Abstract

This document specifies a framework for using existing, modified and potential new networking technologies as components to provide an Enhanced Virtual Private Network (VPN+) service. The purpose is to support the needs of new applications, particularly applications that are associated with 5G services, by utilizing an approach that is based on existing VPN and TE technologies and adds features that specific services require over and above traditional VPNs.

Typically, VPN+ will be used to form the underpinning of network slicing, but could also be of use in its own right. It is not envisaged that large numbers of VPN+ instances will be deployed in a network and, in particular, it is not intended that all VPNs supported by a network will use VPN+ techniques.

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 March 15, 2020.
Copyright Notice

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

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Overview of the Requirements .............................. 6
   2.1. Isolation between Virtual Networks .................. 6
       2.1.1. A Pragmatic Approach to Isolation .............. 7
   2.2. Performance Guarantee .................................. 8
   2.3. Integration .............................................. 10
       2.3.1. Abstraction ....................................... 11
   2.4. Dynamic Management ..................................... 11
   2.5. Customized Control ..................................... 12
   2.6. Applicability ........................................... 12
   2.7. Inter-Domain and Inter-Layer Network ................. 12
3. Architecture of Enhanced VPN ............................ 13
   3.1. Layered Architecture ..................................... 15
   3.2. Multi-Point to Multi-Point (MP2MP) ................. 16
   3.3. Application Specific Network Types ................. 16
   3.4. Scaling Considerations ................................. 16
4. Candidate Technologies ...................................... 17
   4.1. Layer-Two Data Plane ................................. 17
       4.1.1. FlexE ............................................. 18
       4.1.2. Dedicated Queues .................................. 18
       4.1.3. Time Sensitive Networking ...................... 19
   4.2. Layer-Three Data Plane ............................... 19
       4.2.1. Deterministic Networking ....................... 19
       4.2.2. MPLS Traffic Engineering (MPLS-TE) ............ 20
       4.2.3. Segment Routing .................................. 20
   4.3. Non-Packet Data Plane .................................. 21
   4.4. Control Plane ........................................... 21
   4.5. Management Plane ....................................... 22
   4.6. Applicability of Service Data Models to Enhanced VPN .. 23
       4.6.1. Enhanced VPN Delivery in ACTN Architecture .... 24
       4.6.2. Enhanced VPN Features with Service Data Models ... 25
1. Introduction

Virtual private networks (VPNs) have served the industry well as a means of providing different groups of users with logically isolated access to a common network. The common or 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 enhanced overlay services with advanced characteristics such as complete isolation from other services so that changes in one service (such as changes in network load, or events such as congestion or outages) have no effect on the throughput or latency of other services provided to the customer.

Driven largely by needs surfacing from 5G, the concept of network slicing has gained traction [NGMN-NS-Concept] [TS23501] [TS28530] [BBF-SD406]. In [TS23501], Network Slice is defined as "a logical network that provides specific network capabilities and network characteristics", and Network Slice Instance is defined as "A set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice". According to [TS28530], an end-to-end network slice consists of three major network segments: Radio Access Network (RAN), Transport Network (TN) and Core Network (CN). Transport network provides the required connectivity within and between RAN and CN parts, with specific performance commitment. For each end-to-end network slice, the topology and performance requirement on transport network can be very different, which requires transport network to
have the capability of supporting multiple different transport network slices.

A transport network slice is a virtual (logical) network with a particular network topology and a set of shared or dedicated network resources, which are used to provide the network slice consumer with the required connectivity, appropriate isolation and specific Service Level Agreement (SLA). A transport network slice could span multiple technology (IP, Optical) and multiple administrative domains. Depends on the consumer’s requirement, a transport network slice could be isolated from other, often concurrent transport network slices in terms of data plane, control plane and management plane.

In the following sections of this document, network slice refers to transport network slice, and is interchangeable with enhanced VPN. End-to-end network slice is used to refer to the 5G network slice.

Network abstraction is a technique that can be applied to a network domain to select network resources by policy to obtain a view of potential connectivity and a set of service functions.

Network slicing builds on the concept of resource management, network virtualization and abstraction to provide performance assurance, flexibility, programmability and modularity. It may use techniques such as Software Defined Networking (SDN) [RFC7149] and Network Function Virtualization (NFV) [RFC8172][RFC8568] to create multiple logical (virtual) networks, each tailored for a set of services or a particular tenant or a group of tenants that share the same set of requirements, on top of a common network. How the network slices are engineered can be deployment-specific.

Thus, there is a need to create virtual networks with enhanced characteristics. The tenant of such a virtual network can require a degree of isolation and performance that previously could not be satisfied by traditional overlay VPNs. Additionally, the tenant may ask for some level of control to their virtual networks, e.g., to customize the service paths in a network slice.

These enhanced properties cannot be met with pure overlay networks, as they require tighter coordination and integration between the underlay and the overlay network. This document introduces a new network service called Enhanced VPN: VPN+. VPN+ is built from a virtual network which has a customized network topology and a set of dedicated or shared network resources, including invoked service functions, allocated from the underlay network. Unlike a traditional VPN, an enhanced VPN can achieve greater isolation with strict performance guarantees. These new properties, which have general applicability, may also be of interest as part of a network slicing
solution, but it is not envisaged that VPN+ techniques will be
applied to normal VPN services that can continue to be deployed using
pre-existing mechanisms. Furthermore, it is not intended that large
numbers of VPN+ instances will be deployed within a single network.
See Section 5 for a discussion of scalability considerations.

This document specifies a framework for using existing, modified and
potential new technologies as components to provide a VPN+ service.
Specifically we are concerned with:

- The design of the enhanced data plane.
- The necessary protocols in both the underlay and the overlay of
  the enhanced VPN.
- The mechanisms to achieve integration between overlay and
  underlay.
- The necessary Operation, Administration, and Management (OAM)
  methods to instrument an enhanced VPN to make sure that the
  required Service Level Agreement (SLA) is met, and to take any
  corrective action to avoid SLA violation, such as switching to an
  alternate path.

The required layered network structure to achieve this is shown in
Section 3.1.

Note that, in this document, the four terms "VPN", "Enhanced VPN" (or
"VPN+"), "Virtual Network (VN)", and "Network Slice" may be
considered as describing similar concepts dependent on the viewpoint
from which they are used.

- An enhanced VPN can be considered as a form of VPN, but with
  additional service-specific commitments. Thus, care must be taken
  with the term "VPN" to distinguish normal or legacy VPNs from VPN+
  instances.

- A Virtual Network is a type of service that connects customer edge
  points with the additional possibility of requesting further
  service characteristics in the manner of an enhanced VPN.

- An enhanced VPN or VN is made by creating a slice through the
  resources of the underlay network.

- The general concept of network slicing in a TE network is a larger
  problem space than is addressed by VPN+ or VN, but those concepts
  are tools to address some aspects or realizations of network
  slicing.
2. Overview of the Requirements

In this section we provide an overview of the requirements of an enhanced VPN.

2.1. Isolation between Virtual Networks

One element of the SLA demanded for an enhanced VPN is the degree of isolation from other services in the network. Isolation is a feature requested by some particular customers in the network. Such a feature is offered by a network operator where the traffic from one service instance is isolated from the traffic of other services. There are different grades of isolation that range from simple separation of traffic on delivery (ensuring that traffic is not delivered to the wrong customer) all the way to complete separation within the underlay so that the traffic from different services use distinct network resources.

The terms hard and soft isolation are introduced to identify different isolation cases. A VPN has soft isolation if the traffic of one VPN cannot be received by the customers of another VPN. Both IP and MPLS VPNs are examples of soft isolated VPNs because the network delivers the traffic only to the required VPN endpoints. However, with soft isolation, traffic from one or more VPNs and regular non-VPN traffic may congest the network resulting in packet loss and delay for other VPNs operating normally. The ability for a VPN or a group of VPNs to be sheltered from this effect is called hard isolation, and this property is required by some critical applications.

The requirement is for an operator to offer its customers a choice of different degrees of isolation ranging from soft isolation up to hard isolation so that the traffic of tenants/applications using one enhanced VPN can be separated from the traffic of tenants/applications using another enhanced VPN appropriately. Hard isolation is needed so that applications with exacting requirements can function correctly, despite other demands (perhaps a burst of traffic in another VPN) competing for the underlying resources. In practice isolation may be offered as a spectrum between soft and hard, and in some cases soft and hard isolation may be used in a hierarchical manner.

An example of the requirement for hard isolation is a network supporting both emergency services and public broadband multi-media services. During a major incident the VPNs supporting these services would both be expected to experience high data volumes, and it is important that both make progress in the transmission of their data.
In these circumstances the VPNs would require an appropriate degree of isolation to be able to continue to operate acceptably.

In order to provide the required isolation, resources may have to be reserved in the data plane of the underlay network and dedicated to traffic from a specific VPN or a specific group of VPNs to form different network slices in the underlay network. This may introduce scalability concerns, thus some trade-off needs to be considered to provide the required isolation between network slices while still allowing reasonable sharing inside each network slice.

An optical layer can offer a high degree of isolation, at the cost of allocating resources on a long term and end-to-end basis. Such an arrangement means that the full cost of the resources must be borne by the service that is allocated with the resources. On the other hand, where adequate isolation can be achieved at the packet layer, this permits the resources to be shared amongst many services and only dedicated to a service on a temporary basis. This in turn, allows greater statistical multiplexing of network resources and thus amortizes the cost over many services, leading to better economy. However, the different degrees of isolation required by network slicing cannot be entirely met with existing mechanisms such as Traffic Engineered Label Switched Paths (TE-LSPs). This is because most implementations enforce the bandwidth in the data-plane only at the PEs, but at the P routers the bandwidth is only reserved in the control plane, thus bursts of data can accidentally occur at a P router with higher than committed data rate.

There are several new technologies that provide some assistance with these data plane issues. Firstly there is the IEEE project on Time Sensitive Networking [TSN] which introduces the concept of packet scheduling of delay and loss sensitive packets. Then there is [FLEXE] which provides the ability to multiplex multiple channels over one or more Ethernet links in a way that provides hard isolation. Finally there are advanced queueing approaches which allow the construction of virtual sub-interfaces, each of which is provided with dedicated resource in a shared physical interface. These approaches are described in more detail later in this document.

In the remainder of this section we explore how isolation may be achieved in packet networks.

2.1.1. A Pragmatic Approach to Isolation

A key question is whether it is possible to achieve hard isolation in packet networks, which were never designed to support hard isolation. On the contrary, they were designed to provide statistical multiplexing, a significant economic advantage when compared to a
dedicated, or a Time Division Multiplexing (TDM) network. However, there is no need to provide any harder isolation than is required by the application. Pseudowires [RFC3985] emulate services that would have had hard isolation in their native form. An approximation to this requirement is sufficient in most cases.

Thus, for example, using FlexE or a virtual sub-interface together with packet scheduling as the isolation mechanism of interface resources, optionally along with the partitioning of node resources, a type of hard isolation can be provided that is adequate for many enhanced VPN applications. Other applications may be either satisfied with a classical VPN with or without reserved bandwidth, or may need a dedicated point to point underlay connection. The needs of each application must be quantified in order to provide an economic solution that satisfies those needs without over-engineering.

This spectrum of isolation is shown in Figure 1:

```
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistical Multiplexing</td>
</tr>
<tr>
<td>(Traditional VPNs)</td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>--------------------------------------/</td>
</tr>
<tr>
<td>Pragmatic Isolation</td>
</tr>
<tr>
<td>(Enhanced VPN)</td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Absolute Isolation</td>
</tr>
<tr>
<td>(Dedicated Network)</td>
</tr>
</tbody>
</table>
```

Figure 1: The Spectrum of Isolation

At one end of the above figure, we have traditional statistical multiplexing technologies that support VPNs. This is a service type that has served the industry well and will continue to do so. At the opposite end of the spectrum, we have the absolute isolation provided by dedicated transport networks. The goal of enhanced VPN is pragmatic isolation. This is isolation that is better than is obtainable from pure statistical multiplexing, more cost effective and flexible than a dedicated network, but which is a practical solution that is good enough for the majority of applications. Mechanisms for both soft isolation and hard isolation would be needed to meet different levels of service requirement.

2.2. Performance Guarantee

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 the conformance traffic, the out-of-profile traffic will be handled following other requirements.
Guaranteed maximum packet loss is a common parameter, and is usually addressed by setting the packet priorities, queue size and discard policy. However this becomes more difficult when the requirement is combined with the latency requirement. The limiting case is zero congestion loss, and that is the goal of the Deterministic Networking work that the IETF [DETNET] and IEEE [TSN] are pursuing. In modern optical networks, loss due to transmission errors already approaches zero, but there are the possibilities of failure of the interface or the fiber itself. This can only be addressed by some form of signal duplication and transmission over diverse paths.

Guaranteed maximum latency is required in a number of applications particularly real-time control applications and some types of virtual reality applications. The work of the IETF Deterministic Networking (DetNet) Working Group [DETNET] is relevant; however the scope needs to be extended to methods of enhancing the underlay to better support the delay guarantee, and to integrate these enhancements with the overall service provision.

Guaranteed maximum delay variation is a service that may also be needed. [RFC8578] calls up a number of cases where this is needed, for example electrical utilities have an operational need for this. Time transfer is one example of a service that needs this, 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 virtual networks. Alternatively a dedicated virtual network may be used to provide this as a shared service.

This suggests that a spectrum of service guarantee be considered when deploying an enhanced VPN. As a guide to understanding the design requirements we can consider four types:

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

Best effort service is the basic service that current VPNs can provide.

An assured bandwidth service is one in which the bandwidth over some period of time is assured, this can be achieved either simply based on best effort with over-capacity provisioning, or it can be based on TE-LSPs with bandwidth reservation. The instantaneous bandwidth is however, not necessarily assured, depending on the technique used.
Providing assured bandwidth to VPNs, for example by using TE-LSPs, is not widely deployed at least partially due to scalability concerns. Guaranteed latency and enhanced delivery are not yet integrated with VPNs.

A guaranteed latency service has a latency upper bound provided by the network. Assuring the upper bound is more important than achieving the minimum latency.

In Section 2.1 we considered the work of the IEEE Time Sensitive Networking (TSN) project [TSN] and the work of the IETF DetNet Working group [DETNET] in the context of isolation. The TSN and DetNet work is of greater relevance in assuring end-to-end packet latency. It is also of importance in considering enhanced delivery.

An enhanced delivery service is one in which the underlay network (at layer 3) attempts to deliver the packet through multiple paths in the hope of eliminating packet loss due to equipment or media failures.

It is these last two characteristics that an enhanced VPN adds to a VPN service.

Flex Ethernet [FLEXE] is a useful underlay to provide these guarantees. This is a method of providing time-slot based channelization over an Ethernet bearer. Such channels are fully isolated from other channels running over the same Ethernet bearer. As noted elsewhere this produces hard isolation but makes the reclamation of unused bandwidth more difficult.

These approaches can be used in tandem. It is possible to use FlexE to provide tenant isolation, and then to use the TSN/Detnet approach to provide a performance guarantee inside the a slice or tenant VPN.

2.3. Integration

The only way to achieve the enhanced characteristics provided by an enhanced VPN (such as guaranteed or predicted performance) is by integrating the overlay VPN with a particular set of network resources in the underlay network. This needs be done in a flexible and scalable way so that it can be widely deployed in operator networks to support a reasonable number of enhanced VPN customers.

Taking mobile networks and in particular 5G into consideration, the integration of network and the service functions is a likely requirement. The work in IETF SFC working group [SFC] provides a foundation for this integration.
2.3.1. Abstraction

Integration of the overlay VPN and the underlay network resources does not need to be a tight mapping. As described in [RFC7926], abstraction is the process of applying policy to a set of information about a 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.

Virtual networks can be built on top of an abstracted topology that represents the connectivity capabilities of the underlay network as described in the framework for Abstraction and Control of TE Networks (ACTN) described in [RFC8453] as discussed further in Section 4.5.

2.4. Dynamic Management

Enhanced VPNs need to be created, modified, and removed from the network according to service demand. An enhanced VPN that requires hard isolation must not be disrupted by the instantiation or modification of another enhanced VPN. Determining whether modification of an enhanced VPN can be disruptive to that VPN, and in particular whether the traffic in flight will be disrupted can be a difficult problem.

The data plane aspects of this problem are discussed further in Section 4.

The control plane aspects of this problem are discussed further in Section 4.4.

The management plane aspects of this problem are discussed further in Section 4.

Dynamic changes both to the VPN and to the underlay transport network need to be managed to avoid disruption to services that are sensitive to the change of network performance?

In addition to non-disruptively managing the network as a result of gross change such as the inclusion of a new VPN endpoint or a change to a link, VPN traffic might need to be moved as a result of traffic volume changes.
2.5. Customized Control

In some cases it is desirable that an enhanced VPN has a customized control plane, so that the tenant of the enhanced VPN can have some control to the resources and functions allocated to this enhanced VPN. For example, the tenant may be able to specify the service paths in his own enhanced VPN. Depending on the requirement, an enhanced VPN may have its own dedicated controller, or it may be provided with an interface to a control system which is shared with a set of other tenants, or it may be provided with an interface to the control system provided by the network operator.

Further detail on this requirement will be provided in a future version of the draft.

A description of the control plane aspects of this problem are discussed further in Section 4.4. A description of the management plane aspects of this feature can be found in Section 4.5.

2.6. Applicability

The technologies described in this document should be applicable to a number types of VPN services such as:

- Layer 2 point to point services such as pseudowires [RFC3985]
- Layer 2 VPNs [RFC4664]
- Ethernet VPNs [RFC7209]
- Layer 3 VPNs [RFC4364], [RFC2764]

Where such VPN types need enhanced isolation and delivery characteristics, the technology described here can be used to provide an underlay with the required enhanced performance.

2.7. Inter-Domain and Inter-Layer Network

In some scenarios, an enhanced VPN services may span multiple network domains. A domain is considered to be any collection of network elements within a common realm of address space or path computation responsibility [RFC5151]. And in some domains the operator may own a multi-layered network, for example, a packet network over an optical network. When enhanced VPNs are provisioned in such network scenarios, the technologies used in different network plane (data plane, control plane and management plane) need to provide necessary mechanisms to support multi-domain and multi-layer coordination and integration, so as to provide the required service characteristics.
for different enhanced VPNs, and improve network efficiency and operational simplicity.

3. Architecture of Enhanced VPN

A number of enhanced VPN services will typically be provided by a common network infrastructure. Each enhanced VPN consists of both the overlay and a specific set of dedicated network resources and functions allocated in the underlay to satisfy the needs of the VPN tenant. The integration between overlay and various underlay resources ensures the isolation between different enhanced VPNs, and achieves the guaranteed performance for different services.

An enhanced VPN needs to be designed with consideration given to:

- A enhanced data plane
- A control plane to create enhanced VPN, making use of the data plane isolation and guarantee techniques
- A management plane for enhanced VPN service life-cycle management

These required characteristics are expanded below:

- Enhanced data plane
  * Provides the required resource isolation capability, e.g. bandwidth guarantee.
  * Provides the required packet latency and jitter characteristics.
  * Provides the required packet loss characteristics.
  * Provides the mechanism to identify network slice and the associated resources.

- Control plane
  * Collect the underlying network topology and resources available and export this to other nodes and/or the centralized controller as required.
  * Create the required virtual networks with the resource and properties needed by the enhanced VPN services that are assigned to it.
* Determine the risk of SLA violation and take appropriate avoiding action.

* Determine the right balance of per-packet and per-node state according to the needs of enhanced VPN service to scale to the required size.

  o Management plane

* Provides an interface between the enhanced VPN provider (e.g. the Transport Network (TN) Manager) and the enhanced VPN clients (e.g. the 3GPP Management System) such that some of the operation requests can be met without interfering with the enhanced VPN of other clients.

* Provides an interface between the enhanced VPN provider and the enhanced VPN clients to expose transport network capability information toward the enhanced VPN client.

* Provides the service life-cycle management and operation of enhanced VPN (e.g. creation, modification, assurance/monitoring and decommissioning).

OAM

* Provides the OAM tools to verify the connectivity and performance of the enhanced VPN.

* Provide the OAM tools to verify whether the underlay network resources are correctly allocated and operated properly.

  o Telemetry

* Provides the mechanism to collect the data plane, control plane and management plane data of the network, more specifically:

* Provides the mechanism to collect network data of the underlay network for overall performance evaluation and the enhanced VPN service planning.

* Provides the mechanism to collect network data of each enhanced VPN for the monitoring and analytics of the characteristics and SLA fulfilment of enhanced VPN services.
3.1. Layered Architecture

The layered architecture of enhanced VPN is shown in Figure 2.

Underpinning everything is the physical network infrastructure layer consisting of partitioned links and nodes which provide the underlying resources used to provision the separated virtual networks. Various components and techniques as discussed in Section 4 can be used to provide the resource partition, such as FlexE, Time Sensitive Networking, Deterministic Networking, etc. These partitions may be physical, or virtual so long as the SLA required by the higher layers is met.

These techniques can be used to provision the virtual networks with the dedicated resources that they need. To get the required
functionality there needs to be integration between these overlays and the underlay providing the physical resources.

The centralized controller is used to create the virtual networks, to allocate the resources to each virtual network and to provision the enhanced VPN services within the virtual networks. A distributed control plane may also be used for the distribution of the topology and attribute information of the virtual networks.

The creation and allocation process needs to take a holistic view of the needs of all of its tenants, and to partition the resources accordingly. However within a virtual network these resources can, if required, be managed via a dynamic control plane. This provides the required scalability and isolation.

3.2. Multi-Point to Multi-Point (MP2MP)

At the VPN service level, the connectivity is usually mesh or partial-mesh. To support such kinds of VPN service, the corresponding underlay is also an abstract MP2MP medium. However when service guarantees are provided, the point-to-point path through the underlay of the enhanced VPN needs to be specifically engineered to meet the required performance guarantees.

3.3. Application Specific Network Types

Although a lot of the traffic that will be carried over the enhanced VPN will likely be IPv4 or IPv6, the design has to be capable of carrying other traffic types, in particular Ethernet traffic. This is easily accomplished through the various pseudowire (PW) techniques [RFC3985]. Where the underlay is MPLS, Ethernet can be carried over the enhanced VPN encapsulated according to the method specified in [RFC4448]. Where the underlay is IP, Layer Two 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 layer-2 types for both PW over MPLS and for L2TPv3.

3.4. Scaling Considerations

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 are able to deliver services without placing per-service state in the core of the underlay network.

Enhanced VPNs may need to install some additional state within the network to achieve the additional features that they require. Solutions must consider minimising and controlling the scale of such
state, and deployment architectures should constrain the number of enhanced VPNs that would exist where such services would place additional state in the network. It is expected that the number of enhanced VPN would be a small number in the beginning, and even in future the number of enhanced VPN will be much less than traditional VPNs, because pre-existing VPN techniques would be 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 VPN+ instances. It will usually be possible to aggregate a set of VPN+ services so that they share the same virtual network and the same set of network resources (much in the way that current VPNs are aggregated over transport tunnels) so that collections of enhanced VPNs that require the same behaviour from the network in terms of resource reservation, latency bounds, resiliency, etc. are able to be grouped together. This is an important feature to assist with the scaling characteristics of VPN+ deployments.

See Section 5 for a greater discussion of scalability considerations.

4. Candidate Technologies

A VPN is a network created by applying a multiplexing technique to the underlying network (the underlay) in order to distinguish the traffic of one VPN from that of another. A VPN path that travels by other than the shortest path through the underlay normally requires state in the underlay to specify that path. State is normally applied to the underlay through the use of the RSVP Signaling protocol, or directly through the use of an SDN controller, although other techniques may emerge as this problem is studied. This state gets harder to manage as the number of VPN paths increases. Furthermore, as we increase the coupling between the underlay and the overlay to support the enhanced VPN service, this state will increase further.

In an enhanced VPN different subsets of the underlay resources can be dedicated to different enhanced VPNs or different groups of enhanced VPNs. An enhanced VPN solution thus needs tighter coupling with underlay than is the case with existing VPNs. We cannot, for example, share the network resource between enhanced VPNs which require hard isolation.

4.1. Layer-Two Data Plane

A number of candidate Layer-2 packet or frame-based data plane solutions which can be used provide the required isolation and guarantee are described in following sections.
FlexE [FLEXE] is a method of creating a point-to-point Ethernet with a specific fixed bandwidth. FlexE provides the ability to multiplex multiple channels over an Ethernet link in a way that provides hard isolation. FlexE also supports the bonding of multiple links, which can be used to create larger links out of multiple low capacity links in a more efficient way than traditional link aggregation. FlexE also supports the sub-rating of links, which allows an operator to only use a portion of a link. However it is a only a link level technology. When packets are received by the downstream node, they need to be processed in a way that preserves that isolation in the downstream node. This in turn requires a queuing and forwarding implementation that preserves the end-to-end isolation.

If different FlexE channels are used for different services, then no sharing is possible between the FlexE channels. This in turn means that it may be difficult to dynamically redistribute unused bandwidth to lower priority services. This may increase the cost of providing services on the network. On the other hand, FlexE can be used to provide hard isolation between different tenants on a shared interface. The tenant can then use other methods to manage the relative priority of their own traffic in each FlexE channel.

Methods of dynamically re-sizing FlexE channels and the implication for enhanced VPN are for further study.

4.1.2. Dedicated Queues

In order to provide multiple isolated virtual networks for enhanced VPN, the conventional DiffServ based queuing system [RFC2475] [RFC4594] is considered insufficient, as DiffServ does not always provide enough queues to differentiate between traffic of different enhanced VPNs, or the range of service classes that each need to provide to their tenants. This problem is particularly acute with an MPLS underlay, because MPLS only provides 8 Traffic Classes (TC), and it’s highly likely that there will be more than eight enhanced VPN instances supported by a network. In addition, DiffServ, as currently implemented, mainly provides relative priority-based scheduling, and is difficult to achieve quantitative resource reservation. In order to address this problem and reduce the interference between enhanced VPNs, it is necessary to steer traffic
of enhanced VPNs to dedicated input and output queues. Some routers have large amount of queues and sophisticated queuing systems, which could be used or enhanced to provide the granularity and level of isolation required by the applications of enhanced VPN. For example, on one physical interface, the queuing system can provide a set of virtual sub-interfaces, each allocated with dedicated queueing and buffer resources. Sophisticated queuing systems of this type may be used to provide end-to-end virtual isolation between traffic of different enhanced VPNs.

4.1.3. Time Sensitive Networking

Time Sensitive Networking (TSN) [TSN] is an IEEE project that is designing a method of carrying time sensitive information over Ethernet. It introduces the concept of packet scheduling where a high priority packet stream may be given a scheduled time slot thereby guaranteeing that it experiences no queuing delay and hence a reduced latency. However, when no scheduled packet arrives, its reserved time-slot is handed over to best effort traffic, thereby improving the economics of the network. The mechanisms defined in TSN can be used to meet the requirements of time sensitive services of an enhanced VPN.

Ethernet can be emulated over a Layer 3 network using a pseudowire. However the TSN payload would be opaque to the underlay and thus not treated specifically as time sensitive data. The preferred method of carrying TSN over a layer 3 network is through the use of deterministic networking as explained in the following section of this document.

4.2. Layer-Three Data Plane

We now consider the problem of slice differentiation and resource representation in the network layer. The candidate technologies are:

- Deterministic Networking
- MPLS-TE
- Segment Routing

4.2.1. Deterministic Networking

Deterministic Networking (DetNet) [I-D.ietf-detnet-architecture] is a technique being developed in the IETF to enhance the ability of layer-3 networks to deliver packets more reliably and with greater control over the delay. The design cannot use re-transmission techniques such as TCP since that can exceed the delay tolerated by
the applications. Even the delay improvements that are achieved with Stream Control Transmission Protocol Partial Reliability Extension (SCTP-PR) [RFC3758] do not meet the bounds set by application demands. DetNet pre-emptively sends copies of the packet over various paths to minimize the chance of all copies of a packet being lost, and trims duplicate packets to prevent excessive flooding of the network and to prevent multiple packets being delivered to the destination. It also seeks to set an upper bound on latency. The goal is not to minimize latency; the optimum upper bound paths may not be the minimum latency paths.

DetNet is based on flows. It currently does not specify the use of underlay topology other than the base topology. To be of use for enhanced VPN, DetNet needs to be integrated with different virtual topologies of enhanced VPNs.

The detailed design that allows the use DetNet in a multi-tenant network, and how to improve the scalability of DetNet in a multi-tenant network are topics for further study.

4.2.2. MPLS Traffic Engineering (MPLS-TE)

MPLS-TE introduces the concept of reserving end-to-end bandwidth for a TE-LSP, which can be used as the underlay of VPNs. It also introduces the concept of non-shortest path routing through the use of the Explicit Route Object [RFC3209]. VPN traffic can be run over dedicated TE-LSPs to provide reserved bandwidth for each specific connection in a VPN. Some network operators have concerns about the scalability and management overhead of RSVP-TE system, and this has lead them to consider other solutions for their networks.

4.2.3. Segment Routing

Segment Routing [RFC8402] is a method that prepends instructions to packets at the head-end node and optionally at various points as it passes through the network. These instructions allow the packets to be routed on paths other than the shortest path for various traffic engineering reasons. With SR, a path needs to be dynamically created through a set of segments by simply specifying the Segment Identifiers (SIDs), i.e. instructions rooted at a particular point in the network. By encoding the state in the packet, per-path state is transitioned out of the network.

With current segment routing, the instructions are used to specify the nodes and links to be traversed. An SR traffic engineered path operates with a granularity of a link with hints about priority provided through the use of the traffic class (TC) or Differentiated Services Code Point (DSCP) field in the header. However to achieve
the latency and isolation characteristics that are sought by the enhanced VPN users, steering packets through specific queues and resources will likely be required. With SR, it is possible to introduce such fine-grained packet steering by specifying the queues and resources through an SR instruction list.

Note that the concept of a queue is a useful abstraction for many types of underlay mechanism that may be used to provide enhanced isolation and latency support. How the queue satisfies the requirement is implementation specific and is transparent to the layer-3 data plane and control plane mechanisms used.

Both SR-MPLS and SRv6 are candidate data plane technologies for enhanced VPN. In some cases they can further be used for DetNet to meet the packet loss, delay and jitter requirement of particular service. How to provide the DetNet enhanced delivery in an SRv6 environment is specified in [I-D.geng-spring-srv6-for-detnet].

4.3. Non-Packet Data Plane

Non-packet underlay data plane technologies often have TE properties and behaviors, and meet many of the key requirements in particular 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 (and hence slices).

The control and management planes for non-packet data plane technologies have most in common with MPLS-TE (Section 4.2.2) and offer the same set of advanced features [RFC3945]. Furthermore, management techniques such as ACTN ([RFC8453] and Section 4.6) can be used to aid in the reporting of underlying network topologies, and the creation of virtual networks with the resource and properties needed by the enhanced VPN services.

4.4. Control Plane

Enhanced VPN would likely be based on a hybrid control mechanism, which takes advantage of the logically centralized controller for on-demand provisioning and global optimization, whilst still relies on distributed control plane to provide scalability, high reliability, fast reaction, automatic failure recovery etc. Extension and optimization to the distributed control plane is needed to support the enhanced properties of VPN+.

RSVP-TE provides the signaling mechanism of establishing a TE-LSP with end-to-end resource reservation. It can be used to bind the VPN
to specific network resource allocated within the underlay, but there are the above mentioned scalability concerns.

SR does not have the capability of signaling the resource reservation along the path, nor do its currently specified distributed link state routing protocols. On the other hand, the SR approach provides a way of efficiently binding the network underlay and the enhanced VPN overlay, as it reduces the amount of state to be maintained in the network. An SR-based approach with per-slice resource reservation can easily create dedicated SR network slices, and the VPN services can be bound to a particular SR network slice. A centralized controller can perform resource planning and reservation from the controller’s point of view, but this does not ensure resource reservation is actually done in the network nodes. Thus, if a distributed control plane is needed, either in place of an SDN controller or as an assistant to it, the design of the control system needs to ensure that resources are uniquely allocated in the network nodes for the correct services, and not allocated to other services causing unintended resource conflict.

In addition, in multi-domain and multi-layer networks, the centralized and distributed control mechanisms will be used for inter-domain coordination and inter-layer optimization, so that the diverse and customized enhanced VPN service requirement could be met. The detailed mechanisms will be described in a future version.

4.5. Management Plane

In the context of 5G end-to-end network slicing, the management of enhanced VPN is considered as the management of transport network part of the end-to-end network slice. 3GPP management system may provide the topology and QoS parameters as requirement to the management plane of transport network. It may also require the transport network to expose the capability and status of the transport network slice. Thus an interface between enhanced VPN management plane and 3GPP network slice management system and relevant service data models are needed for the coordination of end-to-end network slice management.

The management plane interface and data models for enhanced VPN can be based on the service models such as:

- VPN service models defined in [RFC8299] and [RFC8466]
- Possible augmentations and extensions (e.g., [I-D.ietf-teas-te-service-mapping-yang]) to VPN service models
o ACTN related service models such as [I-D.ietf-teas-actn-vn-yang] and [I-D.ietf-teas-actn-pm-telemetry-autonomics].

o VPN network model as defined in [I-D.aguado-opsawg-l3sm-l3nm].

o TE Tunnel model as defined in [I-D.ietf-teas-yang-te].

These data models can be applicable in the provisioning of enhanced VPN service. The details are described in Section 4.6.

4.6. Applicability of Service Data Models to Enhanced VPN

ACTN supports operators in viewing and controlling different domains and presenting virtualized networks to their customers. The ACTN framework [RFC8453] highlights how:

o Abstraction of the underlying network resources are provided to higher-layer applications and customers.

o Virtualization of underlying resources, whose selection criterion is the allocation of those resources for the customer, application, or service.

o Creation of a virtualized environment allowing operators to view and control multi-domain networks as a single virtualized network.

o The presentation to customers of networks as a virtual network via open and programmable interfaces.

The infrastructure managed through the Service Data models comprises traffic engineered network resources (e.g. bandwidth, time slot, wavelength) and VPN service related resources (e.g. Route Target (RT) and Route Distinguisher (RD)).

The type of network virtualization enabled by ACTN managed infrastructure provides customers and applications (tenants) with the capability to utilize and independently control allocated virtual network resources as if they were physically their own resources.

The Customer VPN model (e.g. L3SM) or an ACTN Virtual Network (VN) model is a customer view of the ACTN managed infrastructure, and is presented by the ACTN provider as a set of abstracted services or resources.

L3VPN network model or TE tunnel model is a network view of the ACTN managed infrastructure, and is presented by the ACTN provider as a set of transport resources.
Depending on the agreement between customer and provider, various VPN/VN operations and VPN/VN views are possible.

- **Virtual Network Creation**: A VPN/VN could be pre-configured and created via static or dynamic request and negotiation between customer and provider. It must meet the specified SLA attributes which satisfy the customer’s objectives.

- **Virtual Network Operations**: The virtual network may be further modified and deleted based on customer request to request changes in the network resources reserved for the customer, and used to construct the network slice. The customer can further act upon the virtual network to manage traffic flow across the virtual network.

- **Virtual Network View**: The VPN/VN topology from a customer point of view. These may be a variety of tunnels, or an entire VN topology, or an VPN service topology. Such connections may comprise of customer end points, access links, intra-domain paths, and inter-domain links.

Dynamic VPN/VN Operations allow a customer to modify or delete the VPN/VN. The customer can further act upon the virtual network to create/modify/delete virtual links and nodes or VPN sites. These changes will result in subsequent tunnel management or VPN service management in the operator’s networks.

### 4.6.1. Enhanced VPN Delivery in ACTN Architecture

ACTN provides VPN connections or VN connections between multiple sites as requested via a VPN requestor enabled by the Customer Network Controller (CNC). The CNC is managed by the customer themselves, and interacts with the network provider’s Multi-Domain Service Controller (MDSC). The Provisioning Network Controllers (PNC) are responsible for network resource management, thus the PNCs are remain entirely under the management of the network provider and are not visible to the customer.

The benefits of this model include:

- **Provision of edge-to-edge VPN multi-access connectivity.**

- **Management is mostly performed by the network provider, with some flexibility delegated to the customer-managed CNC.**

Figure 3 presents a more general representation of how multiple enhanced VPNs may be created from the resources of multiple physical networks using the CNC, MDSC, and PNC components of the ACTN.
architecture. Each enhanced VPN is controlled by its own CNC. The CNCs send requests to the provider’s MDSC. The provider manages two different physical networks each under the control of PNC. The MDSC asks the PNCs to allocate and provision resources to achieve the enhanced VPNs. In this figure, one enhanced VPN is constructed solely from the resources of one of the physical networks, while the VPN uses resources from both physical networks.

![Diagram of generic VPN+ delivery in the ACTN architecture](image)

**Figure 3: Generic VPN+ Delivery in the ACTN Architecture**

### 4.6.2. Enhanced VPN Features with Service Data Models

This section discusses how the service data models can fulfill the enhanced VPN requirements described earlier in this document. As previously noted, key requirements of the enhanced VPN include:

1. Isolation between VPNs/VNs
2. Guaranteed Performance
3. Integration

4. Dynamic Management

5. Customized Control

The subsections that follow outline how each requirement is met using ACTN.

4.6.2.1. Isolation Between VPN/VNs

The VN YANG model [I-D.ietf-teas-actn-vn-yang] and the TE-service mapping model [I-D.ietf-teas-te-service-mapping-yang] fulfill the VPN/VN isolation requirement by providing the following features for the VPN/VNs:

- Each VN is identified with a unique identifier (vn-id and vn-name) and so is each VN member that belongs to the VN (vn-member-id).
- Each VPN is identified with a unique identifier (vpn-id) and can be mapped to one specific VN. While multiple VPNs may be mapped to the same VN according to service requirement and operator’s policy.
- Each VPN and the corresponding VN is managed and controlled independent of other VPNs/VNs in the network with proper availability level.
- Each VPN/VN is instantiated with an isolation requirement described by the TE-service mapping model [I-D.ietf-teas-te-service-mapping-yang]. This mapping supports:
  * Hard isolation with deterministic characteristics (e.g., this case may need an optical bypass tunnel or a DetNet/TSN tunnel to guarantee latency with no jitter)
  * Hard isolation (i.e., dedicated TE resources in all underlays)
  * Soft isolation (i.e., resource in some layer may be shared while in some other layers is dedicated).
  * No isolation (i.e., sharing with other VPN/VN).

4.6.2.2. Guaranteed Performance

Performance objectives of a VN need first to be expressed in order to assure the performance guarantee.
Performance objectives of a VPN [RFC8299][RFC8466] are expressed with QoS profile, either standard profile or customer profile. The customer QoS profile include the following properties:

- Rate-limit
- Bandwidth
- Latency
- Jitter

[I-D.ietf-teas-actn-vn-yang] and [I-D.ietf-teas-yang-te-topo] allow configuration of several TE parameters that may affect the VN performance objectives as follows:

- Bandwidth
- Objective function (e.g., min cost path, min load path, etc.)
- Metric Types and their threshold:
  - TE cost, IGP cost, Hop count, or Unidirectional Delay (e.g., can set all path delay <= threshold)

Once these requests are instantiated, the resources are committed and guaranteed through the life cycle of the VPN/VN.

4.6.2.3. Integration

L3VPN network model provides mechanism to correlate customer’s VPN and the VPN service related resources (e.g. RT and RD) allocated in the provider’s network.

VPN/Network performance monitoring model [I-D.www-bess-yang-vpn-service-pm] provides mechanisms to monitor and manage network Performance on the topology at different layer or the overlay topology between VPN sites.

VN model and Performance Monitoring Telemetry model provides mechanisms to correlate customer’s VN and the actual TE tunnels instantiated in the provider’s network. Specifically:

- Link each VN member to actual TE tunnel.
- Each VN can be monitored on a various level such as VN level, VN member level, TE-tunnel level, and link/node level.
Service function integration with network topology (L3 and TE topology) is in progress in [I-D.ietf-teas-sf-aware-topo-model]. Specifically, [I-D.ietf-teas-sf-aware-topo-model] addresses a number of use-cases that show how TE topology supports various service functions.

4.6.2.4. Dynamic Management

ACTN provides an architecture that allows the CNC to interact with the MDSC which is network provider’s SDN controller. This gives the customer control of their VPN or VNs.

e.g., the ACTN VN model [I-D.ietf-teas-actn-vn-yang] allows the VN to life-cycle management such as create, modify, and delete VNs on demand. Another example is L3VPN service model [RFC8299] which allows the VPN lifecycle management such as VPN creation, modification and deletion on demand.

4.6.2.5. Customized Control

ACTN provides a YANG model that allows the CNC to control a VN as a "Type 2 VN" that allows the customer to provision tunnels that connect their endpoints over the customized VN topology.

For some VN members, the customers are allowed to configure the path (i.e., the sequence of virtual nodes and virtual links) over the VN/abstract topology.

4.6.3. 5G Transport Service Delivery via Coordinated Data Modules

The overview of network slice structure as defined in the 3GPP 5GS is shown in Figure 5. The terms are described in specific 3GPP documents (e.g. [TS23501] and [TS28530].)
Figure 4: Overview of Structure of Network Slice in 3GPP 5GS

To support 5G service (e.g., 5G MBB service), L3VPN service model [RFC8299] and TEAS VN model [I-D.ietf-teas-actn-vn-yang] can be both provided to describe 5G MBB Transport Service or connectivity service. L3VPN service model is used to describe end-to-end IP connectivity service while TEAS VN model is used to describe TE connectivity service between VPN sites or between RAN NFs and Core network NFs. VN in TEAS VN model and support point-to-point or multipoint-to-multipoint connectivity service and can be seen as one example of network slice.

TE Service mapping model can be used to map L3VPN service requests onto underlying network resource and TE models to get TE network setup.
For IP VPN service provision, the service parameters in the L3VPN service model [RFC8299] can be decomposed into a set of configuration parameters described in the L3VPN network model [I-D.aguado-opsawg-l3sm-l3nm] which will get VPN network setup.

5. Scalability Considerations

Enhanced VPN provides the performance guaranteed services in packet networks, but with the potential cost of introducing additional states into the network. There are at least three ways that this adding state might be presented in the network:

- Introduce 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. The cost is also that systems will have capabilities enabled in case they are called upon by a service. This is a type of latent state, and increases as we more precisely specify the path and resources that need to be exclusively available to a VPN.

- Introduce the state to the network. This is normally done by creating a path using RSVP-TE, which can be extended to introduce any element that needs to be specified along the path, for example explicitly specifying queuing policy. It is of course possible to use other methods to introduce path state, such as via a Software Defined Network (SDN) controller, or possibly by modifying a routing protocol. With this approach there is state per path per path characteristic that needs to be maintained over its life-cycle. This is more state than is needed using SR, but the packets are shorter.

- Provide a hybrid approach based on using binding SIDs to create path fragments, and bind them together with SR.

Dynamic creation of a VPN path using SR requires less state maintenance in the network core at the expense of larger VPN headers on the packet. 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 resource on the routers are specified. Reducing the state in the network is important to enhanced VPN, as it requires the overlay to be more closely integrated with the underlay than with traditional VPNs. This tighter coupling would normally mean that more state needed to be created and maintained in the network, as the state about fine granularity processing would need to be loaded and maintained in the routers. However, a segment routed
approach allows much of this state to be spread amongst the network ingress nodes, and transiently carried in the packets as SIDs.

These approaches are for further study.

5.1. 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, or minimizing state and increasing the stack depth.

5.2. RSVP Scalability

The traditional method of creating a resource allocated path through an MPLS network is to use the RSVP protocol. However there have been concerns that this requires significant continuous state maintenance in the network. There are ongoing works to improve the scalability of RSVP-TE LSPs in the control plane [RFC8370].

There is also concern at the scalability of the forwarder footprint of RSVP as the number of paths through an LSR grows [RFC8577] proposes to address this by employing SR within a tunnel established by RSVP-TE.

5.3. SDN Scaling

The centralized approach of SDN requires state to be stored in the network, but does not have the overhead of also requiring control plane state to be maintained. Each individual network node may need to maintain a communication channel with the SDN controller, but that compares favourably with the need for a control plane to maintain communication with all neighbors.

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

6. OAM Considerations

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

- Instrumentation of the underlay so that the network operator can be sure that the resources committed to a tenant are operating correctly and delivering the required performance.
o Instrumentation of the overlay by the tenant. 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 isolation and the various committed performance characteristics.

o Instrumentation of the overlay by the network 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.

o Verification of the conformity of the path to the service requirement. This may need to be done as part of a commissioning test.

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

7. Telemetry Considerations

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

As defined in [I-D.ietf-opsawg-ntf], 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.

How the telemetry mechanisms could be used or extended for the enhanced VPN service will be described in a future version.

8. Enhanced Resiliency

Each enhanced VPN has a life-cycle, and needs modification during deployment as the needs of its tenant change. Additionally, as the network as a whole evolves, there will need to be garbage collection 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. This is a single action by the head-end 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 up and meet the required SLA before traffic is
transitioned to it. It is possible for deadlocks arise as a result
of the network becoming fragmented over time, such that it is
impossible to create a new path or modify a existing path without
impacting the SLA of other paths. Resolution of this situation is as
much a commercial issue as it is a technical issue and is outside the
scope of this document.

There are however two manifestations of the latency problem that are
for further study in any of these approaches:

- The problem of packets overtaking one and other if a path latency
  reduces during a transition.

- The problem of the latency transient 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 50ms [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 proposed by the IETF deterministic network work with
multiple in-network replication and the culling of later packets
[I-D.ietf-detnet-architecture].

In addition to the approach used to protect high priority packets,
consideration has to be given to the impact of best effort traffic on
the high priority packets during a transient. Specifically if a
conventional re-convergence process is used there will inevitably be
micro-loops and whilst 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.

9. Operational Considerations

TBD in a future version.

10. Security Considerations

All types of virtual network require special consideration to be
given to the isolation between the tenants. In this regard enhanced
VPNs neither introduce, no experience a greater security risk than
another VPN of the same base type. However, in an enhanced virtual network service the isolation requirement needs to be considered. If a service requires a specific latency then it can be damaged by simply delaying the packet through the activities of another tenant. In a network with virtual functions, depriving a function used by another tenant of compute resources can be just as damaging as delaying transmission of a packet in the network. The measures to address these dynamic security risks must be specified as part to the specific solution.

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 own 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.

11. IANA Considerations

There are no requested IANA actions.

12. Contributors
13. Acknowledgements

The authors would like to thank Charlie Perkins, James N Guichard and John E Drake 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).

14. References

14.1. Normative References

[I-D.ietf-teas-actn-vn-yang]

[I-D.ietf-teas-te-service-mapping-yang]


14.2. Informative References


Dong, et al. Expires March 15, 2020
[DETNET] "Deterministic Networking", March ,
<https://datatracker.ietf.org/wg/detnet/about/>.

[FLEXE] "Flex Ethernet Implementation Agreement", March 2016,

[I-D.aguado-opsawg-l3sm-l3nm]
Aguado, A., Dios, O., Lopezalvarez, V.,
daniel.voyer@bell.ca, d., and L. Munoz, "Layer 3 VPN
Network Model", draft-aguado-opsawg-l3sm-l3nm-01 (work in
progress), July 2019.

[I-D.geng-spring-srv6-for-detnet]
Geng, X., Li, Z., and M. Chen, "SRv6 for Deterministic
Networking (DetNet)", draft-geng-spring-srv6-for-detnet-00
(work in progress), July 2019.

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

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

[I-D.ietf-opsawg-ntf]
Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and
A. Wang, "Network Telemetry Framework", draft-ietf-opsawg-
ntf-01 (work in progress), June 2019.

[I-D.ietf-teas-actn-pm-telemetry-autonomics]
Lee, Y., Dhody, D., Karunanithi, S., Vilata, R., King, D.,
and D. Ceccarelli, "YANG models for VN & TE Performance
Monitoring Telemetry and Scaling Intent Autonomics",
draft-ietf-teas-actn-pm-telemetry-autonomics-00 (work in
progress), July 2019.

[I-D.ietf-teas-sf-aware-topo-model]
Brysken, I., Liu, X., Lee, Y., Guichard, J., Contreras,
L., Ceccarelli, D., and J. Tantsura, "SF Aware TE Topology
YANG Model", draft-ietf-teas-sf-aware-topo-model-03 (work
in progress), March 2019.
[I-D.ietf-teas-yang-te]

[I-D.ietf-teas-yang-te-topo]

[I-D.www-bess-yang-vpn-service-pm]

[NGMN-NS-Concept]


Authors’ Addresses

Jie Dong
Huawei

Email: jie.dong@huawei.com

Stewart Bryant
Futurewei

Email: stewart.bryant@gmail.com

Zhenqiang Li
China Mobile

Email: lizhenqiang@chinamobile.com

Takuya Miyasaka
KDDI Corporation

Email: ta-miyasaka@kddi.com

Young Lee
Sung Kyun Kwan University

Email: younglee.tx@gmail.com