

When the modification of an enhanced VPN service is possible, the management system must make every effort to make the changes in a non-disruptive way. That is, the modification of the enhanced VPN service or the underlying NRP must not perturb traffic on the enhanced VPN service in a way that causes the service level to drop below the agreed levels. Furthermore, changes to one enhanced VPN service should not cause disruption to other enhanced VPN services.

The network operator for the underlay network (i.e., the provider of the enhanced VPN service) may delegate some operational aspects of the overlay VPN and the underlying NRP to the customer. In this way, the enhanced VPN is presented to the customer as a virtual network, and the customer can choose how to use that network. Some mechanisms in the operator's network are needed so that:

- a customer cannot exceed the capabilities of the virtual links and nodes, but
- it can decide how to load traffic onto the network, for example, by assigning different metrics to the virtual links so that the customer can control how traffic is routed through the virtual network.

This approach requires a management system for the virtual network but does not necessarily require any coordination between the management systems of the virtual network and the physical network, except that the virtual network management system might notice when the NRP is close to capacity or considerably under-used and automatically request changes in the service provided by the underlay network.

5.6. Applicability of Service Data Models to Enhanced VPNs

This section describes the applicability of the existing and in-progress service data models to enhanced VPNs. [RFC8309] describes the scope and purpose of service models and shows where a service model might fit into an SDN-based network management architecture. New service models may also be introduced for some of the required management functions.

Service data models are used to represent, monitor, and manage the virtual networks and services enabled by enhanced VPNs. The VPN customer service models (e.g., the L3VPN Service Model (L3SM) in [RFC8299], the L2VPN Service Model (L2SM) in [RFC8466]), or the ACTN Virtual Network (VN) model in [RFC9731]) are service models that can provide the customer's view of the enhanced VPN service. The L3VPN Network Model (L3NM) from [RFC9182] and the L2VPN Network Model (L2NM) from [RFC9291] provide the operator's view of the managed infrastructure as a set of virtual networks and the associated resources. The Service Attachment Points (SAPs) model in [RFC9408] provides an abstract view of the Service Attachment Points

(SAPs) to various network services in the provider network, where enhanced VPN could be one of the service types. [RFC9375] provides the data model for performance monitoring of network and VPN services. Augmentation to these service models may be needed to provide the enhanced VPN services. The NRP model in [NRP-YANG] further provides the management of the NRP topology and resources both in the controller and in the network devices to instantiate the NRPs needed for the enhanced VPN services.

6. Applicability in Network Slice Realization

This section describes the applicability of NRP-based enhanced VPN for network slice realization.

In order to provide network slice services to customers, a technology-agnostic network slice service model [NETWORK-SLICE-YANG] is needed for the customers to communicate the requirements of network slices (SDPs, connectivity, SLOs, and SLEs). These requirements may be realized using technology specified in this document to instruct the network to deliver an enhanced VPN service so as to meet the requirements of the network slice customers. According to the location of SDPs used for the network slice service (see Section 5.2 of [RFC9543]), an SDP can be mapped to a Customer Edge (CE), a PE, a port on a CE, or a customer-facing port on a PE, any of which can be correlated to the endpoint of the enhanced VPN service. The detailed approach for SDP mapping is described in [NETWORK-SLICE-YANG].

6.1. NRP Planning

An NRP is used to support the SLOs and SLEs required by the network slice services. According to the network operators' network resource planning policy, or based on the requirements of one or a group of customers or services, an NRP may need to be created to meet the requirements of network slice services. One of the basic requirements for the NRP is to provide a set of dedicated network resources to avoid unexpected interference from other services in the same network. Other possible requirements may include the required topology and connectivity, bandwidth, latency, reliability, etc.

A centralized network controller can be responsible for calculating a subset of the underlay network topology (which is called a logical topology) to support the NRP requirement. On the network nodes and links within the logical topology, the set of network resources to be allocated to the NRP can also be determined by the controller. Normally, such calculation needs to take the underlay network connectivity information and the available network resource information of the underlay network into consideration. The network controller may also take the status of the existing NRPs into consideration in the planning and calculation of a new NRP.

6.2. NRP Creation

According to the result of the NRP planning, the network nodes and links involved in the logical topology of the NRP are instructed to allocate the required set of network resources for the NRP. One or multiple mechanisms as specified in Section 5.1 can be used to partition the forwarding-plane network resources and allocate different subsets of resources to different NRPs. In addition, the data plane identifiers that are used to identify the set of network resources

allocated to the NRP are also provisioned on the network nodes. Depending on the data plane technologies used, the set of network resources of an NRP can be identified using, e.g., resource-aware SR segments as specified in [RESOURCE-AWARE-SEGMENTS] and [SR-ENHANCED-VPN] or a dedicated Resource ID as specified in [IPv6-NRP-OPTION] can be introduced. The network nodes involved in an NRP may distribute the logical topology information, the NRP-specific network resource information, and the Resource ID of the NRP using the control plane. Such information could be used by the controller and the network nodes to compute the TE or shortest paths within the NRP and to install the NRP-specific forwarding entries to network nodes.

6.3. Network Slice Service Provisioning

According to the connectivity requirements of a network slice service, an overlay VPN can be created using the existing or future multi-tenancy overlay technologies as described in Section 3.6.

Then, according to the SLO and SLE requirements of a network slice service, the network slice service is mapped to an appropriate NRP as the virtual underlay. The integration of the overlay VPN and the underlay NRP provides a network slice service.

6.4. Network Slice Traffic Steering and Forwarding

At the edge of the operator's network, network slice traffic can be classified based on the rules defined by the operator's policy; this is so that the traffic that matches the rules for specific network slice services can be mapped to the corresponding NRP. Thus, packets belonging to a specific network slice service will be processed and forwarded by network nodes based on either:

- the traffic-engineered paths or
- the shortest paths in the associated network topology

using the set of network resources of the corresponding NRP.

7. Scalability Considerations

NRP-based enhanced VPNs provide performance guaranteed services in packet networks; however, this comes with the potential cost of introducing additional state into the network. There are at least three ways that this additional state might be added:

- by introducing the complete state into the packet, as is done in SR. This allows the controller to specify the detailed series of forwarding and processing instructions for the packet as it transits the network. The cost of this is an increase in the packet header size. A further cost is that systems will have to provide NRP-specific segments in case they are called upon by a service. This is a type of latent state, and it increases as the segments and resources that need to be exclusively available to enhanced VPN service are specified more precisely.
- by introducing the state to the network. This is normally done by creating a path using signaling such as RSVP-TE. This could be extended to include any element that needs to be specified along the path, for example, explicitly specifying queuing policy. It is also possible

to use other methods to introduce path state, such as via an SDN controller or possibly by modifying a routing protocol. With this approach, there is state per path: a per-path characteristic that needs to be maintained over the life of the path. This is more network state than is needed using SR, but the packets are usually shorter.

- by providing a hybrid approach. One example is based on using binding SIDs (see [RFC8402]) to represent path fragments and binding them together with SR. Dynamic creation of a VPN service path using SR requires less state maintenance in the network core at the expense of larger packet headers. The packet size can be lower if a form of loose source routing is used (using a few nodal SIDs), and it will be lower if no specific functions or resources on the routers are specified. For SRv6, the packet size may also be reduced by utilizing the compression techniques specified in [SRv6-SRH-COMPRESSION].

Reducing state in the network is important to enhanced VPNs, as it requires the overlay to be more closely integrated with the underlay than with conventional VPNs. This tighter coupling would normally mean that more state needs to be created and maintained in the network, as state about fine-granularity processing would need to be loaded and maintained in the routers. Aggregation is a well-established approach to reduce the amount of state and improve scaling, and NRP is considered to be the network construct to aggregate the states of enhanced VPN services. In addition, an SR approach allows much of the state to be spread amongst the network ingress nodes and transiently carried in the packets as SIDs.

The following subsections describe some of the scalability concerns that need to be considered. Further discussion of the scalability considerations of the underlaying network constructs of NRP-based enhanced VPNs can be found in [NRP-SCALABILITY].

7.1. Maximum Stack Depth of SR

One of the challenges with SR is the stack depth that nodes are able to impose on packets [RFC8491]. This leads to a difficult balance between:

- adding state to the network and minimizing stack depth and
- minimizing state and increasing the stack depth.

7.2. RSVP-TE Scalability

The established method of creating a resource-reserved path through an MPLS network is to use the RSVP-TE protocol. However, there have been concerns that this requires significant continuous state maintenance in the network. Work to improve the scalability of RSVP-TE LSPs in the control plane can be found in [RFC8370].

There is also concern at the scalability of the forwarder footprint of RSVP-TE as the number of paths through a Label Switching Router (LSR) grows. [RFC8577] addresses this by employing SR within a tunnel established by RSVP-TE.

7.3. SDN Scaling

The centralized approach of SDN requires control plane state to be stored in the network, but can reduce the overhead of control channels to be maintained. Each individual network node may need to maintain a control channel with an SDN controller, which is considered more scalable compared to the need of maintaining control channels with a set of neighbor nodes.

However, SDN may transfer some of the scalability concerns from the network to a centralized controller. In particular, there may be a heavy processing burden at the controller and a heavy load in the network surrounding the controller. A centralized controller may also present a single point of failure within the network.

8. Enhanced Resiliency

Each enhanced VPN service has a life cycle and may need modification during deployment as the needs of its tenant change (see Section 5.5). Additionally, as the network evolves, garbage collection may need to be performed to consolidate resources into usable quanta.

Systems in which the path is imposed, such as SR or some form of explicit routing, tend to do well in these applications because it is possible to perform an atomic transition from one path to another. That is, a single action by the headend that changes the path without the need for coordinated action by the routers along the path. However, implementations and the monitoring protocols need to make sure that the new path is operational and meets the required SLA before traffic is transitioned to it. It is possible for deadlocks to arise as a result of the network becoming fragmented over time, such that it is impossible to create a new path or to modify an existing path without impacting the SLA of other paths. The GCO mechanisms as described in [RFC5557] and discussed in [RFC7399] may be helpful, while complete resolution of this situation is as much a commercial issue as it is a technical issue.

However, there are two manifestations of the latency problem that are for further study in any of these approaches:

- Packets overtaking one another if path latency reduces during a transition.
- Transient variation in latency in either direction as a path migrates.

There is also the matter of what happens during failure in the underlay infrastructure. Fast reroute is one approach, but that still produces a transient loss with a normal goal of rectifying this within 50 ms [RFC5654]. An alternative is some form of N+1 delivery such as has been used for many years to support protection from service disruption. This may be taken to a different level using the techniques of DetNet with multiple in-network replications and the culling of later packets [RFC8655].

In addition to the approach used to protect high-priority packets, consideration should be given to the impact of best-effort traffic on the high-priority packets during a transition. Specifically, if a conventional re-convergence process is used, there will inevitably be micro-loops and, while some form of explicit routing will protect the high-priority traffic, lower-priority traffic on best-

effort shortest paths will micro-loop without the use of a loop-prevention technology. To provide the highest quality of service to high-priority traffic, either this traffic must be shielded from the micro-loops or micro-loops must be prevented completely.

9. Manageability Considerations

This section describes the considerations about the OAM and telemetry mechanisms used to support the verification, monitoring, and optimization of the characteristics and SLA fulfillment of NRP-based enhanced VPN services. It should be read along with Section 5.5, which gives consideration to the management plane techniques that can be used to build NRPs.

9.1. OAM Considerations

The design of OAM for enhanced VPN services needs to consider the following requirements:

- Instrumentation of the NRP (the virtual underlay) so that the network operator can be sure that the resources committed to a customer are operating correctly and delivering the required performance. It is important that the OAM packets follow the same path and set of resources as the service packets mapped to the NRP.
- Instrumentation of the overlay by the customer. This is likely to be transparent to the network operator and to use existing methods. Particular consideration needs to be given to the need to verify the various committed performance characteristics.
- Instrumentation of the overlay by the service provider to proactively demonstrate that the committed performance is being delivered. This needs to be done in a non-intrusive manner, particularly when the tenant is deploying a performance-sensitive application.

A study of OAM in SR networks is documented in [RFC8403].

9.2. Telemetry Considerations

Network visibility is essential for network operation. Network telemetry has been considered to be an ideal means to gain sufficient network visibility with better flexibility, scalability, accuracy, coverage, and performance than conventional OAM technologies.

As defined in [RFC9232], the objective of network telemetry is to acquire network data remotely for network monitoring and operation. It is a general term for a large set of network visibility techniques and protocols. Network telemetry addresses the current network operation issues and enables smooth evolution toward intent-driven autonomous networks. Telemetry can be applied on the forwarding plane, the control plane, and the management plane in a network. Telemetry for enhanced VPN service needs to consider the following requirements:

- Collecting data of NRPs for overall performance evaluation and the planning of the enhanced VPN services.
- Collecting data of each enhanced VPN service for monitoring and analytics of the service characteristics and SLA fulfillment.

How the telemetry mechanisms could be used or extended for enhanced VPN services is out of the scope of this document.

10. Operational Considerations

It is expected that NRP-based enhanced VPN services will be introduced in networks that already have conventional VPN services deployed. Depending on service requirements, the tenants or the operator may choose to use a VPN or an enhanced VPN to fulfill a service requirement. The information and parameters to assist such a decision needs to be supplied on the management interface between the tenant and the operator. The management interface and data models (as described in Section 5.6) can be used for the life-cycle management of enhanced VPN services, such as service creation, modification, performance monitoring, and decommissioning.

11. Security Considerations

All types of virtual networks require special consideration to be given to the isolation of traffic belonging to different tenants. That is, traffic belonging to one VPN must not be delivered to endpoints outside that VPN. In this regard, the enhanced VPN neither introduces nor experiences greater security risks than other VPNs.

However, in an enhanced VPN service, the additional service requirements need to be considered. For example, if a service requires a specific upper bound to latency, then it can be damaged by simply delaying the packets through the activities of another tenant, i.e., by introducing bursts of traffic for other services. In some respects, this makes the enhanced VPN more susceptible to attacks since the SLA may be broken. Another view is that the operator must, in any case, preform monitoring of the enhanced VPN to ensure that the SLA is met; thus, the operator may be more likely to spot the early onset of a security attack and be able to take preemptive protective action.

The measures to address these dynamic security risks must be specified as part of the specific solution to the isolation requirements of an enhanced VPN service.

While an enhanced VPN service may be sold as offering encryption and other security features as part of the service, customers would be well advised to take responsibility for their security requirements themselves, possibly by encrypting traffic before handing it off to the service provider.

The privacy of enhanced VPN service customers must be preserved. It should not be possible for one customer to discover the existence of another customer nor should the sites that are members of an enhanced VPN be externally visible.

An enhanced VPN service (even one with traffic isolation requirements or with limited interaction with other enhanced VPNs) does not provide any additional guarantees of privacy for customer traffic compared to regular VPNs: the traffic within the network may be intercepted and errors may lead to mis-delivery. Users who wish to ensure the privacy of their traffic must take their own precautions including end-to-end encryption.

12. IANA Considerations

This document has no IANA actions.

13. References

13.1. Normative References

[RFC9543] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "A Framework for Network Slices in Networks Built from IETF Technologies", RFC 9543, DOI 10.17487/RFC9543, March 2024, <https://www.rfc-editor.org/info/rfc9543>.

13.2. Informative References

[FLEXE] Optical Internetworking Forum, "Flex Ethernet Implementation Agreement", IA # OIF-FLEXE-01.0, March 2016, <https://www.oiforum.com/wp-content/uploads/2019/01/OIF-FLEXE-01.0.pdf>.

[IPv6-NRP-OPTION] Dong, J., Li, Z., Xie, C., Ma, C., and G. S. Mishra, "Carrying Network Resource (NR) related Information in IPv6 Extension Header", Work in Progress, Internet-Draft, draft-ietf-6man-enhanced-vpn-vtn-id-09, 3 November 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-enhanced-vpn-vtn-id-09>.

[NETWORK-SLICE-YANG] Wu, B., Dhody, D., Rokui, R., Saad, T., and J. Mullooly, "A YANG Data Model for the RFC 9543 Network Slice Service", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slice-nbi-yang-20, 27 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slice-nbi-yang-20>.

[NGMN-NS-Concept] hao ,, "NGMN NS Concept", <https://www.ngmn.org/fileadmin/user_upload/161010_NGMN_Network_Slicing_framework_v1.0.8.pdf>.

[NRP-SCALABILITY] Dong, J., Li, Z., Gong, L., Yang, G., and G. S. Mishra, "Scalability Considerations for Network Resource Partition", Work in Progress, Internet-Draft, draft-ietf-teas-nrp-scalability-06, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-nrp-scalability-06>.

[NRP-YANG] Wu, B., Dhody, D., Beeram, V. P., Saad, T., and S. Peng, "YANG Data Models for Network Resource Partitions (NRPs)", Work in Progress, Internet-Draft, draft-ietf-teas-nrp-yang-02, 5 July 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-nrp-yang-02>.

[RESOURCE-AWARE-SEGMENTS] Dong, J., Miyasaka, T., Zhu, Y., Qin, F., and Z. Li, "Introducing Resource Awareness to SR Segments", Work in Progress, Internet-Draft, draft-ietf-spring-resource-aware-segments-10, 12 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-resource-aware-segments-10>.

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

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <https://www.rfc-editor.org/info/rfc2475>.

[RFC2702] Awduche, D., Malcolm, J., Agogbua, J., O'Dell, M., and J. McManus, "Requirements for Traffic Engineering Over MPLS", RFC 2702, DOI 10.17487/RFC2702, September 1999, <https://www.rfc-editor.org/info/rfc2702>.

[RFC2764] Gleeson, B., Lin, A., Heinanen, J., Armitage, G., and A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, DOI 10.17487/RFC2764, February 2000, <https://www.rfc-editor.org/info/rfc2764>.

[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>.

[RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed., "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, DOI 10.17487/RFC3931, March 2005, <https://www.rfc-editor.org/info/rfc3931>.

[RFC3985] Bryant, S., Ed. and P. Pate, Ed., "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, DOI 10.17487/RFC3985, March 2005, <https://www.rfc-editor.org/info/rfc3985>.

[RFC4026] Andersson, L. and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, DOI 10.17487/RFC4026, March 2005, <https://www.rfc-editor.org/info/rfc4026>.

[RFC4176] El Mghazli, Y., Ed., Nadeau, T., Boucadair, M., Chan, K., and A. Gonguet, "Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management", RFC 4176, DOI 10.17487/RFC4176, October 2005, <https://www.rfc-editor.org/info/rfc4176>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/rfc4364>.

[RFC4448] Martini, L., Ed., Rosen, E., El-Aawar, N., and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks", RFC 4448, DOI 10.17487/RFC4448, April 2006, <https://www.rfc-editor.org/info/rfc4448>.

[RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, DOI 10.17487/RFC4594, August 2006, <https://www.rfc-editor.org/info/rfc4594>.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[RFC4664] Andersson, L., Ed. and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, DOI 10.17487/RFC4664, September 2006, <https://www.rfc-editor.org/info/rfc4664>.

[RFC4719] Aggarwal, R., Ed., Townsley, M., Ed., and M. Dos Santos, Ed., "Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)", RFC 4719, DOI 10.17487/RFC4719, November 2006, <https://www.rfc-editor.org/info/rfc4719>.

[RFC5557] Lee, Y., Le Roux, JL., King, D., and E. Oki, "Path Computation Element Communication Protocol (PCEP) Requirements and Protocol Extensions in Support of Global Concurrent Optimization", RFC 5557, DOI 10.17487/RFC5557, July 2009, <https://www.rfc-editor.org/info/rfc5557>.

[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>.

[RFC7209] Sajassi, A., Aggarwal, R., Uttaro, J., Bitar, N., Henderickx, W., and A. Isaac, "Requirements for Ethernet VPN (EVPN)", RFC 7209, DOI 10.17487/RFC7209, May 2014, <https://www.rfc-editor.org/info/rfc7209>.

[RFC7297] Boucadair, M., Jacquenet, C., and N. Wang, "IP Connectivity Provisioning Profile (CPP)", RFC 7297, DOI 10.17487/RFC7297, July 2014, <https://www.rfc-editor.org/info/rfc7297>.

[RFC7399] Farrel, A. and D. King, "Unanswered Questions in the Path Computation Element Architecture", RFC 7399, DOI 10.17487/RFC7399, October 2014, <https://www.rfc-editor.org/info/rfc7399>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <https://www.rfc-editor.org/info/rfc7432>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC7926] Farrel, A., Ed., Drake, J., Bitar, N., Swallow, G., Ceccarelli, D., and X. Zhang, "Problem Statement and Architecture for Information Exchange between Interconnected Traffic-Engineered Networks", BCP 206, RFC 7926, DOI 10.17487/RFC7926, July 2016, <https://www.rfc-editor.org/info/rfc7926>.

[RFC8299] Wu, Q., Ed., Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN Service Delivery", RFC 8299, DOI 10.17487/RFC8299, January 2018, <https://www.rfc-editor.org/info/rfc8299>.

[RFC8309] Wu, Q., Liu, W., and A. Farrel, "Service Models Explained", RFC 8309, DOI 10.17487/RFC8309, January 2018, <https://www.rfc-editor.org/info/rfc8309>.

[RFC8370] Beeram, V., Ed., Minei, I., Shakir, R., Pacella, D., and T. Saad, "Techniques to Improve the Scalability of RSVP-TE Deployments", RFC 8370, DOI 10.17487/RFC8370, May 2018, <https://www.rfc-editor.org/info/rfc8370>.

[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>.

[RFC8403] Geib, R., Ed., Filsfils, C., Pignataro, C., Ed., and N. Kumar, "A Scalable and Topology-Aware MPLS Data-Plane Monitoring System", RFC 8403, DOI 10.17487/RFC8403, July 2018, <https://www.rfc-editor.org/info/rfc8403>.

[RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453, DOI 10.17487/RFC8453, August 2018, <https://www.rfc-editor.org/info/rfc8453>.

[RFC8466] Wen, B., Fioccola, G., Ed., Xie, C., and L. Jalil, "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery", RFC 8466, DOI 10.17487/RFC8466, October 2018, <https://www.rfc-editor.org/info/rfc8466>.

[RFC8491] Tantsura, J., Chunduri, U., Aldrin, S., and L. Ginsberg, "Signaling Maximum SID Depth (MSD) Using IS-IS", RFC 8491, DOI 10.17487/RFC8491, November 2018, <https://www.rfc-editor.org/info/rfc8491>.

[RFC8577] Sitaraman, H., Beeram, V., Parikh, T., and T. Saad, "Signaling RSVP-TE Tunnels on a Shared MPLS Forwarding Plane", RFC 8577, DOI 10.17487/RFC8577, April 2019, <https://www.rfc-editor.org/info/rfc8577>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

[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>.

[RFC8660] Bashandy, A., Ed., Filsfils, C., Ed., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing with the MPLS Data Plane", RFC 8660, DOI 10.17487/RFC8660, December 2019, <https://www.rfc-editor.org/info/rfc8660>.

[RFC8665] Psenak, P., Ed., Previdi, S., Ed., Filsfils, C., Gredler, H., Shakir, R., Henderickx, W., and J. Tantsura, "OSPF Extensions for Segment Routing", RFC 8665, DOI 10.17487/RFC8665, December 2019, <https://www.rfc-editor.org/info/rfc8665>.

[RFC8667] Previdi, S., Ed., Ginsberg, L., Ed., Filsfils, C., Bashandy, A., Gredler, H., and B. Decraene, "IS-IS Extensions for Segment Routing", RFC 8667, DOI 10.17487/RFC8667, December 2019, <https://www.rfc-editor.org/info/rfc8667>.

[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>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

[RFC9085] Previdi, S., Talaulikar, K., Ed., Filsfils, C., Gredler, H., and M. Chen, "Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing", RFC 9085, DOI 10.17487/RFC9085, August 2021, <https://www.rfc-editor.org/info/rfc9085>.

[RFC9182] Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., Munoz, L., and A. Aguado, "A YANG Network Data Model for Layer 3 VPNs", RFC 9182, DOI 10.17487/RFC9182, February 2022, <https://www.rfc-editor.org/info/rfc9182>.

[RFC9232] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", RFC 9232, DOI 10.17487/RFC9232, May 2022, <https://www.rfc-editor.org/info/rfc9232>.

[RFC9256] Filsfils, C., Talaulikar, K., Ed., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC 9256, DOI 10.17487/RFC9256, July 2022, <https://www.rfc-editor.org/info/rfc9256>.

[RFC9291] Boucadair, M., Ed., Gonzalez de Dios, O., Ed., Barguil, S., and L. Munoz, "A YANG Network Data Model for Layer 2 VPNs", RFC 9291, DOI 10.17487/RFC9291, September 2022, <https://www.rfc-editor.org/info/rfc9291>.

[RFC9375] Wu, B., Ed., Wu, Q., Ed., Boucadair, M., Ed., Gonzalez de Dios, O., and B. Wen, "A YANG Data Model for Network and VPN Service Performance Monitoring", RFC 9375, DOI 10.17487/RFC9375, April 2023, <https://www.rfc-editor.org/info/rfc9375>.

[RFC9408] Boucadair, M., Ed., Gonzalez de Dios, O., Barguil, S., Wu, Q., and V. Lopez, "A YANG Network Data Model for Service Attachment Points (SAPs)", RFC 9408, DOI 10.17487/RFC9408, June 2023, <https://www.rfc-editor.org/info/rfc9408>.

[RFC9552] Talaulikar, K., Ed., "Distribution of Link-State and Traffic Engineering Information Using BGP", RFC 9552, DOI 10.17487/RFC9552, December 2023, <https://www.rfc-editor.org/info/rfc9552>.

[RFC9731] Lee, Y., Ed., Dhody, D., Ed., Ceccarelli, D., Bryskin, I., and B. Y. Yoon, "A YANG Data Model for Virtual Network (VN) Operations", RFC 9731, DOI 10.17487/RFC9731, January 2025, <https://www.rfc-editor.org/info/rfc9731>.

[SR-ENHANCED-VPN] Dong, J., Miyasaka, T., Zhu, Y., Qin, F., and Z. Li, "Segment Routing based Network Resource Partition (NRP) for Enhanced VPN", Work in Progress, Internet-Draft, draft-ietf-spring-sr-for-enhanced-vpn-08, 12 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-for-enhanced-vpn-08>.

[SRv6-SRH-COMPRESSION] Cheng, W., Ed., Filsfils, C., Li, Z., Decraene, B., and F. Clad, Ed., "Compressed SRv6 Segment List Encoding", Work in Progress, Internet-Draft, draft-ietf-spring-srv6-srh-compression-18, 22 July 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-srv6-srh-compression-18>.

[TS23501] 3GPP, "System architecture for the 5G system (5GS)", 3GPP TS 23.501, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>.

[TS28530] 3GPP, "Management and orchestration; Concepts, use cases and requirements", 3GPP TS 28.530, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3273>.

[TSN] IEEE 802.1 Working Group, "Time-Sensitive Networking (TSN) Task Group", <https://1.ieee802.org/tsn/>.

Acknowledgements

The authors would like to thank Charlie Perkins, James N. Guichard, John E. Drake, Shunsuke Homma, Luis M. Contreras, and Joel Halpern for their review and valuable comments.

This work was supported in part by the European Commission funded H2020-ICT-2016-2 METRO-HAUL project (G.A. 761727).

Contributors

Daniel King
Email: daniel@olddog.co.uk

Adrian Farrel
Email: adrian@olddog.co.uk

Jeff Tantsura
Email: jefftant.ietf@gmail.com

Zhenbin Li
Email: lizhenbin@huawei.com

Qin Wu
Email: bill.wu@huawei.com

Bo Wu
Email: lana.wubo@huawei.com

Daniele Ceccarelli
Email: daniele.ietf@gmail.com

Mohamed Boucadair
Email: mohamed.boucadair@orange.com

Sergio Belotti
Email: sergio.belotti@nokia.com

Haomian Zheng
Email: zhenghaomian@huawei.com

Authors' Addresses

Jie Dong
Huawei
Email: jie.dong@huawei.com

Stewart Bryant
University of Surrey
Email: stewart.bryant@gmail.com

Zhenqiang Li
China Mobile
Email: lizhenqiang@chinamobile.com

Takuya Miyasaka
KDDI Corporation
Email: ta-miyasaka@kddi.com

Young Lee
Samsung
Email: younglee.tx@gmail.com