LSR Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 25, 2020

J. Dong
Z. Hu
Z. Li
Huawei Technologies
X. Tang
R. Pang
China Unicom
L. JooHeon
LG U+
S. Bryant
Futurewei Technologies

June 23, 2020

# IGP Extensions for Segment Routing based Enhanced VPN
# draft-dong-lsr-sr-enhanced-vpn-04

## Abstract

Enhanced VPN (VPN+) is an enhancement to VPN services to support the needs of new applications, particularly including the applications that are associated with 5G services. These applications require enhanced isolation and have more stringent performance requirements than that can be provided with traditional overlay VPNs. An enhanced VPN may be used for 5G transport network slicing, and will also be of use in more generic scenarios. To meet the requirement of enhanced VPN services, a number of Virtual Transport Networks (VTN) need to be created, each with a subset of the underlay network topology and a set of network resources allocated to meet the requirement of a specific VPN+ service, or a group of VPN+ services.

This document specifies the IGP mechanisms with necessary extensions to build a set of Segment Routing (SR) based VTNs. The VTNs could be used as the underlay of enhanced VPN service. The proposed mechanism is applicable to both Segment Routing with MPLS data plane (SR-MPLS) and segment routing with IPv6 data plane (SRv6).

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

## Status of This Memo

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

## Copyright Notice



## Table of Contents

## 1. Introduction

Enhanced VPN (VPN+) is an enhancement to VPN services to support the needs of new applications, particularly including the applications that are associated with 5G services. These applications require enhanced isolation and have more stringent performance requirements than that can be provided with traditional overlay VPNs. These properties cannot be met with pure overlay networks, as they require integration between the underlay and the overlay networks. [I-D.ietf-teas-enhanced-vpn] specifies the framework of enhanced VPN and describes the candidate component technologies in different network planes and layers. An enhanced VPN can be used for 5G transport network slicing, and will also be of use in more generic scenarios.

To meet the requirement of enhanced VPN services, a number of virtual transport networks (VTN) need to be created, each with a subset of the underlay network topology and a set of network resources allocated to meet the requirement of a specific VPN+ service or a group of VPN+ services.

[I-D.dong-spring-sr-for-enhanced-vpn] specifies how segment routing (SR) [RFC8402] can be used to build virtual transport networks (VTNs) with the required network topology and network resources to support enhanced VPN services. With segment routing based data plane, Segment Identifiers (SIDs) can be used to represent the topology and the set of network resources allocated by network nodes to a virtual network. The SIDs of each VTN and the associated topology and resource attributes need to be distributed using a control plane.

[I-D.dong-teas-enhanced-vpn-vtn-scalability] analyzes the scalability requirements and the control plane and data plane scalability considerations of enhanced VPN, more specificially, the scalability of the VTN as the underlay. In order to support the increasing number of VTNs in the network, one proposed approach is to separate the topology and resource attributes of the VTN in control plane, so that the advertisement and processing of each type of attribute could be decoupled. This also allows flexible combination of topology and resource attribute to build customized VTNs. For example, a group of VTNs can share the same network topology, also a group VTNs can share the same set of network resource on particular network segments.

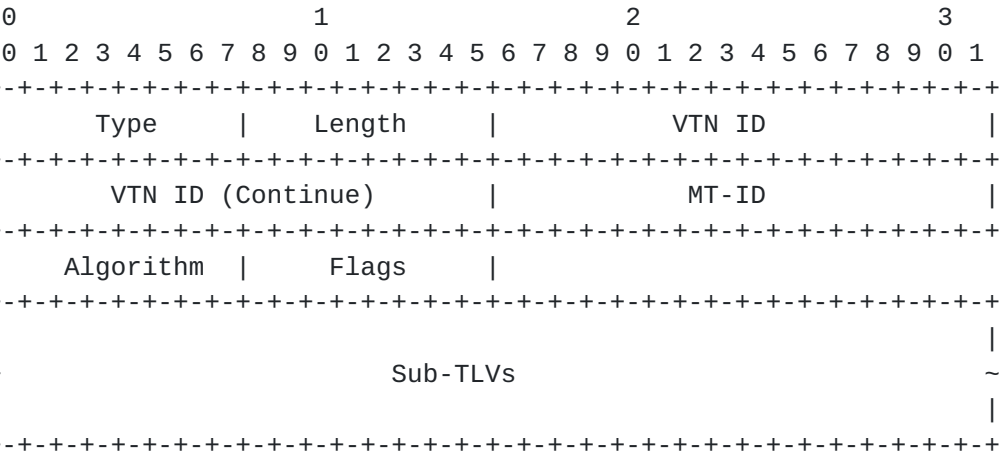
This document specifies the IGP control plane mechanism with necessary extensions to build a set of SR based VTNs. The proposed mechanism is applicable to both segment routing with MPLS data plane (SR-MPLS) and segment routing with IPv6 data plane (SRv6).

In general this approach applies to both IS-IS and OSPF, while the specific protocol extensions and encodings are different. In the current version of this document, the required IS-IS extensions are described. The required OSPF extensions will be described in a future version or a separate document.

## 2. VTN Definition Advertisement

According to [I-D.ietf-teas-enhanced-vpn], a virtual transport network (VTN) has a customized network topology and a set of dedicated or shared network resources. Thus a VTN can be defined as the combination of a set of network attributes, which include the topology attribute and other attributes, such as network resources. IS-IS Virtual Transport Network Definition (VTND) sub-TLV is used to advertise the definition of a virtual transport network. It is a sub-TLV of the IS-IS Router-Capability TLV 242 as defined in [RFC7981].

The format of IS-IS VTND sub-TLV is as below:




Where:

- Type: TBD
- Length: The length of the value field of the sub-TLV. It is variable dependent on the included sub-TLVs.
- VTN ID: A global significant 32-bit identifier which is used to identify a virtual transport network.
- MT-ID: 16-bit field which indicates the multi-topology identifier as defined in [RFC5120]. The first 4-bit are set to zero.

- Algorithm: 8-bit identifier which indicates the algorithm which applies to this virtual transport network. It can be either a normal algorithm [RFC8402] or a Flex-Algorithm [I-D.ietf-lsr-flex-algo].

- Flags: 8-bit flags. Currently all the flags are reserved for future use. They SHOULD be set to zero on transmission and MUST be ignored on receipt.

- Sub-TLVs: optional sub-TLVs to specify the additional attributes of a virtual transport network. Currently no sub-TLV is defined in this document.

The VTND Sub-TLV MAY be advertised in an LSP of any number. A node SHOULD advertise the VTND sub-TLV for each VTN it participates in, but it MUST NOT advertise more than one VTND Sub-TLV for a given VTN ID.

## 3. Advertisement of VTN Topology Attribute

This section describes the mechanisms used to advertise the topology attribute of SR based VTNs. Basically the topology attribute of a VTN can be determined by the MT-ID and the algorithm included in the VTN definition. In practice, it could be described using two approaches.

The first approach is to use Multi-Topology Routing (MTR) [RFC4915] [RFC5120] with the segment routing extensions to advertise the topologies of the SR based VTNs. Different algorithms MAY be used to further specify the computation algorithm or the metric type used for path computation within a topology.

The second approach is to use Flex-Algo [I-D.ietf-lsr-flex-algo] to describe the topological constraints of different SR based VTNs on a shared network topology.

### 3.1. MTR based Topology Advertisement

Multi-Topology Routing (MTR) has been defined in [RFC4915] and [RFC5120] to create different network topologies in one network. It also has the capability of specifying customized attributes for each topology. The traditional use cases of multi-topology are to maintain separate topologies for unicast and multicast services, or to create different topologies for IPv4 and IPv6 in a network. There are some limitations when MTR is used with native IP forwarding, the considerations about MT based IP forwarding are described in [RFC5120].

MTR can be used with SR-MPLS data plane. [RFC8667] specifies the IS-IS extensions to support SR-MPLS data plane, in which the Prefix-SID sub-TLVs can be carried in IS-IS TLV 235 (MT IP Reachability) and TLV 237 (MT IPv6 IP Reachability), and the Adj-SID sub-TLVs can be carried in IS-IS TLV 222 (MT-ISN) and TLV 223 (MT IS Neighbor Attribute).

MTR can also be used with SRv6 data plane. [I-D.ietf-lsr-isis-srv6-extensions] specifies the IS-IS extensions to support SRv6 data plane, in which the MT-ID is included in the SRv6 Locator TLV. The SRv6 End SIDs inherit the topology/algorithm from the parent locator. In addition, the SRv6 End.X SID sub-TLVs can be carried in the IS-IS TLV 222 (MT-ISN) and TLV 223 (MT IS Neighbor Attribute).

These IGP extensions for SR-MPLS and SRv6 can be used to advertise and build the topology of SR based VTNs.

On each topology, the algorithm MAY be used to further specify the computation algorithm or the metric type used for path computation within the topology.

### 3.2. Flex-Algo based Topology Advertisement

[I-D.ietf-lsr-flex-algo] specifies the mechanisms to provide distributed computation of constraint-based paths, and how the SR-MPLS prefix-SIDs and SRv6 locators can be used to steer packets along the constraint-based paths.

The Flex-Algo definition can be used to describe the topological constraints for path computation on a network topology. According to the network nodes' participation of a Flex-Algo, and the rules of including or excluding specific Administrative Groups (colors) and Shared Risk Link Groups (SRLGs), the topology of a VTN can be determined using the associated Flex-Algo on a default topology.

With the mechanisms defined in[RFC8667] [I-D.ietf-lsr-flex-algo], prefix-SID advertisement can be associated with a specific topology and a specific algorithm, which can be a Flex-Algo. This allows the nodes to use the prefix-SID to steer traffic along distributed computed paths according to the identified Flex-Algo in the associated topology.

[I-D.ietf-lsr-isis-srv6-extensions] specifies the IS-IS extensions to support SRv6 data plane, in which the SRv6 locators advertisement can be associated with a specific topology and a specific algorithm, which can be a Flex-Algo. With the mechanism defined in [I-D.ietf-lsr-flex-algo], The SRv6 locator can be used to steer

traffic along distributed computed paths according to the identified Flex-Algo in the associated topology. In addition, topology/ algorithm specific SRv6 End SID and End.X SID can be used to enforce traffic over the LFA computed backup path.

In some cases, multiple Flex-Algos MAY be defined to describe the topological constraints on a shared network topology.

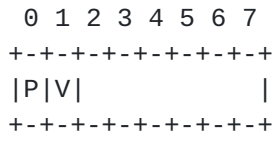
## 4. Advertisement of VTN Resource Attribute

This section specifies the mechanism to advertise the network resource attributes associated with the VTNs. The mechanism of advertising the link level resources is described. The mechanism of advertising node resource are for further study.

On a Layer 3 interface, a subset of the link resource can be allocated to a specific VTN. This subset of link resource can be represented as a virtual layer-2 member link of the Layer 3 interface. If the Layer 3 interface is a Layer 2 link bundle, it is possible that the subset of link resource is provided by a physical Layer 2 member link.

[RFC8668] describes the IS-IS extensions to advertise the link attributes of the Layer 2 member links which comprise an Layer 3 interface. Such mechanism can be extended to advertise the attributes of each physical or virtual member links, and its associated VTNs.

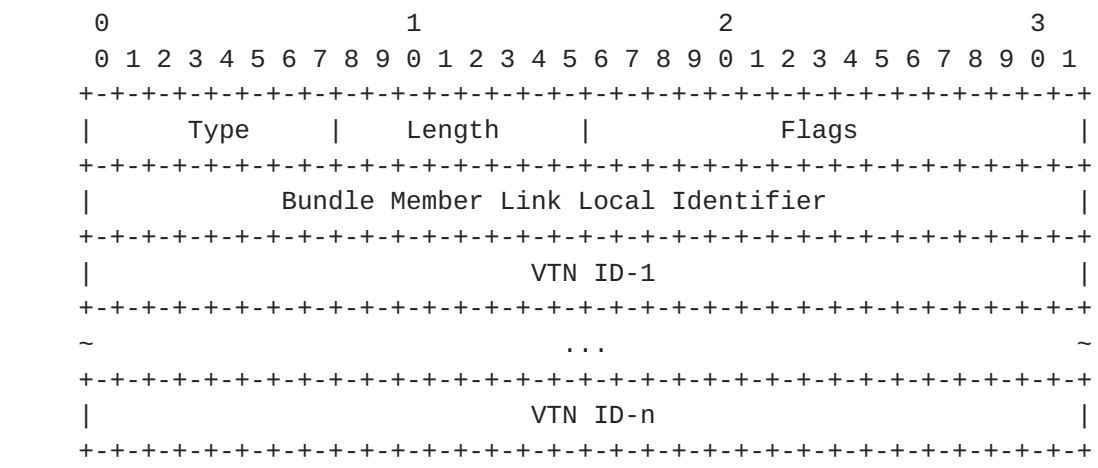
A new flag "V" (Virtual) is defined in the flag field of the Parent L3 Neighbor Descriptor in the L2 Bundle Member Attributes TLV (25).




V flag: When the V flag is set, it indicates the member links under the Parent L3 link are virtual member links. When the V flag is clear, it indicates the member links are physical member links.

A new VTN-ID sub-TLV is carried under the L2 Bundle member attribute to describe the mapping relationship between the VTNs and the virtual or physical member links of a Layer 3 interface. As one or more VTNs may use the same set of link resource on a specific network segment, these VTN IDs will be advertised under the same virtual or physical member link.

The format of the VTN-ID Sub-TLV is as below:




Where:

- Type: TBD
- Length: The length of the value field of the sub-TLV. It is variable dependent on the number of VTN IDs included.
- Flags: 16 bit flags. All the bits are reserved for future use, which SHOULD be set to 0 on transmission and MUST be ignored on receipt.
- Bundle Member Link Local Identifier: A 32-bit local identifier of a physical or virtual member link.
- VTN IDs: One or more 32-bit identifier to identify the VTNs this member link belongs to.

Each physical or virtual member link of an L3 link MAY be associated with a different VTN. Thus multiple VTN-ID sub-TLVs will be carried in the L2 Bundle Attribute Descriptors of the L2 Bundle Member Attributes TLV.

The TE attributes of each physical or virtual bundle member link, such as the bandwidth and the adj-SIDs, can be advertised using the mechanism as defined in [RFC8668].

## 5. Advertisement of VTN specific Data Plane Identifiers

In order to steer packet of different VTNs to the constraint-based paths computed using the corresponding topology and set of network resources, information which could be used to infer or identify the VTN a packet belongs to SHOULD be carried in the packet. If each VTN is associated with an independent network topology or Flex-Algo, the topology or Flex-Algo specific SIDs or Locators could be used as the

identifier of the VTN in data plane. If multiple VTNs share the same topology or Flex-Algo, some additional data plane identifiers would be needed to identify different VTNs.

This section describes the mechanisms to advertise the VTN identifiers with different data plane encapsulations.

## 5.1. Advertisement of VTN-specific MPLS SIDs

With SR-MPLS data plane, the VTN identification information is implicitly carried in the SR SIDs of the corresponding VTN. Each node SHOULD allocate VTN-specific Prefix-SIDs for each VTN it participates in. Similarly, VTN-specific Adj-SIDs MAY be allocated for each link which participates in the VTN.

A new VTN-specific prefix-SID sub-TLV is defined to advertise the prefix-SID and its associated VTN. This sub-TLV may be advertised as a sub-TLV of the following TLVs:

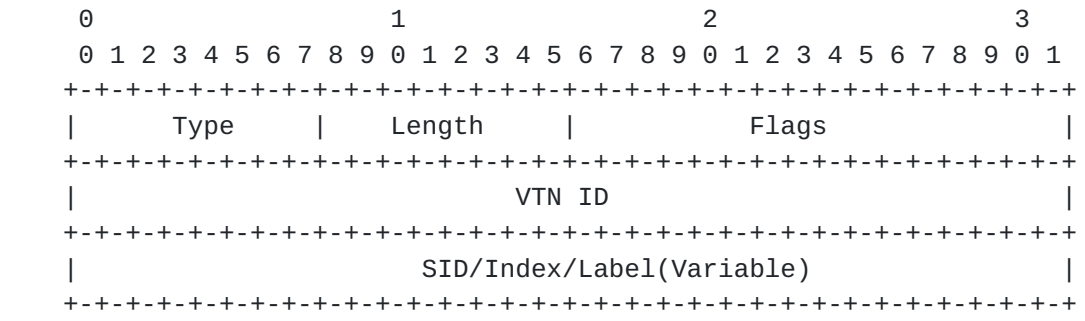
TLV-135 (Extended IPv4 Reachability) defined in [RFC5305].

TLV-235 (MT IP Reachability) defined in [RFC5120].

TLV-236 (IPv6 IP Reachability) defined in [RFC5308].

TLV-237 (MT IPv6 IP Reachability) defined in [RFC5120].

The format of the sub-TLV is shown as below:




Where:

- Type: TBD
- Length: The length of the value field of the sub-TLV. It is variable dependent on the length of the SID/Index/Label field.
- Flags: 16-bit flags. The high-order 8 bits are the same as in the Adj-SID sub-TLV defined in [RFC8667]. The lower-order 8 bits are

reserved for future use, which SHOULD be set to 0 on transmission and MUST be ignored on receipt.

- VTN ID: A 32-bit local identifier to identify the VTN this prefix-SID associates with.

- SID/Index/Label: The same as defined in [RFC8667].

One or more of VTN-specific Prefix-SID sub-TLVs MAY be carried in the Multi-topology IP Reachability TLVs (TLV 235 or TLV 236), the MT-ID of the TLV SHOULD be the same as the MT-ID in the definition of these VTNs.

A new VTN-specific Adj-SID sub-TLV is defined to advertise the adj-SID and its associated VTN. This sub-TLV may be advertised as a sub-TLV of the following TLVs:

TLV-22 (Extended IS reachability) [RFC5305]

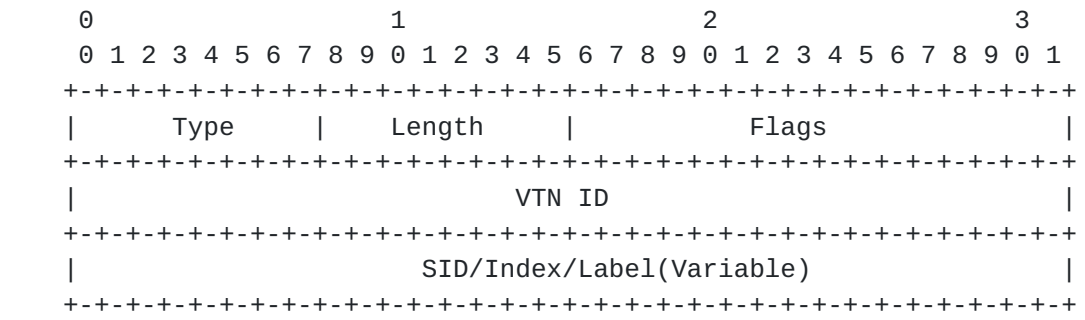
TLV-23 (IS Neighbor Attribute) [RFC5311]

TLV-141 (Inter-AS Reachability Information) [RFC5316]

TLV-222 (MT ISN)[RFC5120]

TLV-223 (MT IS Neighbor Attribute) [RFC5311]

The format of the sub-TLV is shown as below:




Where:

- Type: TBD

- Length: The length of the value field of the sub-TLV. It is variable dependent on the length of the SID/Index/Label field.

- Flags: 16-bit flags. The high-order 8 bits are the same as in the Adj-SID sub-TLV defined in [RFC8667]. The lower-order 8 bits are

reserved for future use, which SHOULD be set to 0 on transmission and MUST be ignored on receipt.

- VTN ID: A 32-bit local identifier to identify the VTN this Adj-SID associates with.

- SID/Index/Label: The same as defined in [RFC8667].

One or more VTN-specific Adj-SID sub-TLV MAY be carried in the Multi-topology ISN or Multi-topology IS Attribute TLVs (TLV 222 or TLV 223), the MT-ID of the TLV SHOULD be the same as the MT-ID in the VTN definition.

### 5.2. Advertisement of VTN-specific SRv6 Locators

With SRv6 data plane, the VTN identification information can be implicitly or explicitly carried in the SRv6 Locator of the corresponding VTN. Network nodes SHOULD allocate VTN-specific Locators for each VTN it participates in. The VTN-specific Locators are used as the covering prefix of VTN-specific SRv6 End SIDs and End.X SIDs.

Each VTN-specific SRv6 Locator MAY be advertised in a separate TLV. If multiple VTNs share the same topology, the topology/algorithm specific Locator is the covering prefix of a group of VTN-specific Locators. Then the advertisement of VTN-specific locators MAY be optimized to reduce the amount of information exchanged in the control plane. More details about this mechanism will be provided in a future version of this document.

### 5.3. Advertisement of Dedicated Data Plane VTN IDs

As the number of VTNs increases, some data plane optimization is needed to reduce the amount of SR SIDs and Locators allocated for VTNs. As described in [I-D.dong-teas-enhanced-vpn-vtn-scalability], one approach is to decouple the identifiers used for topology based forwarding and the identifiers used for the VTN-specific processing executed on packets of different VTNs. Thus a dedicated VTN ID could be encapsulated in the packet. One possible encapsulation is proposed in [I-D.dong-6man-enhanced-vpn-vtn-id].

In that case, the VTN ID encapsulated in data plane can have the same value as the VTN ID in control plane, so that the overhead of advertising the mapping between the VTN ID in control plane and the corresponding data plane identifiers could be saved.

## 6. Security Considerations

This document introduces no additional security vulnerabilities to IS-IS and OSPF.

The mechanism proposed in this document is subject to the same vulnerabilities as any other protocol that relies on IGPs.

## 7. IANA Considerations

IANA is requested to assign a new code point in the "sub-TLVs for TLV 242" registry.

Type: TBD1
Description: Virtual Transport Network Definition

IANA is requested to assign two new code points in the "sub-TLVs for TLVs 22, 23, 25, 141, 222, and 223" registry.

Type: TBD2
Description: Virtual Transport Network Identifiers

Type: TBD3
Description: VTN-specific Adj-SID

IANA is requested to assign a new code point in the "Sub-TLVs for TLVs 135,235,236 and 237 registry".

Type: TBD4
Description: VTN-specific Prefix-SID

## 8. Acknowledgments

The authors would like to thank Mach Chen and Dean Cheng for their review and discussion of this document.

## 9. References

### 9.1. Normative References

[I-D.dong-spring-sr-for-enhanced-vpn]
Dong, J., Bryant, S., Miyasaka, T., Zhu, Y., Qin, F., and Z. Li, "Segment Routing for Resource Guaranteed Virtual Networks", draft-dong-spring-sr-for-enhanced-vpn-08 (work in progress), June 2020.

[I-D.ietf-lsr-flex-algo]
Psenak, P., Hegde, S., Filsfils, C., Talaulikar, K., and A. Gulko, "IGP Flexible Algorithm", draft-ietf-lsr-flex-algo-07 (work in progress), April 2020.

[I-D.ietf-lsr-isis-srv6-extensions]
Psenak, P., Filsfils, C., Bashandy, A., Decraene, B., and Z. Hu, "IS-IS Extension to Support Segment Routing over IPv6 Dataplane", draft-ietf-lsr-isis-srv6-extensions-08 (work in progress), April 2020.

[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>.

[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>.

[RFC7981] Ginsberg, L., Previdi, S., and M. Chen, "IS-IS Extensions for Advertising Router Information", RFC 7981, DOI 10.17487/RFC7981, October 2016, <https://www.rfc-editor.org/info/rfc7981>.

[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>.

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

[RFC8668] Ginsberg, L., Ed., Bashandy, A., Filsfils, C., Nanduri, M., and E. Aries, "Advertising Layer 2 Bundle Member Link Attributes in IS-IS", RFC 8668, DOI 10.17487/RFC8668, December 2019, <https://www.rfc-editor.org/info/rfc8668>.

### 9.2. Informative References

[I-D.dong-6man-enhanced-vpn-vtn-id]
Dong, J. and Z. Li, "Carrying Virtual Transport Network (VTN) Identifier in IPv6 Extensison Header for Enhanced VPN", draft-dong-6man-enhanced-vpn-vtn-id-00 (work in progress), February 2020.

[I-D.dong-teas-enhanced-vpn-vtn-scalability]
Dong, J., Li, Z., and F. Qin, "Virtual Transport Network (VTN) Scalability Considerations for Enhanced VPN", draft-dong-teas-enhanced-vpn-vtn-scalability-00 (work in progress), February 2020.

[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+) Services", draft-ietf-teas-enhanced-vpn-05 (work in progress), February 2020.

## Authors' Addresses

Jie Dong
Huawei Technologies

Email: jie.dong@huawei.com

Zhibo Hu
Huawei Technologies

Email: huzhibo@huawei.com

Zhenbin Li
Huawei Technologies

Email: lizhenbin@huawei.com

Xiongyan Tang
China Unicom

Email: tangxy@chinaunicom.cn

Ran Pang
China Unicom

Email: pangran@chinaunicom.cn

Lee JooHeon
LG U+

Email: playgame@lguplus.co.kr

Stewart Bryant
Futurewei Technologies

Email: stewart.bryant@gmail.com