LSR Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 24, 2018

U. Chunduri, Ed.
Huawei USA
J. Tantsura
Nuage Networks
Y. Qu
Huawei USA
March 23, 2018

Usage of Non Shortest Path Forwarding (NSPF) IDs in IS-IS
draft-ct-isis-nspfid-for-sr-paths-01

Abstract

This document specifies the advertisement of Non Shortest Path Forwarding IDentifier (NSPF ID) TLV and the computation procedures for the same in IS-IS protocol. NSPF ID allows to simplify the data plane path description of data traffic in SR deployments. This helps mitigate the MTU issues that are caused by additional SR overhead of the packet and allows traffic statistics.

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 RFC2119 [RFC2119].

Copyright Notice

Table of Contents

1. Introduction

In a network implementing source routing, packets may be transported through the use of segment identifiers (SIDs), where a SID uniquely identifies a segment as defined in [I-D.ietf-spring-segment-routing]. In SR-MPLS, a segment is encoded as a label and an ordered list of segments is encoded as a stack of labels. In SRv6, a segment is encoded as an IPv6 address, with a new type of IPv6 routing header

called SRH. An ordered list of segments is encoded as an ordered list of IPv6 addresses in SRH [I-D.ietf-6man-segment-routing-header].

The segment may include one or more nodes, unidirectional adjacencies between two nodes or service instruction by a particular node in the network. A Non Shortest Path (NSP) could be a Traffic Engineered (TE) path or an explicitly provisioned FRR path or a service chained path. NSP can be described using list of segments in SR. However, this creates a problem of having a relatively large stack imposed on the data packet. A path that is encoded with SIDs can be a loose or strict path. In a strict path all the nodes/links on the path are encoded as SIDs, with the expense of number of total SIDs in the stack.

1.1. Mitigation with MSD and RLD

The number of SIDs in the stack a node can impose is referred as Maximum SID Depth (MSD) capability [I-D.ietf-isis-segment-routing-msd], which must be taken into consideration when computing a path to transport a data packet in a network implementing segment routing. [I-D.ietf-isis-mpls-elc] defines Readable Label Depth (RLD) that is used by a head-end to insert Entropy Label pair (ELI/EL) at appropriate depth, so it could be read by transit nodes. There are situations where the source routed path can be excessive as path represented by SR SIDs need to describe all the nodes and ELI/EL based on the readability of the nodes in that path.

While MSD (and RLD) capabilities advertisement help mitigate the problem for a central entity to create the right source routed path per application/operator requirements; actual depth is still limited by the underlying hardware in the data path.

1.2. Issues with Increased SID Depth

Consider the following network where SR-MPLS data plane is in use and with same SRGB (5000-6000) on all nodes i.e., A1 to A7 and B1 to B7 for illustration:

```
        SID:10   SID:20   SID:30   SID:40  SID:50 SID:300(Ax)  SID:60   SID:70
        A1-------A2-------A3-------A4-------A5===============A6----------A7
                 \               /  \5     5/ \   SID:310(Ay) \          /
                  \ 10        10/    +-A10-+   \               \10      /10
                   \           /      SID:100   \               \      /
             SID:80 \A8-----A9/SID:90            \  40           \    /
                    /         \                   +---+           \  /
                   /10 B2x:125 \10                     \           \/
        B1--------B2============B3----B4--------B5-------B6----------B7
        SID:110   SID:120  SID:130   SID:140   SID:150  SID:160  SID:170
```

Figure 1: SR-MPLS Network

Global ADJ SIDs are provisioned between A5 and A6 .All other SIDs shown are nodal SID indices.

All metrics of the links are set to 1, other values as configured.

Shortest Path from A1 to A7: A2-A3-A4-A5-A6-A7

NSP1: From A1 to A7 - A2-A8-B2-B2x-A9-A10-Ax-A7; Pushed Label Stack @A1: 5020:5080:5120:5125:5090:5100:5300:5070 (where B2x is a local ADJ-SID and Ax is a global ADJ-SID)

In the above example NSP1 is represented with a combination of Adjacency and Node SIDs with a stack of 8 labels each. However, this value can be larger, if the use of entropy label is desired and based on the RLD capabilities of each node and additional labels required to insert ELI/EL at appropriate places. Though above network is shown with SR-MPLS data plane, problem is similar if the network were a SR-IPv6 network with all SIDs encoded as IPv6 SIDs in SRH.

In various SR deployments, the following issues may arise:

a. Not all nodes in the path can support MSD or RLD needed to satisfy user/operator requirements, when the number of SIDs increased to describe the source routed path. This problem gets multiplied by four times in SRH compared to MPLS data plane because of the SID size (16 bytes) in SRH.

b. Even if all nodes can support the required MSD or RLD, the bigger label stack/depth can cause potential MTU/fragmentation issues.

c. In some deployments, it is also required reducing the overhead in the network layer, especially for low packet size packets, where the actual data can be way lesser than all encapsulations and SR path overheads.

Apart from the above some deployments need path accounting statistics for path monitoring and traffic re-optimizations. [I-D.hegde-spring-traffic-accounting-for-sr-paths] proposes a solution, however this further increases the depth of SID stack. The approach could be counter productive in the environments, where SID depth is already causing deployment issues as listed above.

To mitigate the above issues, and also to facilitate forwarding plane a mechanism to identify the SR path with a corresponding data plane identifier for accounting of traffic for SR paths, this draft proposes a new IS-IS TLV (Section 2) to advertise the NSPs with Non Shortest Path Forwarding IDentifier (NSPF ID).

This draft lays out procedure for IS-IS nodes to how to use NSPF ID TLV in Section 3. With corresponding data plane, Section 3 mechanism, reduces the SID stack in the data plane from 8 SIDs shown in SR-PATH-1 and SR-PATH-2 with a single NSPF ID. This draft also introduce source routed paths with NSPF ID types defined for native IPv4 and IPv6 data planes as defined in Section 2.2.

1.3. Acronyms

EL - Entropy Label

ELI - Entropy Label Indicator

MPLS - Multi Protocol Label Switching

MSD - Maximum SID Depth

MTU - Maximum Transferrable Unit

NSP - Non Shortest Path

SID - Segment Identifier

SPF - Shortest Path First

SR - Segment Routing

SRH - Segment Routing Header

SR-MPLS - Segment Routing with MPLS data plane

SRv6 - Segment Routing with Ipv6 data plane with SRH

SRH - IPv6 Segment Routing Header

TE   - Traffic Engineering

2. Non Shortest Path Forwarding IDentifier TLV

This section describes the encoding of NSPF ID TLV. This TLV can be seen as having 3 logical section viz., encoding od FEC Prefix, encoding of NSPF-ID with description of ordered path with sub-TLVs and a set of optional non-NSP sub-TLVs which can be used to describe one or more parameters of the path. Multiple instances of this TLV MAY be advertised in IS-IS LSPs with different NSPF-ID Type and with corresponding path description sub-TLVS. The NSPF-ID TLV has Type TBD (suggested value xxx), and has the following format:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |     Length    |     Reserved  |     Flags     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           MT-ID               | Prefix Len    | FEC Prefix    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//           FEC Prefix (continued, variable)                  //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| NSPF-ID Type  | NSPF-ID Len   | NSPF-ID Flags |  NSPF-ID Algo |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//           NSPF-ID  (continued, variable)                    //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|No.of NSP-STs  |  NSP sub-TLVs (Variable)                     //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|No.of Other-STs| Non-NSP sub-TLVs(variable)                    //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: NSPF ID TLV Format

Type - TBD from IS-IS top level TLV registry.

Length - Total length of the value field in bytes (variable).

Reserved - 1 Octet reserved bits for future use. Reserved bits MUST be reset on transmission and ignored on receive.

Flags - Flags for this TLV are described in Section 2.1.

MT-ID - is the multi-topology identifier defined in [RFC5120] with 4 most significant bits reset on transmission and ignored on receive. The remaining 12-bit field contains the MT-ID.

Prefix Len - contains the length of the prefix in bits. Only the most significant octets of the Prefix are encoded.

FEC Prefix - represents the Forwarding Equivalence Class at the tail-end of the advertised NSP. The "FEC Prefix" corresponds to a routable prefix of the originating node and it MAY have one of the [RFC7794] flags set (X-Flag/R-Flag/N-Flag). Value of this field MUST be 4 octets for IPv4 "FEC Prefix". Value of this field MUST be 16 octets for IPv6 "FEC Prefix". Encoding is similar to TLV 135 and TLV 236 or MT-Capable [RFC5120] IPv4 (TLV 235) and IPv6 Prefixes (TLV 237) respectively.

2.1. Flags

Flags: 1 octet field of NSPD ID TLV has following flags defined. These flags mostly related to applicability of this TLV in an L1 area or entire IS-IS domain:

```
  NSPF ID Flags Format

      0 1 2 3 4 5 6 7
     +-+-+-+-+-+-+-+-+
     |S|D|A| Rsrvd   |
     +-+-+-+-+-+-+-+-+
```

S - If set, the NSPF ID TLV MUST be flooded across the entire routing domain. If the S flag is not set, the NSPF ID TLV MUST NOT be leaked between IS-IS levels. This bit MUST NOT be altered during the TLV leaking

D - when the NSPF ID TLV is leaked from IS-IS level-2 to level-1, the D bit MUST be set. Otherwise, this bit MUST be clear. NSPF ID TLVs with the D bit set MUST NOT be leaked from level-1 to level-2. This is to prevent TLV looping across levels.

A - The originator of the NSPF ID TLV MUST set the A bit in order to signal that the prefixes and NSPF-IDs advertised in the NSPF ID TLV are directly connected to their originators. If this bit is not set, this allows any other node in the network advertise this TLV on behalf of the originating node of the "FEC Prefix". If the NSPF ID TLV is leaked to other areas/levels the A-flag MUST be cleared.

Rsrvd - reserved bits for future use. Reserved bits MUST be reset on transmission and ignored on receive.

2.2. NSPF-ID Fields

This represents the actual data plane identifier in the packet and could be of any data plane as defined in type field. Both "FEC Prefix" and NSPF-ID MUST belong to a same node in the network.

1. NSPF-ID Type: This is a new registry (TBD IANA) for this TLV and the defined types are as follows. Type: 1 - MPLS SID/Label Type: 2 Native IPv4 Address Type: 3 Native IPv6 Address Type 4: IPv6 SID in SRv6 with SRH

2. NSPF-ID Len: Length of the NSPF Identifier field in octets and this depends on the NSPF-ID type. See NSPF-ID below for the length of this field and other considerations.

3. NSPF-ID Flags: 1 Octet field for NSPF-ID flags. Some of the bits could be NSPF-ID type specific and each new type MUST define the flags applicable to the NSPF-ID type. For NSPF-ID Type 1, the flags are same as Section 2.1 definition in [I-D.ietf-isis-segment-routing-extensions]. For NSPF-ID Type 2, 3 and NSPF-ID Type 4 only 'R' flag is applicable. Undefined flags for each NSPF-ID type MUST be considered as reserved. Reserved flag bits in each NSPF-ID type specific flags MUST be reset on transmission and ignored on receive.

4. NSPF-ID Algo: 1 octet value represents the SPF algorithm. Algorithm registry is as defined in [I-D.ietf-isis-segment-routing-extensions].

5. NSPF-ID: This is the NSP forwarding identifier that would be on the data packet. The value of this field is variable and it depends on the NSPF-ID Type. For Type 1, this is and MPLS SID/ Label. For Type 2 this is a 4 byte IPv4 address. For Type 3 and Type 4, it is a 16 byte IPv6 address. For NSPF-ID Type 2, 3 or 4, if the NSPF-ID Len is set to 0, then FEC Prefix would also become the NSPF-ID. In the case when NSPF-ID Len is 0 and NSPF-ID Type is 2, then FEC Prefix length MUST be a 4 byte IPv4 address. Similarly, if NSPF-ID Type is 3 or 4 with NSPF-ID Len is set to 0, then FEC Prefix MUST be of a 16 byte IPv6 Address. For NSPF-ID Type 2, 3 or 4, if the NSPF-ID Len is set to non zero value, then the NSPF-ID MUST not be advertised as a routable prefix in TLV 135, TLV 235, TLV 236 and TLV 237, but that MUST belog to the node where "FEC Prefix" is advertised.

6. No.of NSP-STs: Total number of the NSP sub-TLVs are defined with this 1-octet field. The value MUST NOT be zero.

2.3. NSP sub-TLVs

A new sub-TLV registry is created (TBD IANA) called NSP sub-TLVs. These are used to describe the path in the form of set of contiguous and ordered sub-TLVs, with first sub-TLV representing the top of the stack or first segment. These set of ordered TLVs can have both topological SIDs and non-topological SIDs (e.g., service segments).

Type 1: SID/Label sub-TLV as defined in [I-D.ietf-isis-segment-routing-extensions]. Only Type is defined and Length/Value fields are per Section 2.3 of the referenced document.

Type 2: Prefix SID sub-TLV as defined in [I-D.ietf-isis-segment-routing-extensions]. Only Type is defined and Length/Value fields are per Section 2.1 of the referenced document.

Type 3: Adjacency SID sub-TLV as defined in [I-D.ietf-isis-segment-routing-extensions]. Only Type is defined and Length/Value fields are per Section 2.2 of the referenced document.

Type 4: Length 4 bytes, value is 4 bytes IPv4 address encoded similar to IPv4 FEC Prefix described above.

Type 5: Length 16 bytes; value is 16 bytes IPv6 address encoded similar to IPv6 FEC Prefix described above.

Type 6: SRv6 Node SID TLV as defined in [I-D.bashandy-isis-srv6-extensions]. Only Type is defined and Length/Value fields are per Section 4 of the referenced document.

Type 7: SRv6 Adjacency-SID sub-TLV as defined in [I-D.bashandy-isis-srv6-extensions]. Only Type is defined and Length/Value fields are per Section 6.1 of the referenced document.

Type 8: SRv6 LAN Adjacency-SID sub-TLV as defined in [I-D.bashandy-isis-srv6-extensions]. Only Type is defined and Length/Value fields are per Section 6.2 of the referenced document.

2.4. Non-NSP sub-TLVs

NSPF ID TLV also defines a new sub-TLV registry (TBD IANA) for defining extensible set of sub-TLVs other than describing the path sub-TLVs. Total number of the path sub-TLVs to describe the path are

defined in 1-octet field "No.of Other-STs" just before the Non-NSP sub-TLVs. This field serves as a demarcation for set of ordered NSP sub-TLVs and Non-NSP sub-TLVs.

Type 1: Length 0 No value field. Specifies a counter to count number of packets forwarded on this NSPF-ID.

Type 2: Length 0 No value field. Specifies a counter to count number of bytes forwarded on this NSPF-ID specified in the network header (e.g. IPv4, IPv6).

Type 3: Length 4 bytes, and Value is metric of this path represented through the NSPF-ID. Different nodes can advertise the same NSPF-ID for the same FEC-Prefix with a different set of NSP sub-TLVs and the receiving node MUST consider the lowest metric value (TBD more, what happens when metric is same for two different set of NSP sub-TLVs).

3. Elements of Procedure

As specified in Section 1, a NSP can be a TE path, locally provisioned by the operator. Consider the following IS-IS network to describe the operation of NSPF ID TLV as defined in Section 2:

```
                                           1
                                        ________
                                       /   1   \
                                   +---R2-------R3---+
                                  /    \_______/      \
                                 /         1           \
                              1 /        2              \ 1
                               /       _______           \
                              /       /      \            \
                            R1------R6       R7-----------R4
                              \  2    \______/    2       /\
                               \          2              /  \
                              3 \                       / 3  \1
                                 \                 4   /      \
                                  +----R8------R9-----R10------R12
                                                \          1   /
                                               1 \            / 1
                                                  +----R11---+
```

Figure 3: IS-IS Network

In the above diagram (Figure 3) node R1 is an ingress node, or a head-end node, and the node R4 may be an egress node or another head-

end node. The numbers shown on each of the links between nodes R1-R11 indicate a IS-IS metric as provisioned by the operator. R1 may be configured to receive TE source routed path information from a central entity (PCE or Controller) that comprise NSP information which relates to sources that are attached to R1. It is also possible to have an NSP provisioned locally by the operator for non-TE needs (FRR or for chaining certain services). The NSP information is encoded as an ordered list of segments from source to a destination node in the network and is represented with an NSPF-ID. The NSP information includes NSP sub-TLVS which represents both topological and non-topological segments and specifies the actual path towards a FEC/Prefix by R4.

The shortest path towards R4 from R1 are through the following sequence of nodes: R1-R2-R3-R4 based on the configured metrics. The central entity may define a few NSPs from R1 to R4 that deviate from the shortest path based on other network characteristic requirements as requested by an application or service. For example, the network characteristics or performance requirements may include bandwidth, jitter, latency, throughput, error rate, etc. A first NSP may be identified by NSPF ID = 2 and may include the path of R1-R6-R7-R4 for a FEC Prefix advertised by R4. A second NSP may be identified by NSPF ID = 3 and may include the path of R1-R8-R9-R10-R4. Though these example shows NSP with all nodal SIDs, it is possible to have an NSP with combination of node and adjacency SIDS (local or global) or with non-topological segments along with these.

Each receiving node, determine whether an advertised NSP includes information regarding the receiving node. This MAY be done, during the end of the SPF computation for MTID that is advertised in this TLV and for the FEC/Prefix. For example, node R9 receives the NSP information, and ignores the first NSP identified by NSPF ID = 2 because this NSP does not include node R9.

However, node R9 may determine that the second NSP identified by NSPF ID = 3 does include the node R9 for the FEC prefix advertised by R4. Therefore, node R9 updates the local forwarding database to include an entry for the destination address of R4 that indicates, that when a data packet comprising a NSPF-ID of 3 is received, forward the data packet to node R10 instead of R11. This is even though from R9 the shortest path cost to reach R4 via R11 is 3 (R9-R11-R12-R4) it chooses the nexthop to R10 to reach R4 as specified in the NSP. Same process happens to all the nodes on the NSP.

In summary, the receiving node checks if this node is on the path, if yes, it adjusts the shortest path nexthop computed towards "FEC Prefix" to the shortest path nexthop towards the next segment as specified in the NSP.

4. NSPF ID Data Plane aspects

Data plane NSPF ID is selected by the entity (e.g., a controller, locally provisioned) which selects a particular NSP in the network. Section 2.2 defines various data plane identifier types and a corresponding data plane identifier type and identifier is selected by the entity which selects the NSP. Other data planes other than described below can also use this TLV to describe the NSP. Further details TBD.

4.1. MPLS Data Plane

If NSPF-ID Type is 1, the NSP belongs to SR-MPLS data plane and the complete NSP stack is represented with a unique SR SID/Label and this gets programmed on the data plane with the appropriate nexthop computed as specified in Section 3 . NSP path description here is a set of ordered SID TLVs and MAY contain both topological and non-topological segments.

4.2. SRv6 Data Plane

If NSPF-ID Type is 4, the NSP belongs to SRv6 with SRH data plane and the complete NSP stack is represented with IPv6 SIDs and this gets programmed on the data plane with the appropriate nexthop computed as specified in Section 3. NSP path description here is a set of ordered SID TLVs and MAY contain both topological and non-topological segments (e.g. network functions, service functions). If NSPF-ID Type is 3 this is the traditional IPv6 mode ([I-D.ietf-dmm-srv6-mobile-uplane]) and this doesn't include SRH and NSP stack description is similar to NSPF-ID Type 4 as described.

5. NSP Traffic Accounting

As described in Section 2.4, each node described in the NSP optional sub-TLVs can provision the hardware to account the traffic statistics as indicated in the non-NSP sub-TLVs for the actual data traffic. with this more granular and dynamic enablement of traffic statistics for only certain NSPs would be possible. This approach, thus is more safe and secure than any mechanism that involves creating state in the nodes with data traffic itself. This is because creation and deletion of the traffic accounting state for NSPs happen through IS-IS LSP processing and IS-IS security Section 8 options are applicable to this TLV.

How the traffic accounting is distributed to a central entity is out of scope of this document. One can use any method (e.g. gRPC) to extract the NSPF-ID traffic stats from various nodes along the path.

6. Acknowledgements

Thanks to Richard Li, Alex Clemm, Kiran Makhijani and Lin Han for initial discussions on this topic.

Earlier versions of draft-ietf-isis-segment-routing-extensions have a mechanism to advertise EROs through Binding SID.

7. IANA Considerations

This document requests the following new TLVin IANA IS-IS TLV code-point registry.

TLV #	Name
TBD	NSPF ID TLV

This document also requests IANA to create new registries for NSPF-ID Type, NSP sub-TLVs and Non-NSP sub-TLVs in NSPF ID TLV as described in Section 2.

8. Security Considerations

Security concerns for IS-IS are addressed in [RFC5304] and [RFC5310]. Further security analysis for IS-IS protocol is done in [RFC7645]. Advertisement of the additional information defined in this document introduces no new security concerns in IS-IS protocol. However as this extension is related to SR-MPLS and SRH data planes as defined in [I-D.ietf-spring-segment-routing], those particular data plane security considerations does apply here.

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>.

9.2. Informative References

[I-D.bashandy-isis-srv6-extensions]
Ginsberg, L., Bashandy, A., Filsfils, C., Decraene, B., and Z. Hu, "IS-IS Extensions to Support Routing over IPv6 Dataplane", draft-bashandy-isis-srv6-extensions-02 (work in progress), March 2018.

[I-D.hegde-spring-traffic-accounting-for-sr-paths]
Hegde, S., "Traffic Accounting for MPLS Segment Routing Paths", draft-hegde-spring-traffic-accounting-for-sr-paths-01 (work in progress), October 2017.

[I-D.ietf-6man-segment-routing-header]
Previdi, S., Filsfils, C., Leddy, J., Matsushima, S., and d. daniel.voyer@bell.ca, "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header-10 (work in progress), March 2018.

[I-D.ietf-dmm-srv6-mobile-uplane]
Matsushima, S., Filsfils, C., Kohno, M., Camarillo, P., daniel.voyer@bell.ca, d., and C. Perkins, "Segment Routing IPv6 for Mobile User Plane", draft-ietf-dmm-srv6-mobile-uplane-01 (work in progress), March 2018.

[I-D.ietf-isis-mpls-elc]
Xu, X., Kini, S., Sivabalan, S., Filsfils, C., and S. Litkowski, "Signaling Entropy Label Capability and Readable Label-stack Depth Using IS-IS", draft-ietf-isis-mpls-elc-03 (work in progress), January 2018.

[I-D.ietf-isis-segment-routing-extensions]
Previdi, S., Ginsberg, L., Filsfils, C., Bashandy, A., Gredler, H., Litkowski, S., Decraene, B., and J. Tantsura, "IS-IS Extensions for Segment Routing", draft-ietf-isis-segment-routing-extensions-15 (work in progress), December 2017.

[I-D.ietf-isis-segment-routing-msd]
Tantsura, J., Chunduri, U., Aldrin, S., and L. Ginsberg, "Signaling MSD (Maximum SID Depth) using IS-IS", draft-ietf-isis-segment-routing-msd-09 (work in progress), January 2018.

[I-D.ietf-spring-segment-routing]
Filsfils, C., Previdi, S., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", draft-ietf-spring-segment-routing-15 (work in progress), January 2018.

[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>.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008, <https://www.rfc-editor.org/info/rfc5304>.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, DOI 10.17487/RFC5310, February 2009, <https://www.rfc-editor.org/info/rfc5310>.

[RFC7413] Cheng, Y., Chu, J., Radhakrishnan, S., and A. Jain, "TCP Fast Open", RFC 7413, DOI 10.17487/RFC7413, December 2014, <https://www.rfc-editor.org/info/rfc7413>.

[RFC7645] Chunduri, U., Tian, A., and W. Lu, "The Keying and Authentication for Routing Protocol (KARP) IS-IS Security Analysis", RFC 7645, DOI 10.17487/RFC7645, September 2015, <https://www.rfc-editor.org/info/rfc7645>.

[RFC7794] Ginsberg, L., Ed., Decraene, B., Previdi, S., Xu, X., and U. Chunduri, "IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability", RFC 7794, DOI 10.17487/RFC7794, March 2016, <https://www.rfc-editor.org/info/rfc7794>.

Authors' Addresses

Uma Chunduri (editor)
Huawei USA
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: uma.chunduri@huawei.com

Jeff Tantsura
Nuage Networks
755 Ravendale Drive
Mountain View, CA 94043
USA

Email: jefftant.ietf@gmail.com

Yingzhen Qu
Huawei USA
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: yingzhen.qu@huawei.com