Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 2, 2020

J. Dong
S. Bryant
Huawei Technologies
T. Miyasaka
KDDI Corporation
Y. Zhu
China Telecom
F. Qin
Z. Li
China Mobile

July 1, 2019

Segment Routing for Enhanced VPN Service
draft-dong-spring-sr-for-enhanced-vpn-04

Abstract

Enhanced VPN (VPN+) is an enhancement to VPN technology to enable it to support the needs of new applications, particularly applications that are associated with 5G services. These applications require better isolation from both control and data plane's perspective and have more stringent performance requirements than can be provided with overlay VPNs. The characteristics of an enhanced VPN as perceived by its tenant needs to be comparable to those of a dedicated private network. This requires tight integration between the overlay VPN and the underlay network topology and resources in a scalable manner. An enhanced VPN may form the underpinning of 5G network slicing, but will also be of use in its own right. This document describes the use of segment routing based mechanisms to provide the enhanced VPN service with required network topology and resources. The overall mechanism of using segment routing to provide enhanced VPN service is also described. The proposed mechanism is applicable to both SR with MPLS data plane and SR with IPv6 data plane (SRv6).

time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 2, 2020.

Table of Contents

1. Introduction

Driven largely by needs arising from the 5G mobile network design, the concept of network slicing has gained traction [NGMN-NS-Concept] [TS23501][TS28530] [BBF-SD406]. Network slicing requires to partition the physical network to several pieces to provide each network slice with the required networking, computing, and storage resources and functions drawn from a shared pool. Each network slice can be seen as (and operated as) an independent virtual network.

For transport network, there is a need to create virtual networks with enhanced characteristics. Such a virtual network can provide a customized network topology, and a degree of isolation and performance guarantee that previously could only be satisfied by dedicated networks. Additionally, a network slice tenant may ask for some level of control to their virtual network e.g. to customize the service paths in the network slice.

The enhanced VPN service (VPN+) as described in [I-D.ietf-teas-enhanced-vpn] is targeted at new applications which require better isolation from both control plane and data plane's perspective, and have more stringent performance requirements than can be provided with existing overlay VPNs. An enhanced VPN may form the underpinning of network slicing, but will also be of use in its own right.

Although a VPN can be associated with a set of dedicated RSVP-TE [RFC3209] LSPs with bandwidth reservation to provide some level of guarantee to service performance, such mechanisms would introduce per-VPN per-path states in the network, which is known to have scalability issues [RFC5439] and has not been widely adopted in production networks.

Segment Routing (SR) [RFC8402] specifies a mechanism to steer packets through an ordered list of segments. It can achieve explicit source routing without introducing per-path state into the network. Compared with RSVP-TE, currently SR does not have the capability of reserving or identifying a particular set of network resources for paricular services or customers. Although a centralized controller can have a global view of network state and can provision different services onto different SR paths, in data plane it still relies on traditional DiffServ QoS mechanism [RFC2474] [RFC2475] to provide coarse-grained traffic differentiation in the network. While such kind of mechanism may be sufficient for some types of services, it cannot meet the stringent requirement of some enhanced VPN services.

This document extends the SR paradigm by introducing additional Segment Identifiers (SIDs) to represent different virtual network

topologies and a corresponding set of network resources allocated on network segments. A group of SR SIDs can be used to specify the customized topology of an enhanced VPN, and can be used to steer the service traffic to be processed with the corresponding set of network resources. The overall mechanism of using segment routing to provide enhanced VPN is described. The proposed mechanism is applicable to both SR with MPLS data plane (SR-MPLS) and SR with IPv6 data plane (SRv6).

2. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC 2119 [RFC2119] RFC8174 [RFC8174][when, and only when, they appear in all capitals, as shown here.

3. Segment Routing with Topology and Resource Awareness

In order to support enhanced VPN service, the overlay VPNs need to be integrated with the underlay network in terms of network topology and resources. More specifically, enhanced VPNs need to be mapped to different virtual topologies to provide customized connectivity, and different set of network resources may be allocated to different enhanced VPNs, or different groups of enhanced VPNs, to meet the diverse performance requirement. When segment routing is used to enable enhanced VPNs, it is necessary that the SR service paths can be associated with a particular virtual network topology, and a particular set of network resources.

In segment routing, several types of segments have been defined to represent topological or service instructions. A topological segment may be a node segment or an adjacency segment. A service segment may be associated with specific service function for service chaining purpose. This document introduces SR segments which can be associated with particular network topology and particular set of network resources.

This section describes the mechanisms to identify the associated virtual network topology and resource information with the two SR data plane instantiations: SR-MPLS and SRv6.

3.1. SR-MPLS

In SR-MPLS [I-D.ietf-spring-segment-routing-mpls], IGP Adjacency Segment (Adj-SID) is an IGP-segment attached to a unidirectional adjacency or a set of unidirectional adjacencies. IGP Node segment is an IGP-Prefix segment that identifies a specific router (e.g., a

loopback). In [I-D.ietf-idr-bgpls-segment-routing-epe], PeerAdj SID is used as instruction to steer over a specific local interface towards a specific peer node in a peering Autonomous System (AS). These types of SIDs can be extended to represent both topological elements and the resources allocated on a particular network element.

For one particular IGP link, multiple Adj-SIDs SHOULD be allocated, each of which is associated with a paritcular virtual network topology, and MAY represent a subset of link resources. Several approaches can be used to partition the link resource, such as logical sub-interfaces, dedicated queues, etc. The detailed mechanism of resource partitioning is out of scope of this document. Similarly, for one particular IGP node, multiple node-SIDs SHOULD be allocated, each of which is associated with a paritcular virtual network topology, and may represent a subset of the node resource (e.g. the processing resources). For one particular inter-domain link, multiple BGP PeerAdj SIDs [I-D.ietf-idr-bgpls-segment-routing-epe] can be allocated, each of which is associated with a paritcular virtual network topology which spans multiple domains, and may represent a subset of link resource on the inter-domain link. Note that this per-segment resource allocation complies to the SR paradigm, which avoids introducing per-path state into the network.

A group of adj-SIDs and node-SIDs associated with the same virtual network can be used to construct the SR SID-lists (either strict or loose) for the service packet forwarding of a particular enhanced VPN. This group of SIDs MAY also represent the set of network resources which are reserved for a particular enhanced VPN, or a group of enhanced VPNs.

In data packet forwarding, the adj-SID and node-SID are used to identify the virtual network the packet belongs to, so that a virtual network specific next-hop can be determined. The adj-SIDs MAY also be used to steer traffic of different enhanced VPNs into different set of link resources. The node SIDs MAY also be used to steer traffic of different enhanced VPNs into different set of node resources. When a node-SID is used in the SID-list to build an SR loose path, the transit nodes use the node SID to identify the virtual network, and MAY process the packet using the local resources allocated for the corresponding virtual network. Note in this case, Penultimate Hop Popping (PHP) [RFC3031] MUST be disabled.

This mechanism requires to allocate additional node-SIDs and adj-SIDs for each virtual network (network slice). As the number of virtual networks increases, the number of SIDs would increase accordingly. It is expected that this mechanism is applicable to a network with a limited number of network slices.

3.2. SRv6

As specified in [I-D.ietf-spring-srv6-network-programming], an SRv6 Segment (SID) is a 128-bit value which consists of a locator (LOC) and a function (FUNCT), optionally it may also contain additional arguments (ARG) immediately after the FUNCT. The LOC of the SID is routable and leads to the node which instantiates that SID, which means the LOC can be parsed by all nodes in the network. The FUNCT part of the SID is an opaque identification of a local function bound to the SID, which means the FUNCT and ARG parts can only be parsed by the node which instantiates that SID.

In order to support multiple virtual networks in a SRv6 network, all the nodes (including the edge nodes and transit nodes) belonging to one particular virtual network MUST have a consistent view of the virtual network and performs consistent forwarding behavior to comply to the network topology and resource constraints. A node which participates in multiple virtual networks MUST be able to distinguish packets which belong to different virtual networks.

Taking the above into consideration, for a particular network node, multiple SRv6 LOCs SHOULD be allocated, each of which is associated with a paritcular virtual network topology, and MAY represent a subset of the network resources associated with the virtual network. The SRv6 SIDs of a particular virtual network SHOULD be allocated from the SID space using the virtual network specific LOC as prefix. These SRv6 SIDs can be used to represent virtual network specific local functions.

A group of SRv6 SIDs associated with the same virtual network can be used to construct the SR SID-lists (either strict or loose) for the service packet forwarding of a particular enhanced VPN. This group of SIDs MAY also represent the set of network resources which are reserved for a particular enhanced VPN, or a group of enhanced VPNs.

In data packet forwarding, the LOC part of SRv6 SID is used by transit nodes to identify the virtual network the packet belongs to, so that a virtual network specific next-hop can be determined. The LOC MAY also be used to indicate the set of local network resources on the transit nodes to be used for the forwarding of the received packet. The SRv6 segment endpoint nodes use the local SRv6 SID to identify the virtual network the packet belongs to, and the particular local function to peform on the received packet. The local SRv6 SID MAY also be used to identify the set of network resource to be used for executing the local function.

This mechanism requires to allocate additional SRv6 Locators and SIDs for each virtual network (network slice). As the number of virtual

networks increases, the number of Locators and SIDs would increase accordingly. It is expected that this mechanism is applicable to a network with a limited number of network slices.

4. Control Plane

The mechanism described in this document makes use of a centralized controller that collects the information about the network (configuration, state, routing databases, etc.) as well as the service information (traffic matrix, performance statistics, etc.). The controller is also responsible for the centralized computation and optimization of the virtual networks used for enhanced VPNs. The SR SIDs can be either explicitly provisioned by the controller, or dynamically allocated by network nodes then reported to the controller. The interaction between the controller and the network nodes can be based on PCEP [RFC5440], Netconf/YANG [RFC6241] [RFC7950] and BGP-LS [RFC7752]. In some scenarios, extensions to some of these protocols is needed , which are out of the scope of this document and will be specified in separate documents.

A distributed control plane can be used for the collection and distribution of the network topology and state information of the virtual networks among network nodes. Distributed route computation for services of a particular enhanced VPN is also needed. The IGP extensions for SR based enhanced VPN are specified in [I-D.dong-lsr-sr-enhanced-vpn].

5. Procedures

This section describes the procedures of provisioning enhanced VPN service based on segment routing with resource awareness.

According to the requirement of an enhanced VPN service, a centralized network controller calculates a subset of the physical network topology to support the enhanced VPN. Within this topology, the subset of network resources needed on each network element is also determined. The subset of network topology and the subset of network resources together constitute a virtual network (network slice). Depending on the service requirement, the network topology and resource can be dedicated for a particular enhanced VPN, or they can be shared among multiple enhanced VPNs.

Following the segment routing paradigm, the network topology and resource are represented in a per-segment manner, and are allocated with different node-SIDs and adj-SIDs. A group of the node-SIDs and adj-SIDs allocated for a paritcular virtual network will be used by network nodes and the network controller to build a SR virtual network topology, which is used as the logical underlay of the

enhanced VPN service. The extensions to IGP protocol to distribute the SIDs and the associated resources allocated for a virtual network are specified in [I-D.dong-lsr-sr-enhanced-vpn].

Suppose customer A requests for an enhanced VPN service from the network operator. The fundamental requirement is that service of customer A does not experience unexpected interference from other services in the same network, such as other customers' VPN services, or the non-VPN services in the network. The detailed requirements can be described with characteristics such as the following:

- Service topology: the service sites and the connectivity between them.
- Service bandwidth: the bandwidth requirement between service sites.
- Isolation: the level of isolation from other services in the network.
- Reliability: whether fast local repair or end-to-end protection is needed or not.
- Latency: the maximum latency for specific service between specific service sites.
- Visibility: the customer may want to have some form of visibility of the virtual network delivering the service.

5.1. Virtual Network Topology and Resource Computation

As described in section 4, a centralized network controller is responsible for the computation of a virtual network for the provisioning of enhanced VPNs. The controller collects the information of network connectivity, network resources, network performance and other relevant network states of the underlay network. This can be done using either IGP [RFC5305] [RFC3630] [RFC7471] [RFC7810] or BGP-LS [RFC7752] [RFC8571].

Based on the information collected from the underlay network, controller obtains the underlay network topology and the information about the allocated and available network resources. When an enhanced VPN service request is received from a tenant, the controller computes the subset of the network topology, along with set of the resources needed on each network element (e.g. links and nodes) of the topology to meet the tenant's service requirements, whilst maintaining the needs of the existing tenants that are using the same network. The subset of network topology and resource

constitute a virtual network, which will be used as the underlay of the requested enhanced VPN.

5.2. Network Resource and SID Allocation

According to the result of virtual network computation, network controller instructs the network devices involved in the virtual network to allocate the required network resources for the enhanced VPN. This can be done with either PCEP [RFC5440] or Netconf/YANG [RFC6241] [RFC7950] with necessary extensions. The network resources are allocated in a per-segment manner. In addition, a set of dedicated SIDs, e.g. node-SIDs and adj-SIDs are allocated to identify the virtual network and the network resources allocated on each network segment for the virtual network.

In forwarding plane, there are multiple ways of partitioning or reserving network resources for different virtual networks. For example, FlexE may be used to partition the link resource into different sub-channels to achieve hard isolation between each other. The candidate data plane technologies to support enhanced VPN can be found in [I-D.ietf-teas-enhanced-vpn]. The SR SIDs are used as a nework layer abstraction for various network resource partitioning or reservation mechanisms in forwarding plane.

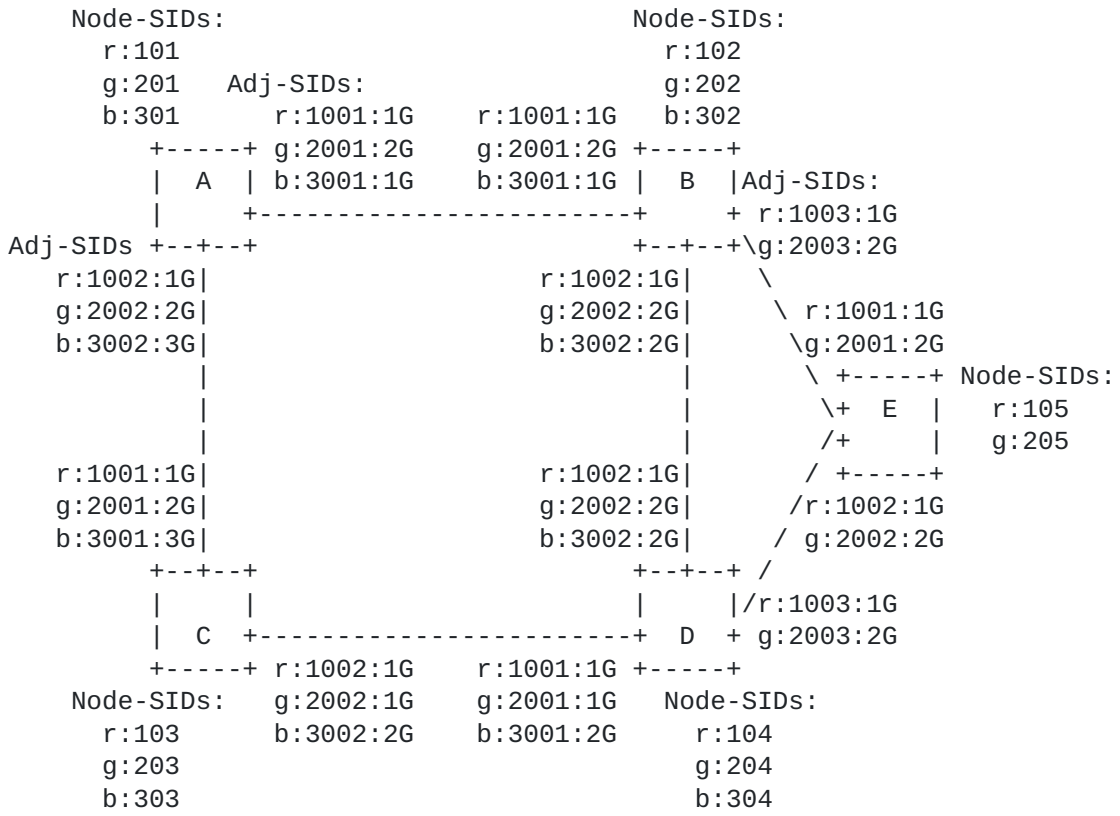

Figure 1. SIDs allocated to different virtual networks

Figure 1 shows a SR network to support enhanced VPN. Note that the format of the SIDs in this figure are for illustration, both SR-MPLS and SRv6 can be used as the data plane. In this example, three virtual networks: red (r) , green (g) and blue (b) are created for different enhanced VPNs. Both the red and green virtual networks consist of nodes A, B, C, D, and E with all their interconnecting links, whilst the blue virtual network only consists of nodes A, B, C and D with all their interconnecting links. Note that different virtual networks may have a set of shared nodes and links. On each link, a dedicated Adj-SID is allocated for each virtual network it participates in. Similarly, on each node, a dedicated Node-SID is allocated for each virtual network it participates in. The Adj-SIDs can be associated with different set of link resources (e.g. bandwidth) allocated to different virtual networks, so that the Adj-SIDs can be used to steer service traffic into different set of link resources in the forwarding plane. The Node-SIDs can be associated with the nodal resources allocated to different virtual network. In addition, the Node-SIDs can be used to build loose SR path within each virtual network, in this case it can be used by the transit

nodes to steer different service traffic into different set of local network resources in the forwarding plane.

In Figure 1, the notation x:nnnn:y means that in virtual network x, the adj-SID nnnn will steer the packet over a link which has bandwidth y reserved for that virtual network. Thus the note r:1002:1G in link C->D says that the red virtual network has a reserved bandwidth of 1Gb/s on link C->D, and will be used by packets arriving at node C with an adj-SID 1002 at the top of the label stack.

5.3. Construction of SR Virtual Networks

To make both the network controller and network nodes aware of the information of the virtual networks created in the network, each network node MUST advertise the virtual networks it participates, together with the set of SIDs and allocated resources into the network and then distributed to the controller. This can be achieve by means such as IGP extensions [I-D.dong-lsr-sr-enhanced-vpn], BGP-LS [RFC7752] with necessary extensions, NETCONF/YANG [RFC6241] [RFC7950].

Based on the collected information of network topology, network resource and SIDs information, both the controller and network nodes are able to construct the SR virtual network and generate the forwarding entries of each virtual network based on the node-SIDs and adj-SIDs allocated for each virtual network. Unlike classic segment routing in which network resources are always shared by all the services and tenants, different SR virtual networks can be associated with different set of resource allocated in the underlay network, so that they can be used to meet the service requirement of enhanced VPNs and provide the required isolation from other services in the same network.

Figure 2 shows the SR virtual networks created from the underlay network in Figure 1.

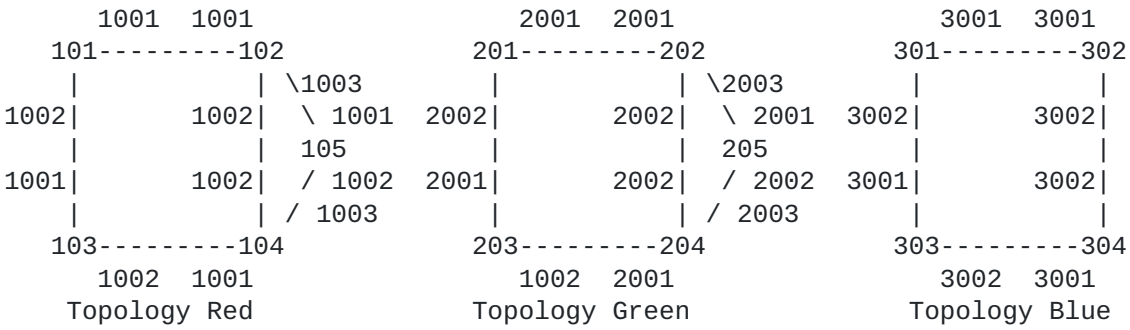

Figure 2. SR virtual networks using different groups of SIDs

In each SR virtual network, SR path is computed within the virtual network taking its network topology and resource as constraints. The SR path can be an explicit path instantiated using SR policy [I-D.ietf-spring-segment-routing-policy], in which the segment-list is built with the SIDs allocated to the virtual network. The service path can also be an IGP computed path associated with a particular node-SIDs of the virtual network. Different service paths in the same virtual network would share the network resources allocated to that virtual network.

For example, to create an explicit path A-B-D-E in the virtual network red in Figure 2, the SR segment list encapsulated in the service packet would be (1001, 1002, 1003). For the same explicit path A-B-D-E in virtual network green, the SR segment list would be (2001, 2002, 2003). In the case where we wish to construct a loose path A-D-E in virtual network green, the service packet SHOULD be encapsulated with the SR segment list (201, 204, 205). At node A, the packet can be sent towards D via either node B or C using the link and node resources allocated for virtual network green. At node D the packet is forwarded to E using the link and node resource allocated for virtual network green. Similarly, a packet to sent via loose path A-D-E in virtual network red would be encapsulated with segment list (101, 104, 105). In the case where an IGP computed path is good enough, the packet can be simply encapsulated with the node SID of egress node E in the corresponding virtual network.

5.4. VPN Service to SR Virtual Network Mapping

The enhanced VPN services can be provisioned using the customized SR virtual networks as the underlay network. Different enhanced VPNs can be provisioned in different SR virtual networks, each of which would use the network resources allocated to a particular virtual network, so that they will not interfere with each other. In another case, a set of enhanced VPNs can be provisioned in the same SR virtual network, in this case the network resources allocated to the

virtual network are shared by this set of enhanced VPNs, but will not be shared with other services in the network.

5.5. Virtual Network Visibility to Customer

The tenants of enhanced VPNs may request different granularity of visibility to the network which deliver the service. Depending on the requirement, the network can be exposed to the tenant either as a virtual network, or a set of computed paths with transit nodes, or simply the abstract connectivity between endpoints without any path information. The visibility can be delivered through different possible mechanisms, such as IGPs (e.g. IS-IS, OSPF) or BGP-LS. In addition, the network operator may want to restrict the visibility of the information it delivers to the tenant by either hiding the transit nodes between sites (and only delivering the endpoints connectivity) or by hiding portions of the transit nodes (summarizing the path into fewer nodes). Mechanisms such as BGP-LS allow the flexibility of the advertisement of aggregated virtual network information.

6. Benefits of the Proposed Mechanism

The proposed mechanism provides several key characteristics:

- Flexibility: Multiple customized virtual networks can be created in a shared network to meet different customer's connectivity and service requirement. Each customer is only aware of the topology and attributes of a particular virtual network, and provision services on the virtual network instead of the physical network. This provides an efficient mechanism to support network slicing.

- Isolation: Each virtual network can have independent SR path instantiation and computation. In addition, a virtual network can be associated with a set of network resources, which can avoid resource competition and performance interference from other services in the network. The proposed mechanism also allows resource sharing between different services in the same enhanced VPN, or between a set of enhanced VPNs which are provisioned in the same virtual network. This gives the operator and the enhanced VPN customer flexibility in network planning and service provisioning. The performance of critical services in a particular enhanced VPN can be further ensured using the mechanisms defined in [DetNet].

- Scalability: The proposed mechanism seeks to achieve a compromise between the state limitations of traditional end-to-end TE mechanism and the lack of resource awareness in basic segment routing. Following the segment routing paradigm, network

resources are allocated to network segments of the virtual networks, there is no per-flow state introduced in the network. Operator can choose the granularity of resource allocation to network segments. In network segments where resource is scarce such that the service requirement may not always be met, the SR approach can be used to allocate specific resources to the segment in a particular virtual network. By contrast, in other segment of the network where resource is considered plentiful, the resource may be shared between a number of virtual networks. The decision to do this is in the hands of the operator. Because of the segmented nature of the virtual network, resource aggregation is easier and more flexible than RSVP-TE based approach.

7. Service Assurance

In order to provide service assurance for enhanced VPNs, it is necessary to instrument the network at multiple levels. The network operator needs to ascertain that the underlay is operating correctly. A tenant needs to ascertain that their services are operating correctly. In principle these can use existing techniques. These are well known problems and solutions either exist or are in development to address them.

New work is needed to instrument the virtual networks that are created for the enhanced VPNs. Such instrumentation needs to operate without causing disruption to other services using the network. Given the sensitivity of some applications, care needs to be taken to ensure that the instrumentation itself does not cause disruption either to the service being instrumented or to other services. In case of failure or performance degradation of a service path in a particular virtual network, it is necessary that either local protection or end-to-end protection mechanism is used to switch to another path which could meet the service performance requirement and does not impact other services in the network.

8. IANA Considerations

This document makes no request of IANA.

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

9. Security Considerations

The normal security considerations of VPNs are applicable and it is assumed that industry best practise is applied to an enhanced VPN.

The security considerations of segment routing are applicable and it is assumed that these are applied to an enhanced VPN that uses SR based virtual networks.

Some applications of enhanced VPNs are sensitive to packet latency; the enhanced VPNs provisioned to carry their traffic have latency SLAs. By disrupting the latency of such traffic an attack can be directly targeted at the customer application, or can be targeted at the network operator by causing them to violate their SLA, triggering commercial consequences. Dynamic attacks of this sort are not something that networks have traditionally guarded against, and networking techniques need to be developed to defend against this type of attack. By rigorously policing ingress traffic and carefully provisioning the resources provided to critical services this type of attack can be prevented. However case needs to be taken when providing shared resources, and when the network needs to be reconfigured as part of ongoing maintenance or in response to a failure.

The details of the underlay MUST NOT be exposed to third parties, to prevent attacks aimed at exploiting a shared resource.

10. Contributors

The following people contributed to the content of this document.

11. Acknowledgements

The authors would like to thank Mach Chen, Zhenbin Li, Stefano Previdi, Charlie Perkins and Bruno Decraene for the discussion and suggestions to this document.

12. References

12.1. Normative References

[I-D.ietf-spring-segment-routing-mpls]
Bashandy, A., Filsfils, C., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing with MPLS data plane", draft-ietf-spring-segment-routing-mpls-22 (work in progress), May 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

12.2. Informative References

[BBF-SD406]
"BBF SD-406: End-to-End Network Slicing", 2016, <https://wiki.broadband-forum.org/display/BBF/SD-406+End-to-End+Network+Slicing>.

[DetNet] "DetNet WG", 2016, <https://datatracker.ietf.org/wg/detnet>.

[I-D.dong-lsr-sr-enhanced-vpn]
Dong, J. and S. Bryant, "IGP Extensions for Segment Routing based Enhanced VPN", draft-dong-lsr-sr-enhanced-vpn-01 (work in progress), October 2018.

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

[I-D.ietf-idr-bgpls-segment-routing-epe]
Previdi, S., Talaulikar, K., Filsfils, C., Patel, K., Ray, S., and J. Dong, "BGP-LS extensions for Segment Routing BGP Egress Peer Engineering", draft-ietf-idr-bgpls-segment-routing-epe-19 (work in progress), May 2019.

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

[I-D.ietf-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J., daniel.voyer@bell.ca, d., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-00 (work in progress), April 2019.

[I-D.ietf-teas-enhanced-vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Networks (VPN+) Service", draft-ietf-teas-enhanced-vpn-01 (work in progress), February 2019.

[NGMN-NS-Concept]
"NGMN NS Concept", 2016, <https://www.ngmn.org/fileadmin/user_upload/161010_NGMN_Network_Slicing_framework_v1.0.8.pdf>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[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>.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, DOI 10.17487/RFC3031, January 2001, <https://www.rfc-editor.org/info/rfc3031>.

[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>.

[RFC3630] Katz, D., Kompella, K., and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, DOI 10.17487/RFC3630, September 2003, <https://www.rfc-editor.org/info/rfc3630>.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, DOI 10.17487/RFC5305, October 2008, <https://www.rfc-editor.org/info/rfc5305>.

[RFC5439] Yasukawa, S., Farrel, A., and O. Komolafe, "An Analysis of Scaling Issues in MPLS-TE Core Networks", RFC 5439, DOI 10.17487/RFC5439, February 2009, <https://www.rfc-editor.org/info/rfc5439>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6790] Kompella, K., Drake, J., Amante, S., Henderickx, W., and L. Yong, "The Use of Entropy Labels in MPLS Forwarding", RFC 6790, DOI 10.17487/RFC6790, November 2012, <https://www.rfc-editor.org/info/rfc6790>.

[RFC7471] Giacalone, S., Ward, D., Drake, J., Atlas, A., and S. Previdi, "OSPF Traffic Engineering (TE) Metric Extensions", RFC 7471, DOI 10.17487/RFC7471, March 2015, <https://www.rfc-editor.org/info/rfc7471>.

[RFC7752] Gredler, H., Ed., Medved, J., Previdi, S., Farrel, A., and S. Ray, "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP", RFC 7752, DOI 10.17487/RFC7752, March 2016, <https://www.rfc-editor.org/info/rfc7752>.

[RFC7810] Previdi, S., Ed., Giacalone, S., Ward, D., Drake, J., and Q. Wu, "IS-IS Traffic Engineering (TE) Metric Extensions", RFC 7810, DOI 10.17487/RFC7810, May 2016, <https://www.rfc-editor.org/info/rfc7810>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8571] Ginsberg, L., Ed., Previdi, S., Wu, Q., Tantsura, J., and C. Filsfils, "BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions", RFC 8571, DOI 10.17487/RFC8571, March 2019, <https://www.rfc-editor.org/info/rfc8571>.

[TS23501] "3GPP TS23.501", 2016,
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>.

[TS28530] "3GPP TS28.530", 2016,
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3273>.

Authors' Addresses

Jie Dong
Huawei Technologies

Email: jie.dong@huawei.com

Stewart Bryant
Huawei Technologies

Email: stewart.bryant@gmail.com

Takuya Miyasaka
KDDI Corporation

Email: ta-miyasaka@kddi.com

Yongqing Zhu
China Telecom

Email: zhuyq@gsta.com

Fengwei Qin
China Mobile

Email: qinfengwei@chinamobile.com

Zhenqiang Li
China Mobile

Email: li_zhenqiang@hotmail.com