SPRING Working Group
Internet-Draft
Intended status: Informational
Expires: 18 June 2026

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

15 December 2025

Segment Routing based Network Resource Partition (NRP) for Enhanced VPN
draft-ietf-spring-sr-for-enhanced-vpn-10

Abstract

Enhanced VPNs aim to deliver VPN services with enhanced characteristics, such as guaranteed resources, latency, jitter, etc., so as to support customers requirements on connectivity services with these enhanced characteristics. Enhanced VPN requires integration between the overlay VPN connectivity and the characteristics provided by the underlay network. A Network Resource Partition (NRP) is a subset of the network resources and associated policies on each of a connected set of links in the underlay network. An NRP could be used as the underlay to support one or a group of enhanced VPN services.

Segment Routing (SR) leverages the source routing paradigm. A node steers a packet through an ordered list of instructions, called "segments". A segment is referred to by its Segment Identifier (SID). SIDs can represent topological or service based instructions. SIDs can further be associated with a set of network resources used for executing the instruction. Such SIDs are called resource-aware SIDs. A group of resource-aware SIDs may be used to build SR based NRPs, which provide customized network topology and resource attributes required by one or a group of enhanced VPN services.

This document describes an approach to build SR based NRPs using resource-aware SIDs. The SR based NRP can be used to deliver enhanced VPN services in SR networks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 18 June 2026.

Copyright Notice

Table of Contents

1. Introduction 3
2. Resource-Aware SIDs for NRPs 4
  2.1. SR-MPLS based NRPs 4
  2.2. SRv6 based NRPs 5
  2.3. NRP Identification 5
  2.4. Scalability Considerations 6
3. Procedures 6
  3.1. NRP Topology and Resource Planning 7
  3.2. NRP Network Resource and SID Allocation 7
  3.3. Construction of SR based NRPs 10
  3.4. Mapping Services to SR based NRP 13
  3.5. NRP Visibility to Customers 13
4. Characteristics of SR based NRPs 13
5. Service Assurance of NRPs 14
6. IANA Considerations 15
7. Operational Considerations 15
8. Security Considerations 15
9. Contributors 16
10. Acknowledgements 16
11. References 16

11.1. Normative References 16
11.2. Informative References 17
Authors' Addresses 20

1. Introduction

Enhanced VPNs aim to deliver VPN services with enhanced characteristics, such as low-latency guarantees, bounded jitter, or isolation from other services or customers etc., so as to support customers requirements on connectivity services with these enhanced characteristics. Enhanced VPN requires integration between the overlay VPN connectivity and the characteristics provided by the underlay network. [RFC9543] discusses the general framework, the components, and interfaces for requesting and operating network slices using IETF technologies. Network slice is considered as one target use case of enhanced VPNs.

[RFC9543] also introduces the concept of the Network Resource Partition (NRP), which is a subset of the buffer/queuing/scheduling resources and associated policies on each of a connected set of links in the underlay network. An NRP can be associated with a logical network topology to select or specify the set of links and nodes involved. [RFC9732] specifies the framework of NRP-based enhanced VPN, and describes the candidate component technologies in different network planes and network layers. An NRP could be used as the underlay to meet the requirements of one or a group of enhanced VPN services. In an underlay network, a number of NRPs can be created, each with a subset of network resources allocated on network nodes and links which are associated with a customized logical topology.

Segment Routing (SR) [RFC8402] specifies a mechanism to steer packets through an ordered list of segments. Segments are referred to by its Segment Identifiers (SIDs). With SR, explicit source routing can be achieved without introducing per-path state into the network. [I-D.ietf-spring-resource-aware-segments] extends SR by associating network resource attributes (e.g., bandwidth, processing or storage resources) to SIDs. These resource-aware SIDs retain their original functionality, with the additional semantics of identifying the set of network resources available for the packet processing action. On a particular segment, multiple resource-aware SIDs may be allocated, each of which represents a subset of network resources allocated in the network to meet the resource requirements of one or a group of services. A group of resource-aware SIDs may be used to build an SR based NRP, which provides customized network topology and resource attributes required by one or a group enhanced VPN services.

This document describes an approach to build SR based NRPs using resource-aware SIDs. Although the procedure is illustrated using SR over MPLS data plane (SR-MPLS) [RFC8660], this mechanism is equally applicable to SR over IPv6 data plane (SRv6)[RFC8754] [RFC8986].

2. Resource-Aware SIDs for NRPs

When SR is used as the data plane of NRPs in the network, it is necessary to compute and instantiate the SR paths with the topology and/or algorithm constraints of the NRP, and steer the traffic to only use the set of network resources allocated to the NRP.

Based on the resource-aware SIDs defined in [I-D.ietf-spring-resource-aware-segments], a group of resource-aware SIDs can represent the set of network resources allocated to the NRP on network nodes and links which participate in the NRP. These resource-aware SIDs can also identify the network topological or functional instructions associated with the NRP.

The resource-aware SIDs may be allocated either by a centralized network controller or by the network nodes. The control plane mechanisms for advertising the resource-aware SIDs and their attributes associated with NRPs can be based on [RFC4915], [RFC5120] and [RFC9350] with necessary extensions. This is further described in section 3.3.

2.1. SR-MPLS based NRPs

This section describes a mechanism of allocating resource-aware SIDs for SR-MPLS based NRPs.

For an IGP link, multiple resource-aware adj-SIDs are allocated, each of which is associated with an NRP that the link participates in, and represents a subset of the link resources (e.g., bandwidth, buffer and queuing resources) that are allocated to the NRP.

For an IGP prefix, multiple resource-aware prefix-SIDs are allocated, each of which is associated with an NRP that the attached node participates in. This means each resource-aware prefix-SID is associated with the topology and/or algorithm of the NRP, and is associated with a subset of network resources (e.g., bandwidth, buffer and queuing resources) allocated on network nodes and links participating in the NRP.

In the case of multi-domain NRPs, for an inter-domain link, multiple resource-aware BGP peering SIDs [RFC9086] are allocated, each of which is associated with an NRP which spans multiple domains, and represents a subset of resources allocated on the inter-domain link.

The group of resource-aware adj-SIDs and prefix SIDs associated with the same NRP represents the set of network resources of the NRP. These SIDs are called NRP-specific resource-aware SIDs.

2.2. SRv6 based NRPs

This section describes a mechanism of allocating resource-aware SRv6 Locators and resource-aware SRv6 SIDs for SRv6 based NRPs.

For one SRv6 node, multiple resource-aware SRv6 Locators can be allocated, each of which is associated with an NRP that the node participates in. This means each resource-aware Locator is associated with the topology and/or algorithm of the NRP, and is associated with a subset of network resources (e.g., bandwidth, buffer and queuing resources) allocated on the nodes and links participating in the NRP. These resource-aware SRv6 Locators are called NRP-specific resource-aware Locators.

The resource-aware SRv6 SIDs associated with an NRP are allocated from the SID space using the NRP-specific resource-aware Locator as the covering prefix. These SRv6 SIDs can be used to indicate SRv6 functions in an NRP, and can identify the set of resources used by network nodes for executing the function.

The group of resource-aware SRv6 Locators and SIDs of the same NRP represents the set of network resources of the NRP. They are called NRP-specific resource-aware Locators and SIDs.

2.3. NRP Identification

In a simple deployment case, each NRP can be mapped to a unique topology or algorithm. Then the NRPs can be distinguished by the topology ID or algorithm ID, and the resource-aware SIDs of different NRPs are associated with different <topology, algorithm> tuple in the control plane as described in [RFC8402]. In this case, the number of NRPs supported in a network relies on the number of topologies or algorithms supported in the network.

In a more complicated deployment case, multiple NRPs may be associated with the same <topology, algorithm> tuple, while each is allocated with a separate set of network resources. Then a new NRP Identifier (NRP ID) in the control plane is needed, The resource-aware SIDs of different NRPs are associated with different NRP IDs in the control plane.

In both cases, in the data plane, the resource-aware SIDs are used to distinguish packets to be processed in different NRPs, which means they are used to determine both the forwarding instructions and the set of network resources used for the packet processing action.

2.4. Scalability Considerations

As multiple NRPs can be created in a network, and each NRP is allocated with a group of resource-aware SIDs, the mechanism of SR based NRPs increases the number of SIDs and SRv6 Locators needed in a network. There may be some concerns, especially about the amount of SR-MPLS prefix-SIDs, which are allocated from the Segment Routing Global Block (SRGB), that the SRGB will be used up. As the number of NRP increases, the amount of network state will also increase accordingly. However, based on the SR paradigm, resource-aware SIDs and the associated network state are allocated and maintained per NRP, thus per-path network state can still be avoided in the SR network. In the control plane, the amount of information to be distributed in the distributed control protocols for different NRPs may become a concern. The scalability of resource-aware SID based NRPs are further analysed in [I-D.ietf-teas-nrp-scalability].

3. Procedures

This section describes possible procedures for creating SR based NRPs and the corresponding forwarding tables and entries. The approaches described in this section are not normative, but illustrate how the NRP-specific resource-aware SIDs could be used to build and operate NRPs in SR networks. Although it is illustrated using SR-MPLS, this mechanism is equally applicable to both SR-MPLS and SRv6.

Suppose an NRP is requested by some service. One of the requirements is that the service is allocated with a set of dedicated network bandwidth resource, so that it does not experience unexpected interference from other services in the same network. Other possible requirements specified by the customer may include the requirements on topology, latency, reliability, etc.

According to the service requirements, a centralized network controller calculates a subset of the underlay network topology to support the service. With this topology, the set of network bandwidth resource required on each network element is also determined. The subset of network topology and network resources are the two major characteristics of an NRP. Depending on the service requirements, the network topology and network resource of this NRP can be dedicated for an individual service, or can be shared by a group of services.

Based on the mechanisms described in section 2, a group of resource-aware SIDs are allocated for the NRP. With SR-MPLS, it is a group of prefix-SIDs and adj-SIDs which are allocated to identify the network nodes and links in the NRP, and also to identify the subset of network resources allocated on these network nodes and links for the NRP. As the resource-aware SIDs can be allocated either by a centralized network controller or by the network nodes, control plane protocols such as IGP (e.g., IS-IS or OSPF) and BGP-LS can be used to distribute the resource-aware SIDs, together with the associated network resource and topology attributes of an NRP to other nodes in the same NRP and also to the controller, so that both the network nodes and the controller can generate the NRP-specific forwarding table or forwarding entries based on the resource-aware SIDs of the NRP. The detailed control plane mechanisms and possible extensions are described in separate accompanying documents and are out of the scope of this document.

3.1. NRP Topology and Resource Planning

A centralized network controller can be responsible for the planning of an NRP to meet the received service request. The controller needs to collect the information on network connectivity, network resources, network performance and any other relevant network states from the underlay network. This can be done using either IGP TE extensions such as [RFC5305] [RFC3630] [RFC7471] [RFC8570], and/or BGP-LS [RFC7752] [RFC8571], or any other form of control plane signaling.

Based on the information collected from the underlay network, the controller obtains the underlay network topology and the information about the allocated and available network resources. When a service request is received, the controller determines the subset of the underlay network topology, and the subset of resources needed on each network segment (e.g., links and nodes) in the topology to meet the service requirements, whilst maintaining the needs of the existing services that are using the same network. The subset of the network topology and network resources will be used to constitute an NRP, which will be used as the virtual underlay network of the requested service.

3.2. NRP Network Resource and SID Allocation

According to the result of NRP planning, the network controller instructs the set of network nodes involved to join a specific NRP and allocate the required subset of network resources for the NRP. This may be done with Netconf/YANG [RFC6241] [RFC7950] or with any other control or management plane mechanism with necessary extensions. Thus, the controller not only allocates the resources to

the newly computed NRP, but also keeps track of the remaining available resources in order to cope with subsequent NRP requests.

On each network link involved in the NRP, a subset of network resources (e.g., link bandwidth) is allocated to the NRP. Such network resources can be dedicated for the processing of traffic in that NRP, and may not be used for traffic in other NRPs. Note it is also possible that a group of NRPs may share a set of network resources on some network elements. A group of resource-aware SIDs, such as prefix-SIDs and adj-SIDs are allocated to identify both the network instructions and the set of resources allocated for the NRP. Such group of resource-aware SIDs, e.g., prefix-SIDs and adj-SIDs are used for the data packet forwarding in the NRP.

In the underlying forwarding plane, there can be multiple ways of allocating a subset of network resources to an NRP. The candidate data plane technologies to support resource partitioning or reservation are described in [RFC9732]. The resource-aware SIDs are considered as abstracted data plane identifiers in the network layer, which can be used to represent various network resource partitioning or reservation mechanisms in the underlying forwarding plane.

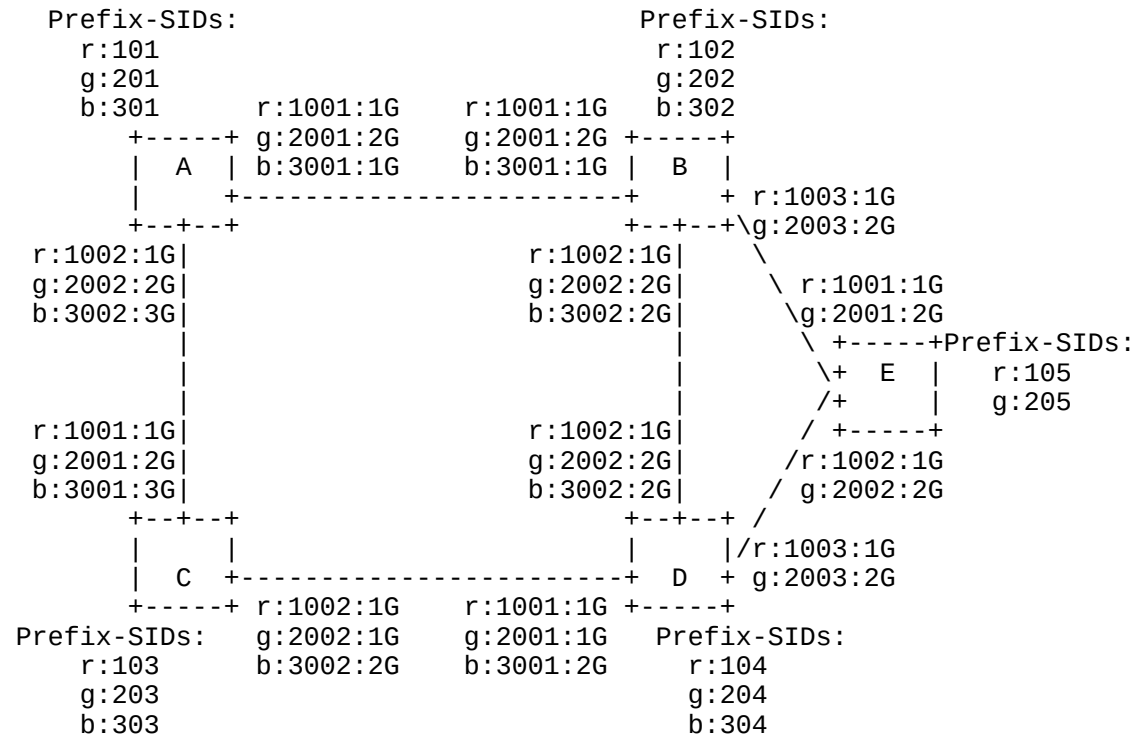

Figure 1. SID and resource allocation for multiple NRPs

Figure 1 shows an example of providing multiple NRPs in an SR network. The prefix-SIDs are labeled as such in the figure. All other SIDs in the figure are adj-SIDs. Note that the format of the SIDs in this figure is for illustration, both SR-MPLS and SRv6 can be used as the data plane. In this example, three NRPs: red (r) , green (g) and blue (b) are created to carry traffic of different customers or services. Both the red and green NRPs consist of nodes A, B, C, D, and E with all their interconnecting links, whilst the blue NRP only consists of nodes A, B, C and D with all their interconnecting links. Note that different NRPs may have a set of shared nodes and links, but with different set of resources allocated. On each node, a resource-aware prefix-SID is allocated for each NRP it participates in. And on each link, a resource-aware adj-SID is allocated for each NRP it participates in.

In Figure 1, the notation x:nnnn:y means that in NRP x, the adj-SID nnnn will steer the packet over a link which has bandwidth y reserved for that NRP. For example, r:1002:1G in link C->D says that the NRP red 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. Similarly, on each node, a resource-aware prefix-SID is allocated for each NRP it participates in. Each resource-aware adj-SID can be associated with a set of link resources (e.g., bandwidth) allocated to a specific NRP, so that different adj-SIDs can be used to steer traffic into different set of link resources for packet forwarding. A resource-aware prefix-SID in an NRP can be associated with the set of network resources allocated to this NRP on all involved network nodes and links. Thus, the prefix-SIDs can be used to build loose SR path within an NRP, and can be used by the transit nodes to steer traffic using the set of local network resources allocated to the NRP.

3.3. Construction of SR based NRPs

The network controller needs to obtain the information about all the NRPs in the network it oversees, including the resource-aware SIDs and the associated network resources and topology information. Based on this information, the controller can have a global view of the NRP topologies, the allocated network resources and the associated SIDs, so as to perform NRP-specific explicit path computation, taking both the topology and resource constraints of the NRPs into consideration, and use the resource-aware SIDs to build the SID list for the explicit SR path. The controller may also compute the shortest paths in the NRP based on the resource-aware prefix-SIDs.

The network nodes also need to obtain the information about the NRPs they participate in, including the resource-aware SIDs and the associated network resources and topology information. Based on the collected information, the network nodes which are the headend of a path can perform NRP-specific path computation, and build the SID list using the collected resource-aware adj-SIDs and prefix-SIDs. The network nodes also need to generate the forwarding entries for the resource-aware prefix-SIDs in each NRP they participates in, and associate these forwarding entries with the subset of local network resources (e.g., bandwidth on the outgoing interface) allocated to the corresponding NRP.

Thus, after receiving the network controller's instruction about network resource and SID allocation, each network node needs to advertise the identifier of the NRPs it participates in, the resource-aware SIDs allocated to the NRP, and the resource attributes (e.g., bandwidth) associated with the resource-aware SIDs in the network. Each resource-aware adj-SID is advertised with the set of associated link resources, and each resource-aware prefix-SID is advertised with the identifier of the associated NRP, as all the prefix-SIDs in an NRP are associated with the same set of network resources allocated to the NRP. Note that, as described in section 2.3, in the control plane, NRPs can be identified either using existing identifiers such as the MT-ID or Flex-Algo ID, or using a newly defined control plane NRP ID.

The control plane mechanisms which reuse the existing IDs (such as Multi-Topology ID or Algorithm ID) as the identifier of NRPs, and distribute the resource-aware SIDs with the associated topology and resource information may be based on the mechanisms described in [I-D.ietf-lsr-isis-sr-vtn-mt] and [I-D.zhu-lsr-isis-sr-vtn-flexalgo] respectively. The corresponding BGP-LS mechanisms which can be used to distribute both the intra-domain NRP information and the inter-domain NRP-specific link information to the controller may be based on the mechanisms described in [I-D.ietf-idr-bgpls-sr-vtn-mt] and [I-D.zhu-idr-bgpls-sr-vtn-flexalgo] respectively. Note that with these mechanisms, the number of NRPs supported relies on the number of topologies or algorithms supported in the network.

For network deployments where multiple NRPs can be associated with the same <topology, algorithm> tuple, while each NRP have different set of network resources, it allows to build a large number of NRPs with a relatively small number of topologies or algorithms. The corresponding control plane mechanisms are out of the scope of this document.

Figure 2 shows the three SR based NRPs created in the network in Figure 1.

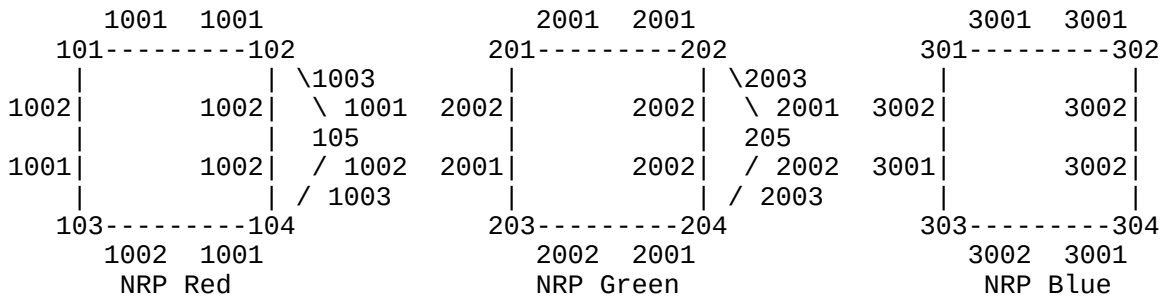

Figure 2. SR based NRPs with different groups of SIDs

For each SR based NRP, SR paths are computed within the NRP, taking the NRP topology and resources as constraints. The SR path can be an explicit path instantiated using SR Policy [RFC9256], in which the SID-list is built only with the resource-aware SIDs of the NRP. The SR path can also be an IGP computed path associated with a resource-aware prefix-SID or SRv6 End SID allocated by a node for the NRP, the IGP path computation is also based on the topology and/or algorithm constraints of the NRP. Different SR paths in the same NRP may use shared network resources when they use the same resource-aware SIDs allocated to the NRP, while SR paths in different NRPs always use different set of network resources even when they traverse the same network links or nodes. These NRP-specific SR paths need to be installed in the corresponding forwarding tables.

For example, to create an explicit path A-B-D-E in NRP red in Figure 2, the SR SID-list encapsulated in the service packet would be (1001, 1002, 1003). For the same explicit path A-B-D-E in NRP 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 NRP green, the packet should be encapsulated with the SR SID-list (201, 204, 205). At node A, the packet can be sent towards D via either node B or C using the network resources allocated by these nodes for NRP green. At node D, the packet is forwarded to E using the link and node resource allocated for NRP green. Similarly, a packet to be sent via loose path A-D-E in NRP red would be encapsulated with segment list (101, 104, 105). In the case where an IGP computed path can meet the service requirement, the packet can be simply encapsulated with the resource-aware prefix-SID of the egress node E in the corresponding NRP.

3.4. Mapping Services to SR based NRP

Network services can be provisioned using SR based NRPs as the virtual underlay networks. For example, different services may be provisioned in different SR based NRPs, each of which would use the subset of network resources allocated to the NRP, so that their data traffic will not interfere with each other in the network. In another case, a group of services which have similar characteristics and requirements may be provisioned in the same NRP, in this case the subset of network resources allocated to the NRP are only shared among this group of services, but will not be shared with services mapped to other NRPs in the network. The steering of service traffic to SR based NRPs can be based on local policy or the mechanisms as defined in [RFC9256].

3.5. NRP Visibility to Customers

NRPs can be used by network operators to organize and split their network infrastructure into different virtual underlay networks for different customers or services. Some customers may also request different granularity of visibility into the NRP which is used to deliver the service. Depending on the requirement and the network operator’s policy, NRPs may be exposed to the customer either as a virtual network with both the edge nodes and the intermediate nodes, as a set of paths with some of the transit nodes, or simply as a set of virtual connections between the endpoints without any transit node information. The visibility may be delivered through different mechanisms, such as IGPs (e.g., IS-IS, OSPF), BGP-LS or Netconf/YANG. On the other hand, a network operator may want to restrict the visibility of the underlay network information it delivers to the customer by either hiding the transit nodes between sites (and only delivering information about the endpoint connectivity), or by hiding some of the transit nodes (summarizing the path into fewer nodes). The information about NRPs which are not used by the customer should also be filtered. Mechanisms such as BGP-LS allow the flexibility of the advertisement of aggregated virtual network information and configurable filtering policies.

4. Characteristics of SR based NRPs

The mechanism described in this document provides several key characteristics:

* Customization: Different customized NRPs can be created in a shared physical network to meet different customers' connectivity and service requirement. The customers are only aware of the topology and attributes of their own NRPs, and services are provisioned only on the NRP instead of the physical network. This provides a practical mechanism to support network slicing [RFC9543].

* Resource isolation: The computation and instantiation of SR paths in one NRP can be independent from other NRPs or other services in the network. In addition, an NRP can be associated with a set of dedicated network resources, which can avoid resource competition and performance interference from services in other NRPs in the network. This mechanism also allows resource sharing between different service flows of the same customer, or between a group of services which are provisioned in the same NRP. This gives the operators and the customers the flexibility in network planning and service provisioning. In a NRP, the performance of critical services can be further ensured using other mechanisms, e.g., those as defined in [RFC8655].

* Scalability: The introduction of resource aware SIDs for different NRPs would increase the amount of SIDs and state in the network. While the increased network state is considered an inevitable price in meeting the requirements of some customers or services, the SR based NRP mechanism seeks to achieve a balance between the state limitations of traditional end-to-end TE mechanism and the lack of resource awareness in classic segment routing. Following the segment routing paradigm, network resources are allocated on network segments in a per NRP manner and represented as SIDs, this ensures that there is no per-path state introduced in the network. In addition, operators can choose the granularity of resource partition on different network segments. In network segments where resource is scarce and service requirement may not always be met, this approach can be used to allocate a set of resources to specific NRPs to avoid possible resource competition. By contrast, in other segment of the network where resource is considered plentiful, the resource may be shared between a number of NRPs. The decision to do this is in the hands of the operator.

5. Service Assurance of NRPs

In order to provide assurance for services provisioned in the SR based NRPs, it is necessary to instrument the network at multiple levels, e.g., in both the underlay network level and the NRP level. The operator or the customer may also monitor and measure the performance of the services carried by the NRPs. In principle these can be achieved using existing or in development techniques in IETF,

such as network telemetry [RFC9232]. The detailed mechanisms are out of the scope of this document.

In case of failure or service performance degradation in an NRP, it is necessary that some recovery mechanisms, e.g., local protection or end-to-end protection mechanism is used to switch the traffic to another path in the same NRP which could meet the service performance requirement. Care must be taken that the service or path recovery mechanism in one NRP does not impact other NRPs in the same physical network.

6. IANA Considerations

This document makes no request of IANA.

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

7. Operational Considerations

In data plane, each SR based NRP can be seen as a separate SR underlay network. A separate group of resource-aware SR SIDs need to be assigned to each SR based NRP by the operator, and distributed in the network using control protocols. As the number of SR based NRP increases, the amount of SIDs to be managed and distributed would increase proportionally. Taking the complexity in management plane and control plane into consideration, the number of SR based NRPs supported in a network will not be large. It is expected that the SR based NRP mechanism may be used for network scenarios where the required number of NRP is at the level of 10s to less than 100.

8. Security Considerations

The security considerations of segment routing [RFC8402] [RFC8754] and resource-aware SIDs [I-D.ietf-spring-resource-aware-segments] are applicable to this document.

The SR NRPs may be used carry services with specific SLA parameters. An attack can be directly targeted at the customer application by disrupting the SLA, and can be targeted at the network operator by causing them to violate the SLA, triggering commercial consequences. By rigorously policing the traffic at the ingress and carefully provisioning the network resources provided to the NRP, this type of attack can be prevented. However care needs to be taken when shared resources are provided between NRPs at some point in the network, and when the network needs to be reconfigured as part of ongoing maintenance or in response to a failure.

Considering the scalability of the SR NRP mechanism, the system may be destabilised by an attack or accident that causes a large number of NRPs to be configured. This can be mitigated by placing thresholds (for alarms or cut-off) in the configuration process.

Traffic within a network may be marked as belonging to a specific NRP and this makes it possible to carry out targeted attacks on traffic and to deduce customer-sensitive traffic patterns.

The details of the underlying network should not be exposed to third parties, some abstraction would be needed, this is also to prevent attacks aimed at exploiting a shared resource between NRPs.

9. Contributors

Stwart Bryant
Email: stewart.bryant@gmail.com

Francois Clad
Email: fclad@cisco.com

Zhenbin Li
Email: lizhenbin@huawei.com

Zhibo Hu
Email: huzhibo@huawei.com

10. Acknowledgements

The authors would like to thank Mach Chen, Stefano Previdi, Charlie Perkins, Bruno Decraene, Loa Andersson, Alexander Vainshtein, Joel Halpern, James Guichard, Adrian Farrel and Shunsuke Homma for the valuable discussion and suggestions to this document.

11. References

11.1. Normative References

[I-D.ietf-spring-resource-aware-segments]
Dong, J., Miyasaka, T., Zhu, Y., Qin, F., and Z. Li, "Introducing Resource Awareness to SR Segments", Work in Progress, Internet-Draft, draft-ietf-spring-resource-aware-segments-16, 20 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-resource-aware-segments-16>.

[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>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

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

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

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

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

[RFC9732] Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for NRP-Based Enhanced Virtual Private Networks", RFC 9732, DOI 10.17487/RFC9732, March 2025, <https://www.rfc-editor.org/info/rfc9732>.

11.2. Informative References

[I-D.ietf-idr-bgpls-sr-vtn-mt] Xie, C., Li, C., Dong, J., and Z. Li, "Applicability of Border Gateway Protocol - Link State (BGP-LS) with Multi-Topology (MT) for Segment Routing based Network Resource Partitions (NRPs)", Work in Progress, Internet-Draft, draft-ietf-idr-bgpls-sr-vtn-mt-14, 16 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-bgpls-sr-vtn-mt-14>.

[I-D.ietf-lsr-isis-sr-vtn-mt]
Xie, C., Ma, C., Dong, J., and Z. Li, "Applicability of IS-IS Multi-Topology (MT) for Segment Routing based Network Resource Partition (NRP)", Work in Progress, Internet-Draft, draft-ietf-lsr-isis-sr-vtn-mt-11, 13 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lsr-isis-sr-vtn-mt-11>.

[I-D.ietf-teas-nrp-scalability]
Dong, J., Li, Z., Gong, L., Yang, G., and G. S. Mishra, "Scalability Considerations for Network Resource Partition", Work in Progress, Internet-Draft, draft-ietf-teas-nrp-scalability-08, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-nrp-scalability-08>.

[I-D.zhu-idr-bgpls-sr-vtn-flexalgo]
Zhu, Y., Dong, J., and Z. Hu, "BGP-LS with Flex-Algo for Segment Routing based Virtual Transport Networks", Work in Progress, Internet-Draft, draft-zhu-idr-bgpls-sr-vtn-flexalgo-01, 22 February 2021, <https://datatracker.ietf.org/doc/html/draft-zhu-idr-bgpls-sr-vtn-flexalgo-01>.

[I-D.zhu-lsr-isis-sr-vtn-flexalgo]
Zhu, Y., Dong, J., and Z. Hu, "Using Flex-Algo for Segment Routing (SR) based Network Resource Partition (NRP)", Work in Progress, Internet-Draft, draft-zhu-lsr-isis-sr-vtn-flexalgo-08, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-zhu-lsr-isis-sr-vtn-flexalgo-08>.

[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>.

[RFC4915] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915, DOI 10.17487/RFC4915, June 2007, <https://www.rfc-editor.org/info/rfc4915>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

[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>.

[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>.

[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>.

[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>.

[RFC8570] Ginsberg, L., Ed., Previdi, S., Ed., Giacalone, S., Ward, D., Drake, J., and Q. Wu, "IS-IS Traffic Engineering (TE) Metric Extensions", RFC 8570, DOI 10.17487/RFC8570, March 2019, <https://www.rfc-editor.org/info/rfc8570>.

[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>.

[RFC9086] Previdi, S., Talaulikar, K., Ed., Filsfils, C., Patel, K., Ray, S., and J. Dong, "Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing BGP Egress Peer Engineering", RFC 9086, DOI 10.17487/RFC9086, August 2021, <https://www.rfc-editor.org/info/rfc9086>.

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

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

[RFC9350] Psenak, P., Ed., Hegde, S., Filsfils, C., Talaulikar, K., and A. Gulko, "IGP Flexible Algorithm", RFC 9350, DOI 10.17487/RFC9350, February 2023, <https://www.rfc-editor.org/info/rfc9350>.

Authors' Addresses

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

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

Yongqing Zhu
China Telecom
Email: zhuyq8@chinatelecom.cn

Fengwei Qin
China Mobile
Email: qinfengwei@chinamobile.com

Zhenqiang Li
China Mobile
Email: li_zhenqiang@hotmail.com