SPRING Working Group
Internet-Draft
Intended status: Informational
Expires: October 2, 2021

C. Li
Z. Li
H. Yang
Huawei Technologies

March 31, 2021

IPv6-based Cloud-Oriented Networking (CON)
draft-li-rtgwg-ipv6-based-con-01

Abstract

This document describes the scenarios, requirements and technologies for IPv6-based Cloud-oriented Networking.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

With the development of cloud computing, increasing services have been migrated from enterprises to cloud data centers. Compared with interconnections between branches and headquarters, new connections between enterprise sites to cloud data centers and inter-cloud are added, which bring new requirements and challenges for existing networks.

When enterprises have workloads & applications & data split among different data centers, especially for those enterprises with multiple sites that are already interconnected by VPNs (e.g., MPLS L2VPN/L3VPN), challenges are introduced. [I-D.ietf-rtgwg-net2cloud-problem-statement] describes the problems that enterprises face today when interconnecting their branch offices with dynamic workloads in third party data centers (a.k.a. Cloud DCs).

SD-WAN is a flexible WAN architecture that enables flexible network-to-cloud and inter-clouds connections. It supports to use alternative paths like internet or 4G / 5G connection instead of expensive MPLS leased lines to exchange data between sites and clouds. However, when a WAN path travels multiple MPLS domains, the configurations are complicated due to multiple services touch points need to be configured. Therefore, it is hard to support end-to-end path programming in IPv4/MPLS based SD-WAN.

When using VXLAN in SD-WAN, only the overlay path or anchor points can be specified while the underlay forwarding path can not be specified. Therefore, strict TE requirements like deterministic delay, specified path forwarding can not be satisfied.

In order to resolve these challenges, this document propose IPv6-based Cloud-Oriented Networking (CON). In addition, it describes the challenges for existing networks when clouds and networks are converged, requirements that IPv6-based CON should satisfy, and the solutions in IPv6-based CON that satisfy the requirements.

IPv6-based CON supports quick and flexible connections between sites and clouds and inter-clouds, it also supports end-to-end path programming, which can be used for many use cases, such as strict path traffic engineering, deterministic delay forwarding, and service function chaining, to provide better network services for cloud-network and inter-cloud interconnections.

2. Terminology

This document makes use of the terms defined in [RFC8754] and [RFC8200], and the reader is assumed to be familiar with that terminology. This document introduces the following terms:

POP: Point of Presence

CON: Cloud-Oriented Networking.

EC: Edge Computing.

EDC: Edge Data center

RDC: Regional Data Center

CDC: Core Data Center

2.1. Requirements Language

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Problem Statement

As development of cloud, many clouds have been deployed, such as Private cloud, Public Cloud, and Hybrid Cloud. The cloud services can be provided by a third party, such as an OTT (Over-The-Top) content provider, and it can be provided by a network operator as well. Furthermore, cloud can be deployed not only in IT data centers but also CT data centers.

With the development and successful application of cloud native design in the IT field and Network Functions Virtualization (NFV) technologies, virtualization and cloudification have gradually matured and evolved to provide a new level of productivity, offering a new approach to telecom network construction. Building cloud-based telecom networks (also known as telco clouds) becomes a new way of telecom network construction.

In order to support low latency communication, the request should be responded at the near cloud data center, therefore edge computing data center (a.k.a Edge Cloud) is introduced. Telecommunication services and third-party OTT services can be deployed in the edge cloud.

As the deployment of clouds, the traffic pattern in the network has changed significantly, which results in new challenges for existing networks.

3.1. Underlay

From the aspect of underlay, cloud services requires the network to provide quick and flexible connection.

The typical topology of telco cloud is shown in figure 1.

```
                 +++++++        +++++++            ++++++
                 | EDC |        | RDC |            | CDC|
                 +++++++        +++++++            ++++++
                    |   *********  |   ************  |
                    |   *       *  |   *          *  |
       OLT/CSG/CPE---PE--* Metro *--PE--* Backbone *--PE--IGW---Internet
                        *       *      *          *
                        *********      ************
```

Figure 1.Typical topology of telco cloud

The edge cloud is deployed in edge data center (EDC) in the access network usually, so that the servers in the edge cloud can respond to the delay-sensitive requests rapidly, like 5G URLLC traffic. The traffic is not delay-sensitive can be responded in regional cloud DC, which is located in the metro or core network. Most cloud services may be deployed in the core cloud DC considering reducing the cost, which is far from the end user. Like, the UPF may locate in the regional cloud DC or Core cloud DC, so that it can support more users.

The traffic from end users to cloud servers are forwarded along with different paths due to the different locations of the end users and the cloud servers.

In addition, when deploying new services, for instance, deploying a leased line from an enterprise site to a cloud data center, it will take probably weeks in the current IPv4/MPLS carrier network. Because the VPN configuration is needed to be done at multiple PE nodes if the leased line travels multiple domains (when using Option A between domains). Also, the cloud operator needs to negotiate with network operators if the cloud services and the network services are provided by different operators. For example, thousands of chain stores such as grocery stores or super markets are needed to connect to their enterprise VPNs, and they may use the cloud services. However, in IPv4/MPLS network, it may take weeks to establish a new VPN connection from a site to headquarter or cloud tenant networks.

Furthermore, different traffic of different enterprise/tenant/users are treated differently in clouds, and they MAY be forwarded along with different service function chains (SFC). However, it is hard to support SFC in IPv4 or MPLS based network in carrier's networks or data center networks. Normally, to support SFC, the traffic steering policies are configured at multiple nodes along the SFC path, which is complicated.

3.2. Overlay

In order to provide quick and flexible cloud connection, overlay connection is provided by cloud providers, especially the OTT cloud providers.

SD-WAN is a typical fabric for DCI connection between clouds and sites, which provides a cheaper and smarter WAN connection. Many SD-WAN providers builds their own WAN backbone network by connecting their POP GWs to provide better SLA assurance for tenants. The typical topology of SD-WAN with POP GWs is shown in figure 2.

```
  Site CPE1--POP GW1 --------------------------POP GW2---Site CPE2
                |                                  |
                |          SD-WAN Backbone         |
                |                                  |
    Cloud1---POP GW3---------------------------POP GW4--Cloud2
```

Figure 2. Typical topology of SD-WAN

Currently, the traffic from the CPE to POP GW is forwarded through the shortest forwarding path over the Internet, or an MPLS tunnel.

In addition, traffic from POP GW to another POP GW can be forwarded along with the MPLS tunnel that is a leased line, or over the internet, depending on the forwarding policies.

When the traffic is forwarded over the internet, it can be forwarded over a VXLAN tunnel. However, when using VXLAN, only the overlay connection is provided to enterprises/tenants, while the underlay forwarding path can not be specified and programmed. Therefore the SLA requirements can not be guaranteed when the traffic is forwarded overlay.

4. IPv6-based Cloud-Oriented Networking

This document describes a networking architecture called IPv6-based Cloud-Oriented Networking (CON). IPv6-based CON is an IPv6-based networking which provide quick, flexible connection to support dynamic site to cloud, and inter-cloud connections. Also, it supports end-to-end underlay forwarding path programming, so that services like strict path TE and SFC can be supported better.

The following section describes the requirements in IPv6-based CON, and the related solutions that meet the requirements.

4.1. Requirements

This section describes the overall requirements which need to be fulfilled by IPv6-based Cloud-Oriented Networking.

4.1.1. Quick Connection

Enterprise sites can locate at any location around the world, they need to connect to the clouds or other sites in any time, from any where. Also, enterprises may have some Virtual Private Clouds (VPC) in different clouds, they need to connect to each other in real time as well. The servers may locate in different cloud data centers or enterprise sites, which provide services for employees or other users. Therefore quick connection is required in IPv6-based CON.

4.1.2. Hybrid Network Connection

The enterprise VPN traffic can be forwarded around the world, which may travel heterogeneous networks, such as IPv4, MPLS and IPv6.

Typically, when a SD-WAN network connects multiple sites and clouds, it may cover hybrid networks. For example, the sub-path from the CPE to POP WG could be an IPv4 sub-path without any resource guarantee. The sub-path between POP GWs could be an MPLS LSP with resource reservation.

Therefore, connection over hybrid networks MUST be supported in IPv6-based CON.

4.1.3. Path Programming

When the enterprise VPN traffic is forwarded among sites or clouds, it may be forwarded along different paths. Each path has different performance such as different bandwidth, delay, etc. For instance, path A is the shortest path from site 1 to cloud 1, which has the lowest delay, while the path B can provide more bandwidth than path A. Therefore, the delay-sensitive traffic like PC gaming traffic SHOULD be forwarded along with path A, and the traffic that is delay-insensitive but requiring large bandwidth SHOULD be forwarded along with path B.

In order to meet the different SLA requirements, IPv6-based CON MUST support path programming.

4.1.4. Resource Assurance

In RSVP-TE MPLS, resources like bandwidth can be reserved for an LSP. When the traffic is forwarded along the LSP, the bandwidth can be guaranteed, which makes sure that the traffic will not be affected by other traffic. In order to provide SLA guaranteed services, IPv6-based CON MUST support Resource Assurance.

Network slicing is an approach to provide separate and independent end-to-end logical network over the physical network infrastructure. Each Network Slicing has its own resources, which can meet the specific SLA requirements. In order to provide SLA guaranteed services, IPv6-based CON MUST support network slicing.

4.1.5. Deterministic Delay

Delay-sensitive traffic has the strict requirements of network delay. Especially, when the servers moved to clouds instead of locating locally within the enterprise site, the long physical distance of packet forwarding path will introduce larger delay. In the traditional network, the shortest forwarding path is calculated based on the metric, and the metric is usually associated to the physical hops instead of latency. However, minimum delay forwarding is required for delay-sensitive traffic, like real-time video broadcast and video meeting.

Therefore, IPv6-based CON MUST have the capability to support path computing based on delay. Also, it MUST be able to provide deterministic delay forwarding.

4.1.6. Service Function Chaining

Service Function Chaining [RFC7665] is a mechanism to provide different value-added services (VAS) for packets.

A service function chain defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification [RFC7665].

An example of an abstract service function is "a firewall". Typically, different tenant's traffic in cloud data center will traverse different services function chain containing Firewall, DPI or other VAS.

Therefore, IPv6-based CON MUST have the capability to support SFC.

4.1.7. Performance Measurement

Many OAM mechanisms are used to support network operation. Performance Measurement (PM) is one of the most important part of OAM. With PM, the real-time QoS of the forwarding path, like delay, packet loss ratio and throughput, can be measured.

PM can be implemented in one of three ways: active, passive, or hybrid [RFC7799], differing in whether OAM packets need to be proactively sent.

On-path telemetry [I-D.song-opsawg-ifit-framework] is an hybrid mode OAM/PM mechanism, which provides better accuracy than active PM. Therefore, on-path Performance Measurement MUST be supported in IPv6-based CON.

4.1.8. Reliability

In Cloud-Network Interconnection scenarios, the enterprise traffic is forwarded over the WAN paths. The traffic can be sensitive to delay or packet losing, so high reliability is required in these scenarios. Therefore, protection of node and links MUST be supported in IPv6-based CON. Furthermore, redundancy transmission SHOULD be supported.

4.1.9. Security

As mentioned above, the enterprise traffic is forwarded over the WAN paths in IPv6-based CON. The security of the traffic MUST be ensured.

Also, in SD-WAN scenarios, customers are most concerned about security.

Therefore, IPv6-based CON MUST support secure connection, and MUST provide security assurance for the traffic in transmission.

4.1.10. Forwarding Efficiency

Tenants/Customers rent the physical or logical WAN links/paths from network operators for building they cloud-network interconnection enterprise network, so the forwarding efficiency is important for the WAN path tenant.

Path Maximum Transmission Unit indicates the maximum size of a packet that it can be forwarded along a path. Setting an appropriate PMTU for packets can avoid fragmentation or dropping, so that the forwarding efficiency can be raised.

Also, the overhead of packets MUST be added very carefully since it affects the forwarding efficiency directly. Especially, when many SIDs are inserted in an SRv6 packet, the overhead of the SID list is too large. [I-D.srcompdt-spring-compression-requirement] describes the requirements of SRv6 compression.

Therefore, the IPv6-based CON MUST support PMTU probing and configuration. In addition, it MUST support SRv6 compression.

4.1.11. Application-Aware Networking

Network operators are typically unaware of which applications are traversing their networks, which is because the network layer is decoupled from application layer. Adding application knowledge to the network layer enables finer granularity requirements of applications to be specified to the network operator. As IPv6 is being widely deployed, the programmability provided by IPv6 encapsulations can be augmented by conveying application information.

In IPv6-based CON, many types of applications' traffic is exchanged between sites and clouds. They have various requirements of QoS, and should be treated differently. In order to provide finer granularity traffic engineering to reduce the cost of WAN services, application-aware networking SHOULD be supported in IPv6-based CON.

4.2. Solutions

This section describes the candidate solutions that meet the requirements in IPv6-based CON.

4.2.1. VPN

VPN is a basic and essential services for cloud-networks interconnections.

SRv6 supports VPN by encoding the VPN information into the VPN SID [I-D.ietf-spring-srv6-network-programming].

Based on IPv6, SRv6 VPN can be established across multiple domains. It avoids configuring VPN services at each boundary nodes at each domain like the way in IPv4/MPLS networks (Option A). Deploying VPN based on SRv6 can shorten the duration significantly.

Also, L2VPN and L3VPN can be supported uniformly based on EVPN control plane [I-D.ietf-bess-srv6-services]. Therefore, combining the SRv6 data plane and EVPN control plane, the VPN can be deployed in an easy and flexible way in IPv6-based CON.

4.2.2. Path Programming

Based on SRv6, the traffic forwarding path can be programmed at the ingress of the SRv6 domain, so that the traffic from sites to clouds or inter-cloud can be forwarded through the specific underlay path.

For instance, in SD-WAN scenarios, the POP GW can choose a specific underlay forwarding path in WAN by choosing a binding SID [I-D.dukes-spring-sr-for-sdwan]. If the CPE supports SRv6, a controller can convey the programmed path information to the CPE via BGP SRv6 policy [I-D.ietf-idr-segment-routing-te-policy] or PCEP SRv6 policy [I-D.ietf-pce-segment-routing-policy-cp].

If the WAN connection travels multiple domains, the WAN path can be connected by multiple tunnels, such as VXLAN, GRE tunnel. [I-D.dunbar-sr-sdwan-over-hybrid-networks] describes how to associated the tunnels.

In order to shorten the delay, a CPE or PE can choose the nearest server in a specific cloud, and forward the packets through programmed paths.

4.2.3. Service Function Chaining

SFC is required in IPv6-based CON since different tenants subscribe different value-added services.

[I-D.ietf-spring-sr-service-programming] defines the mechanism to support SFC in SRv6. Each service function (SF) can be represented as an SRv6 SID if it supports SRv6. If the SF is SRv6-unaware device, then proxy SID is used. By programming service SIDs into the SRH, the SFC can be supported in SRv6.

Thanks to IPv6 reachability, SRv6 supports to program the end-to-end forwarding path from the carrier network to the inside the cloud data center, even to multiple clouds.

If NSH-based SFC has been deployed, a transition solution should be considered, and [I-D.ietf-spring-nsh-sr] describes a NSH and SR integration SFC solution.

4.2.4. IPv6 based Network Slicing

The tenant traffic MUST be isolated in WAN to avoid affecting by other internet traffic.

A framework, Enhanced VPN (VPN+), to form an enhanced connectivity services between customer sites is defined as per

[I-D.ietf-teas-enhanced-vpn]. Typically, VPN+ will be used to form the underpinning of network slicing. It also defines Virtual Transport Network (VTN). A VTN is a virtual underlay network that connects customer edge points with the capability of providing the isolation and performance characteristics required by an enhanced VPN customer. A VTN usually has a customized topology and a set of dedicated or shared network resources [I-D.ietf-teas-enhanced-vpn].

A VTN-ID option in IPv6 HBH header is defined in [I-D.dong-6man-enhanced-vpn-vtn-id] to identify the Virtual Transport Network (VTN) the packet belongs to. A VTN can be used as the underlay for one or a group of VPNs to provide enhanced VPN (VPN+) services.

By using VTN-ID, an end-to-end IPv6 network slicing is identified in transport network. Tenant traffic in WAN can be forwarded in the VTN with guaranteed resource.

4.2.5. IPv6-based On-path Measurement

The extension of supporting Alternate Marking Method [RFC8321] in IPv6 is defined in [I-D.ietf-6man-ipv6-alt-mark]. It describes how the Alternate Marking Method to be used as the hybrid performance measurement tool in an IPv6 domain by defining a new Extension Header Option.

Alternate Marking Method is a hybrid on-path performance measurement method, and the metadata of each node can be collected by the collector to compute the performance of the path.

IOAM is another on-path measurement method. [I-D.ietf-ippm-ioam-ipv6-options] defines a new IPv6 option, called IOAM option to support carrying IOAM metadata in the IPv6 data packet. However, carrying all the metadata in the data packet will bring challenges for hardware processing. For instance, long-length metadata may cause recircle in processing. Therefore, [I-D.ietf-ippm-ioam-direct-export] defines a direct export option in IOAM, which enables the nodes to export the metadata to collector directly. Furthermore,[I-D.song-opsawg-ifit-framework] outlines a high-level framework to provide an operational environment that utilizes existing and emerging on-path telemetry techniques to enable the collection and correlation of performance information from the network.

4.2.6. Reliability

4.2.6.1. Local Protection

Local protection mechanisms like Fast Reroute (FRR) provide 50 ms protection on nodes for traffic.

Regarding link failures, TI-LFA [I-D.ietf-rtgwg-segment-routing-ti-lfa] provides a fast reroute mechanism by sending the traffic to an expected post-convergence paths from the point of local repair.

Regarding the middle endpoint node failures, [I-D.hu-spring-segment-routing-proxy-forwarding] defines a mechanism for fast reroute protection against the failure of a SR-TE path. It can provide fast reroute protection for an adjacency segment, a node segment and a binding segment of the path. Also, [I-D.chen-rtgwg-srv6-midpoint-protection] defines midpoint protection, which enables the direct neighbor of the failed endpoint to perform the function of the endpoint, replace the IPv6 destination address to the next endpoint, and choose the next hop based on the new destination address.

Regarding the egress node failures, [I-D.ietf-rtgwg-srv6-egress-protection] defines a local protection solution using the mirror SID.

4.2.6.2. End-to-End Protection

End-to-End Protection is also required in IPv6-based CON. Normally, host-standby nodes are deployed for supporting traffic switching from the failed node to the alternative node. In order to detect the failure, End-to-end BFD is required. Once the BFD session is failed, the traffic can be steered into a disjoint forwarding path, and the traffic will be forwarded to the host-standby node.

4.2.6.3. Redundancy Protection

In order to avoid losing packets, [I-D.geng-spring-sr-redundancy-protection] defines a redundancy transmission solution.

The document defines two types of segment including Redundancy Segment and Merging Segment to empower the Segment Routing with the capability of redundancy protection.

4.2.7. Security

As per [I-D.li-spring-srv6-security-consideration], SRv6 inherits potential security vulnerabilities from Source Routing and IPv6, but it does not introduce new critical security threats.

Regarding a limited domain, SPRING architecture [RFC8402] defines clear trusted domain boundaries so that source-routing information is only available within the trusted domain and never exposed to the outside of the domain. It is expected that, by default, explicit routing is only used within the boundaries of the administered domain. Therefore, the data plane does not expose any source-routing information when a packet leaves the trusted domain. The traffic is filtered at the domain boundaries [RFC8402].

However, it has been noted that the AH and ESP are not directly applicable in order to reduce the vulnerabilities of SRv6 due to the presence of mutable fields in the SRH [I-D.li-spring-srv6-security-consideration]. In order to resolve this problem, [RFC8754] defines a mechanism to carry HMAC TLV in the SRH to verify the integrity of packets including the SRH fields.

Regarding end-to-end security protection across multiple domains, an end-to-end IPSec tunnel is suggested to be deployed.

In typical SD-WAN scenarios, the IPSec tunnel should be used between the CPE and POP GW.

4.2.8. IPv6 Forwarding Efficiency

4.2.8.1. PMTU

The host may discover the PMTU by Path MTU Discovery (PMTUD) [RFC8201] or other means. But the ingress node still needs to examine the packet size to drop too large packets to avoid malicious packets or error packets attack. Also, the packet size may exceed the PMTU because of the new encapsulation of SR-MPLS or SRv6 at the ingress. In order to check whether the packet size exceeds the PMTU or not, the ingress node need to know the Path MTU associated to the forwarding path.

However, the path maximum transmission unit (MTU) information for SR path is not available since the SR does not require signaling. [I-D.ietf-idr-bgp-ls-link-mtu] proposes a BGP-LS extensions to collect the link MTU of the links in the networks. [I-D.ietf-idr-sr-policy-path-mtu] and [I-D.li-pce-pcep-pmtu] defines extensions to distribute path MTU information within BGP and PCEP SR policies, respectively. In this way, the controller can compute the appropriate PMTU for an SR path.

4.2.8.2. SRv6 Compression

The overhead of SRv6 encapsulation brings challenges for hardware processing and transmission. [I-D.srcompdt-spring-compression-requirement] describes the requirements of SRv6 compression.

G-SRv6 is proposed in [I-D.cl-spring-generalized-srv6-np], which supports to encode multiple types of SIDs in SRH. This SRH is called Generalized SRH [I-D.lc-6man-generalized-srh] while the SID is called Generalized SID.

G-SRv6 supports to encode the compressed SIDs in the SRH to reduce the size of SRv6 SID list in SRH [I-D.cl-spring-generalized-srv6-for-cmpr]. A COC (Continuation of Compression) flavor is defined to indicate the continuation of SRv6 compressed SIDs in the SID list.

4.2.9. Application-aware IPv6 Networking

Application-aware Networking (APN) is proposed by [I-D.li-apn-framework], where application characteristic information such as application identification and its network performance requirements is carried in the packet encapsulation in order to facilitate service provisioning, perform application-level traffic steering and network resource adjustment.

Application-aware IPv6 Networking (APN6) framework makes use of IPv6 encapsulation in order to convey the application-aware information along with the data packet to the network so to facilitate the service deployment and SLA guarantee. [I-D.li-6man-app-aware-ipv6-network] defines the encodings of the application characteristic information, for the APN6 framework, that can be exchanged between an application and the network infrastructure through IPv6 extension headers.

5. IANA Considerations

TBD

6. Security Considerations

TBD

7. Contributors

TBD

8. Acknowledgements

9. References

9.1. Normative References

[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>.

[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>.

[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>.

[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>.

9.2. Informative References

[I-D.ietf-rtgwg-net2cloud-problem-statement]
Dunbar, L., Malis, A., Jacquenet, C., and M. Toy, "Dynamic Networks to Hybrid Cloud DCs Problem Statement", draft-ietf-rtgwg-net2cloud-problem-statement-11 (work in progress), July 2020.

[I-D.ietf-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-28 (work in progress), December 2020.

[I-D.ietf-bess-srv6-services]
Dawra, G., Filsfils, C., Talaulikar, K., Raszuk, R., Decraene, B., Zhuang, S., and J. Rabadan, "SRv6 BGP based Overlay services", draft-ietf-bess-srv6-services-05 (work in progress), November 2020.

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

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[I-D.dukes-spring-sr-for-sdwan]
Dukes, D., Filsfils, C., Dawra, G., Xu, X., Voyer, D., Camarillo, P., Clad, F., and S. Salsano, "SR For SDWAN: VPN with Underlay SLA", draft-dukes-spring-sr-for-sdwan-02 (work in progress), June 2019.

[I-D.dunbar-sr-sdwan-over-hybrid-networks]
Dunbar, L. and M. Toy, "Segment routing for SDWAN paths over hybrid networks", draft-dunbar-sr-sdwan-over-hybrid-networks-06 (work in progress), November 2019.

[I-D.ietf-idr-segment-routing-te-policy]
Previdi, S., Filsfils, C., Talaulikar, K., Mattes, P., Rosen, E., Jain, D., and S. Lin, "Advertising Segment Routing Policies in BGP", draft-ietf-idr-segment-routing-te-policy-11 (work in progress), November 2020.

[I-D.ietf-pce-segment-routing-policy-cp]
Koldychev, M., Sivabalan, S., Barth, C., Peng, S., and H. Bidgoli, "PCEP extension to support Segment Routing Policy Candidate Paths", draft-ietf-pce-segment-routing-policy-cp-02 (work in progress), January 2021.

[I-D.ietf-spring-sr-service-programming]
Clad, F., Xu, X., Filsfils, C., daniel.bernier@bell.ca, d., Li, C., Decraene, B., Ma, S., Yadlapalli, C., Henderickx, W., and S. Salsano, "Service Programming with Segment Routing", draft-ietf-spring-sr-service-programming-03 (work in progress), September 2020.

[I-D.ietf-spring-nsh-sr]
Guichard, J. and J. Tantsura, "Integration of Network Service Header (NSH) and Segment Routing for Service Function Chaining (SFC)", draft-ietf-spring-nsh-sr-04 (work in progress), December 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+) Service", draft-ietf-teas-enhanced-vpn-06 (work in progress), July 2020.

[I-D.dong-6man-enhanced-vpn-vtn-id]
Dong, J., Li, Z., Xie, C., and C. Ma, "Carrying Virtual Transport Network Identifier in IPv6 Extension Header", draft-dong-6man-enhanced-vpn-vtn-id-02 (work in progress), November 2020.

[RFC8321] Fioccola, G., Ed., Capello, A., Cociglio, M., Castaldelli, L., Chen, M., Zheng, L., Mirsky, G., and T. Mizrahi, "Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8321, DOI 10.17487/RFC8321, January 2018, <https://www.rfc-editor.org/info/rfc8321>.

[I-D.ietf-6man-ipv6-alt-mark]
Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate Marking Method", draft-ietf-6man-ipv6-alt-mark-02 (work in progress), October 2020.

[I-D.ietf-ippm-ioam-ipv6-options]
Bhandari, S., Brockners, F., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mizrahi, T., Kfir, A., Gafni, B., Lapukhov, P., Spiegel, M., Krishnan, S., Asati, R., and M. Smith, "In-situ OAM IPv6 Options", draft-ietf-ippm-ioam-ipv6-options-04 (work in progress), November 2020.

[I-D.ietf-ippm-ioam-direct-export]
Song, H., Gafni, B., Zhou, T., Li, Z., Brockners, F., Bhandari, S., Sivakolundu, R., and T. Mizrahi, "In-situ OAM Direct Exporting", draft-ietf-ippm-ioam-direct-export-02 (work in progress), November 2020.

[I-D.song-opsawg-ifit-framework]
Song, H., Qin, F., Chen, H., Jin, J., and J. Shin, "In-situ Flow Information Telemetry", draft-song-opsawg-ifit-framework-13 (work in progress), October 2020.

[I-D.ietf-rtgwg-segment-routing-ti-lfa]
Litkowski, S., Bashandy, A., Filsfils, C., Decraene, B., and D. Voyer, "Topology Independent Fast Reroute using Segment Routing", draft-ietf-rtgwg-segment-routing-ti-lfa-05 (work in progress), November 2020.

[I-D.hu-spring-segment-routing-proxy-forwarding]
Hu, Z., Chen, H., Yao, J., Bowers, C., and Y. Zhu, "SR-TE Path Midpoint Protection", draft-hu-spring-segment-routing-proxy-forwarding-12 (work in progress), October 2020.

[I-D.chen-rtgwg-srv6-midpoint-protection]
Chen, H., Hu, Z., Chen, H., and X. Geng, "SRv6 Midpoint Protection", draft-chen-rtgwg-srv6-midpoint-protection-03 (work in progress), October 2020.

[I-D.ietf-rtgwg-srv6-egress-protection]
Hu, Z., Chen, H., Chen, H., Wu, P., Toy, M., Cao, C., He, T., Liu, L., and X. Liu, "SRv6 Path Egress Protection", draft-ietf-rtgwg-srv6-egress-protection-02 (work in progress), November 2020.

[I-D.geng-spring-sr-redundancy-protection]
Geng, X., Chen, M., and F. Yang, "Segment Routing for Redundancy Protection", draft-geng-spring-sr-redundancy-protection-00 (work in progress), November 2020.

[I-D.li-spring-srv6-security-consideration]
Li, C., Li, Z., Xie, C., Tian, H., and J. Mao, "Security Considerations for SRv6 Networks", draft-li-spring-srv6-security-consideration-05 (work in progress), October 2020.

[RFC8201] McCann, J., Deering, S., Mogul, J., and R. Hinden, Ed., "Path MTU Discovery for IP version 6", STD 87, RFC 8201, DOI 10.17487/RFC8201, July 2017, <https://www.rfc-editor.org/info/rfc8201>.

[I-D.ietf-idr-bgp-ls-link-mtu]
Zhu, Y., Hu, Z., Peng, S., and R. Mwehair, "Signaling Maximum Transmission Unit (MTU) using BGP-LS", draft-ietf-idr-bgp-ls-link-mtu-00 (work in progress), November 2020.

[I-D.ietf-idr-sr-policy-path-mtu]
Li, C., Zhu, Y., Sawaf, A., and Z. Li, "Segment Routing Path MTU in BGP", draft-ietf-idr-sr-policy-path-mtu-02 (work in progress), November 2020.

[I-D.li-pce-pcep-pmtu]
Peng, S., Li, C., Han, L., and L. Ndifor, "Support for Path MTU (PMTU) in the Path Computation Element (PCE) communication Protocol (PCEP).", draft-li-pce-pcep-pmtu-03 (work in progress), October 2020.

[I-D.srcompdt-spring-compression-requirement]
Cheng, W., "Compressed SRv6 SID List Requirements", draft-srcompdt-spring-compression-requirement-03 (work in progress), January 2021.

[I-D.cl-spring-generalized-srv6-np]
Cheng, W., Li, Z., Li, C., Xie, C., Li, C., Tian, H., and F. Zhao, "Generalized SRv6 Network Programming", draft-cl-spring-generalized-srv6-np-02 (work in progress), September 2020.

[I-D.lc-6man-generalized-srh]
Li, Z., Li, C., Cheng, W., Xie, C., Cong, L., Tian, H., and F. Zhao, "Generalized Segment Routing Header", draft-lc-6man-generalized-srh-01 (work in progress), August 2020.

[I-D.cl-spring-generalized-srv6-for-cmpr]
Cheng, W., Li, Z., Li, C., Clad, F., Aihua, L., Xie, C., Liu, Y., and S. Zadok, "Generalized SRv6 Network Programming for SRv6 Compression", draft-cl-spring-generalized-srv6-for-cmpr-02 (work in progress), November 2020.

[I-D.li-apn-framework]
Li, Z., Peng, S., Voyer, D., Li, C., Geng, L., Cao, C., Ebisawa, K., Previdi, S., and J. Guichard, "Application-aware Networking (APN) Framework", draft-li-apn-framework-01 (work in progress), September 2020.

[I-D.li-6man-app-aware-ipv6-network]
Li, Z., Peng, S., Li, C., Xie, C., Voyer, D., Li, X., Liu, P., Liu, C., and K. Ebisawa, "Application-aware IPv6 Networking (APN6) Encapsulation", draft-li-6man-app-aware-ipv6-network-02 (work in progress), July 2020.

Authors' Addresses

Cheng Li (editor)
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095
China

Email: c.l@huawei.com

Zhenbin Li
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095
China

Email: lizhenbin@huawei.com

Hongjie Yang
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095
China

Email: hongjie.yang@huawei.com