Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 20, 2017

C. Filsfils, Ed.
S. Previdi, Ed.
Cisco Systems, Inc.
E. Aries
Juniper Networks
D. Afanasiev
Yandex

February 16, 2017

Segment Routing Centralized BGP Egress Peer Engineering
draft-ietf-spring-segment-routing-central-epe-04

Abstract

Segment Routing (SR) leverages source routing. A node steers a packet through a controlled set of instructions, called segments, by prepending the packet with an SR header. A segment can represent any instruction topological or service-based. SR allows to enforce a flow through any topological path and service chain while maintaining per-flow state only at the ingress node of the SR domain.

The Segment Routing architecture can be directly applied to the MPLS dataplane with no change on the forwarding plane. It requires minor extension to the existing link-state routing protocols.

This document illustrates the application of Segment Routing to solve the BGP Egress Peer Engineering (BGP-EPE) requirement. The SR-based BGP-EPE solution allows a centralized (SDN) controller to program any egress peer policy at ingress border routers or at hosts within the domain.

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.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

The document is structured as follows:

- Section 1 states the BGP-EPE problem statement and provides the key references.

- Section 2 defines the different BGP Peering Segments and the semantic associated to them.

- Section 3 describes the automated allocation of BGP Peering SID's by the BGP-EPE enabled egress border router and the automated signaling of the external peering topology and the related BGP Peering SID's to the collector [I-D.ietf-idr-bgpls-segment-routing-epe].

- Section 4 overviews the components of a centralized BGP-EPE controller. The definition of the BGP-EPE controller is outside the scope of this document.

- Section 5 overviews the methods that could be used by the centralized BGP-EPE controller to implement a BGP-EPE policy at an ingress border router or at a source host within the domain. The exhaustive definition of all the means to program an BGP-EPE input policy is outside the scope of this document.

For editorial reasons, the solution is described for IPv4 and MPLS SID. This solution is equally applicable to IPv6 with either MPLS-SR or IPv6 SR.

1.1. Segment Routing Documents

The main references for this document are:

- SR Problem Statement: [RFC7855].

- SR Architecture: [I-D.ietf-spring-segment-routing].

- Distribution of External Topology and TE Information using BGP: [I-D.ietf-idr-bgpls-segment-routing-epe].

The SR instantiation in the MPLS dataplane is described in [I-D.ietf-spring-segment-routing-mpls].

The SR IGP protocol extensions are defined in [I-D.ietf-isis-segment-routing-extensions], [I-D.ietf-ospf-segment-routing-extensions] and [I-D.ietf-ospf-ospfv3-segment-routing-extensions].

The Segment Routing PCE protocol extensions are defined in [I-D.ietf-pce-segment-routing].

1.2. Problem Statement

The BGP-EPE problem statement is defined in [RFC7855].

A centralized controller should be able to instruct an ingress Provider Edge router (PE) or a content source within the domain to use a specific egress PE and a specific external interface/neighbor to reach a particular destination.

We call this solution "BGP-EPE" for "BGP Egress Peer Engineering". The centralized controller is called the "BGP-EPE Controller". The egress border router where the BGP-EPE traffic steering functionality is implemented is called a BGP-EPE enabled border router. The input policy programmed at an ingress border router or at a source host is called a BGP-EPE policy.

The requirements that have motivated the solution described in this document are listed here below:

- The solution MUST apply to the Internet use-case where the Internet routes are assumed to use IPv4 unlabeled or IPv6 unlabeled. It is not required to place the Internet routes in a VRF and allocate labels on a per route, or on a per-path basis.

- The solution MUST NOT make any assumption on the currently deployed iBGP schemes (RRs, confederations or iBGP full meshes) and MUST be able to support all of them.

- The solution MUST be applicable to any type of EPE router. While "Egress Peer Engineering" refers to "External" peering, the solution MUST also be applicable to a router having internal peers.

- The solution SHOULD minimize the need for new BGP capabilities at the ingress PEs.

- The solution MUST accommodate an ingress BGP-EPE policy at an ingress EPE or directly at an source host within the domain.

- The solution MUST support automated Fast Reroute (FRR) and fast convergence mechanisms.

The following reference diagram is used throughout this document.

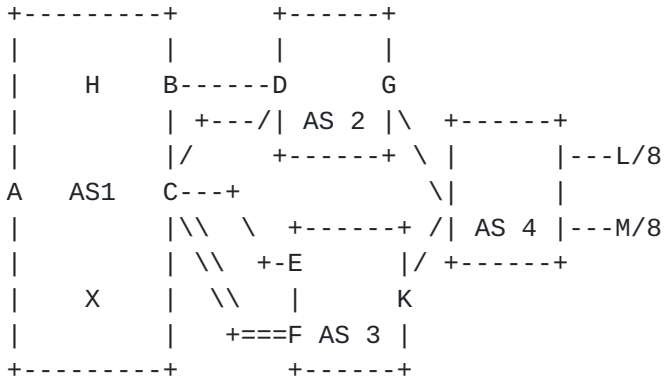

Figure 1: Reference Diagram

IPv4 addressing:

- C's interface to D: 198.51.100.1/30, D's interface: 198.51.100.2/30

- C's interface to E: 198.51.100.5/30, E's interface: 198.51.100.6/30

- C's upper interface to F: 198.51.100.9/30, F's interface: 198.51.100.10/30

- C's lower interface to F: 198.51.100.13/30, F's interface: 198.51.100.14/30

- BGP router-ID of D: 192.0.2.4/32

- BGP router-ID of E: 192.0.2.3/32

- Loopback of F used for eBGP multi-hop peering to C: 192.0.2.2/32

- C's loopback is 203.0.113.3/32 with SID 64

C's BGP peering:

- Single-hop eBGP peering with neighbor 198.51.100.2 (D)
- Single-hop eBGP peering with neighbor 198.51.100.6 (E)
- Multi-hop eBGP peering with F on IP address 192.0.2.2 (F)

C's resolution of the multi-hop eBGP session to F:

- Static route 192.0.2.2/32 via 198.51.100.10
- Static route 192.0.2.2/32 via 198.51.100.14

C is configured with local policy that defines a BGP PeerSet as the set of peers (198.51.100.6 for E and 192.0.2.2 for F)

X is the BGP-EPE controller within AS1 domain.

H is a content source within AS1 domain.

2. BGP Peering Segments

As defined in [I-D.ietf-spring-segment-routing], certain segments are defined by BGP-EPE capable node and corresponding to its attached peers. These segments are called BGP peering segments or BGP Peering SIDs. They enable the expression of source-routed inter-domain paths.

An ingress border router of an AS may compose a list of segments to steer a flow along a selected path within the AS, towards a selected egress border router C of the AS and through a specific peer. At minimum, a BGP Egress Peering Engineering policy applied at an ingress EPE involves two segments: the Node SID of the chosen egress EPE and then the BGP Peering Segment for the chosen egress EPE peer or peering interface.

[I-D.ietf-spring-segment-routing] defines three types of BGP peering segments/SID's: PeerNode SID, PeerAdj SID and PeerSet SID.

A Peer Node Segment is a segment describing a peer, including the SID (PeerNode SID) allocated to it.

A Peer Adjacency Segment is a segment describing a link, including the SID (PeerAdj SID) allocated to it.

A Peer Set Segment is a segment describing a link or a node that is part of the set, including the SID (PeerSet SID) allocated to the set.

3. Distribution of Topology and TE Information using BGP-LS

In ships-in-the-night mode with respect to the pre-existing iBGP design, a BGP-LS session is established between the BGP-EPE enabled border router and the BGP-EPE controller.

As a result of its local configuration and according to the behavior described in [I-D.ietf-idr-bgpls-segment-routing-epe], node C allocates the following BGP Peering Segments ([I-D.ietf-spring-segment-routing]):

- A PeerNode segment for each of its defined peer (D, E and F).
- A PeerAdj segment for each recursing interface to a multi-hop peer (e.g.: the upper and lower interfaces from C to F in figure 1).
- A PeerSet segment to the set of peers (E and F). In this case the PeerSet represents a set of peers (E, F) belonging to the same AS (AS 3).

C programs its forwarding table accordingly:

Incoming Label	Operation	Outgoing Interface
1012	POP	link to D
1022	POP	link to E
1032	POP	upper link to F
1042	POP	lower link to F
1052	POP	load balance on any link to F
1060	POP	load balance on any link to E or to F

C signals the related BGP-LS NLRI's to the BGP-EPE controller. Each such BGP-LS route is described in the following subsections according to the encoding details defined in [I-D.ietf-idr-bgpls-segment-routing-epe].

3.1. PeerNode SID to D

Descriptors:

- Node Descriptors (router-ID, ASN): 203.0.113.3 , AS1
- Peer Descriptors (peer router-ID, peer ASN): 192.0.2.4, AS2
- Link Descriptors (IP interface address, neighbor IP address): 198.51.100.1, 198.51.100.2

Attributes:

- PeerNode SID: 1012

3.2. PeerNode SID to E

Descriptors:

- Node Descriptors (router-ID, ASN): 203.0.113.3 , AS1
- Peer Descriptors (peer router-ID, peer ASN): 192.0.2.3, AS3
- Link Descriptors (IP interface address, neighbor IP address): 198.51.100.5, 198.51.100.6

Attributes:

- PeerNode SID: 1022
- PeerSetSID: 1060
- Link Attributes: see section 3.3.2 of [RFC7752]

3.3. PeerNode SID to F

Descriptors:

- Node Descriptors (router-ID, ASN): 203.0.113.3 , AS1
- Peer Descriptors (peer router-ID, peer ASN): 192.0.2.2, AS3
- Link Descriptors (IP interface address, neighbor IP address): 203.0.113.3, 192.0.2.2

Attributes:

- PeerNode SID: 1052
- PeerSetSID: 1060

3.4. First PeerAdj to F

Descriptors:

- Node Descriptors (router-ID, ASN): 203.0.113.3 , AS1
- Peer Descriptors (peer router-ID, peer ASN): 192.0.2.2, AS3

- Link Descriptors (IP interface address, neighbor IP address): 198.51.100.9, 198.51.100.10

Attributes:

- PeerAdj-SID: 1032
- LinkAttributes: see section 3.3.2 of [RFC7752]

3.5. Second PeerAdj to F

Descriptors:

- Node Descriptors (router-ID, ASN): 203.0.113.3 , AS1
- Peer Descriptors (peer router-ID, peer ASN): 192.0.2.2, AS3
- Link Descriptors (IP interface address, neighbor IP address): 198.51.100.13, 198.51.100.14

Attributes:

- PeerAdj-SID: 1042
- LinkAttributes: see section 3.3.2 of [RFC7752]

3.6. Fast Reroute (FRR)

An BGP-EPE enabled border router SHOULD allocate a FRR backup entry on a per BGP Peering SID basis:

- PeerNode SID
  1. If multi-hop, backup via the remaining PeerADJ SIDs (if available) to the same peer.
  2. Else backup via another PeerNode SID to the same AS.
  3. Else pop the PeerNode SID and perform an IP lookup.
- PeerAdj SID
  1. If to a multi-hop peer, backup via the remaining PeerADJ SIDs (if available) to the same peer.
  2. Else backup via a PeerNode SID to the same AS.
  3. Else pop the PeerNode SID and perform an IP lookup.

- PeerSet SID

  1. Backup via remaining PeerNode SIDs in the same PeerSet.

  2. Else pop the PeerNode SID and IP lookup.

We illustrate the different types of possible backups using the reference diagram and considering the Peering SIDs allocated by C.

PeerNode SID 1052, allocated by C for peer F:

- Upon the failure of the upper connected link CF, C can reroute all the traffic onto the lower CF link to the same peer (F).

PeerNode SID 1022, allocated by C for peer E:

- Upon the failure of the connected link CE, C can reroute all the traffic onto the link to PeerNode SID 1052 (F).

PeerNode SID 1012, allocated by C for peer D:

- Upon the failure of the connected link CD, C can pop the PeerNode SID and lookup the IP destination address in its FIB and route accordingly.

PeerSet SID 1060, allocated by C for the set of peers E and F:

- Upon the failure of a connected link in the group, the traffic to PeerSet SID 1060 is rerouted on any other member of the group.

For specific business reasons, the operator might not want the default FRR behavior applied to a PeerNode SID or any of its dependent PeerADJ SID.

The operator should be able to associate a specific backup PeerNode SID for a PeerNode SID: e.g., 1022 (E) must be backed up by 1012 (D) which overrules the default behavior which would have preferred F as a backup for E.

4. BGP-EPE Controller

In this section, we provide a non-exhaustive set of inputs that an BGP-EPE controller would likely collect such as to perform the BGP-EPE policy decision.

The exhaustive definition is outside the scope of this document.

4.1. Valid Paths From Peers

The BGP-EPE controller should collect all the BGP paths (i.e.: IP destination prefixes) advertised by all the engineered peers.

This could be realized by setting an iBGP session with the BGP-EPE enabled border router, with "add-path all" and the original next-hop preserved.

In this case, C would advertise the following Internet routes to the BGP-EPE controller:

- NLRI <L/8>, nhop 198.51.100.2, AS Path {AS 2, 4}
  - X (i.e.: the BGP-EPE controller) knows that C receives a path to L/8 via neighbor 198.51.100.2 of AS2.
- NLRI <L/8>, nhop 198.51.100.6, AS Path {AS 3, 4}
  - X knows that C receives a path to L/8 via neighbor 198.51.100.6 of AS2.
- NLRI <L/8>, nhop 192.0.2.2, AS Path {AS 3, 4}
  - X knows that C has an eBGP path to L/8 via AS3 via neighbor 192.0.2.2

An alternative option would be for an BGP-EPE collector to use BGP Monitoring Protocol (BMP) to track the Adj-RIB-In of BGP-EPE enabled border routers.

4.2. Intra-Domain Topology

The BGP-EPE controller should collect the internal topology and the related IGP SIDs.

This could be realized by collecting the IGP LSDB of each area or running a BGP-LS session with a node in each IGP area.

4.3. External Topology

Thanks to the collected BGP-LS routes described in the section 2 (BGP-LS advertisements), the BGP-EPE controller is able to maintain an accurate description of the egress topology of node C. Furthermore, the BGP-EPE controller is able to associate BGP Peering SIDs to the various components of the external topology.

4.4. SLA characteristics of each peer

The BGP-EPE controller might collect SLA characteristics across peers. This requires an BGP-EPE solution as the SLA probes need to be steered via non-best-path peers.

Unidirectional SLA monitoring of the desired path is likely required. This might be possible when the application is controlled at the source and the receiver side. Unidirectional monitoring dissociates the SLA characteristic of the return path (which cannot usually be controlled) from the forward path (the one of interest for pushing content from a source to a consumer and the one which can be controlled).

Alternatively, Extended Metrics, as defined in [RFC7810] could also be advertised using BGP-LS ([I-D.ietf-idr-te-pm-bgp]).

4.5. Traffic Matrix

The BGP-EPE controller might collect the traffic matrix to its peers or the final destinations. IPFIX is a likely option.

An alternative option consists in collecting the link utilization statistics of each of the internal and external links, also available in the current definition of [RFC7752].

4.6. Business Policies

The BGP-EPE controller should collect business policies.

4.7. BGP-EPE Policy

On the basis of all these inputs (and likely others), the BGP-EPE Controller decides to steer some demands away from their best BGP path.

The BGP-EPE policy is likely expressed as a two-entry segment list where the first element is the IGP prefix SID of the selected egress border router and the second element is a BGP Peering SID at the selected egress border router.

A few examples are provided hereafter:

- Prefer egress PE C and peer AS AS2: {64, 1012}.
- Prefer egress PE C and peer AS AS3 via eBGP peer 198.51.100.6: {64, 1022}.

- Prefer egress PE C and peer AS AS3 via eBGP peer 192.0.2.2: {64, 1052}.

- Prefer egress PE C and peer AS AS3 via interface 198.51.100.14 of multi-hop eBGP peer 192.0.2.2: {64, 1042}.

- Prefer egress PE C and any interface to any peer in the group 1060: {64, 1060}.

Note that the first SID could be replaced by a list of segments. This is useful when an explicit path within the domain is required for traffic engineering purposes. For example, if the Prefix SID of node B is 60 and the BGP-EPE controller would like to steer the traffic from A to C via B then through the external link to peer D then the segment list would be {60, 64, 1012}.

5. Programming an input policy

The detailed/exhaustive description of all the means to implement an BGP-EPE policy are outside the scope of this document. A few examples are provided in this section.

5.1. At a Host

A static IP/MPLS route can be programmed at the host H. The static route would define a destination prefix, a next-hop and a label stack to push. Assuming a global SRGB, at least on all access routers connecting the hosts, the same policy can be programmed across all hosts, which is convenient.

5.2. At a router - SR Traffic Engineering tunnel

The BGP-EPE controller can configure the ingress border router with an SR traffic engineering tunnel T1 and a steering-policy S1 which causes a certain class of traffic to be mapped on the tunnel T1.

The tunnel T1 would be configured to push the required segment list.

The tunnel and the steering policy could be configured via PCEP according to [I-D.ietf-pce-segment-routing] and [I-D.ietf-pce-pce-initiated-lsp] or via Netconf ([RFC6241]).

Example: at A

Tunnel T1: push {64, 1042}
IP route L/8 set nhop T1

5.3. At a Router - RFC3107 policy route

The BGP-EPE Controller could build a RFC3107 ([RFC3107]) route (from scratch) and send it to the ingress router:

- NLRI: the destination prefix to engineer: e.g., L/8.
- Next-Hop: the selected egress border router: C.
- Label: the selected egress peer: 1042.
- AS path: reflecting the selected valid AS path.
- Some BGP policy to ensure it will be selected as best by the ingress router.

This RFC3107 policy route "overwrites" an equivalent or less-specific "best path". As the best-path is changed, this BGP-EPE input policy option may influence the path propagated to the upstream peer/ customers. Indeed, implementations treating the SAFI-1 and SAFI-4 routes for a given prefix as comparable would trigger a BGP WITHDRAW of the SAFI-1 route to them BGP upstream peers.

5.4. At a Router - VPN policy route

The BGP-EPE Controller could build a VPNv4 route (from scratch) and send it to the ingress router:

- NLRI: the destination prefix to engineer: e.g., L/8.
- Next-Hop: the selected egress border router: C.
- Label: the selected egress peer: 1042.
- Route-Target: selecting the appropriate VRF at the ingress router.
- AS path: reflecting the selected valid AS path.
- Some BGP policy to ensure it will be selected as best by the ingress router in the related VRF.

The related VRF must be preconfigured. A VRF fallback to the main FIB might be beneficial to avoid replicating all the "normal" Internet paths in each VRF.

5.5. At a Router - Flowspec route

A BGP-EPE Controller builds a FlowSpec route and sends it to the ingress router to engineer:

- Dissemination of Flow Specification Rules ([RFC5575].
- Destination/Source IP Addresses, IP Protocol, Destination/Source port (+1 component).
- ICMP Type/Code, TCP Flags, Packet length, DSCP, Fragment.

6. IPv6

The described solution is applicable to IPv6, either with MPLS-based or IPv6-Native segments. In both cases, the same three steps of the solution are applicable:

- BGP-LS-based signaling of the external topology and BGP Peering Segments to the BGP-EPE controller.
- Collection of various inputs by the BGP-EPE controller to come up with a policy decision.
- Programming at an ingress router or source host of the desired BGP-EPE policy which consists in a list of segments to push on a defined traffic class.

7. Benefits

The BGP-EPE solutions described in this document have the following benefits:

- No assumption on the iBGP design within AS1.
- Next-Hop-Self on the Internet routes propagated to the ingress border routers is possible. This is a common design rule to minimize the number of IGP routes and to avoid importing external churn into the internal routing domain.
- Consistent support for traffic engineering within the domain and at the external edge of the domain.
- Support both host and ingress border router BGP-EPE policy programming.
- BGP-EPE functionality is only required on the BGP-EPE enabled egress border router and the BGP-EPE controller: an ingress policy

can be programmed at the ingress border router without any new functionality.

- Ability to deploy the same input policy across hosts connected to different routers (avail the global property of IGP prefix SIDs).

8. IANA Considerations

This document does not request any IANA allocations.

9. Manageability Considerations

The BGP-EPE use-case described in this document requires BGP-LS ([RFC7752]) extensions that are described in [I-D.ietf-idr-bgpls-segment-routing-epe]. The required extensions consists of additional BGP-LS descriptors and TLVs that will follow the same. Manageability functions of BGP-LS, described in [RFC7752] also apply to the extensions required by the EPE use-case.

The operator MUST be capable of configuring, enabling, disabling the advertisement of the EPE information as well as to control which information is advertised to which internal or external peer. This is not different from what is required by a BGP speaker in terms of information origination and advertisement. In addition, the advertisement of EPE information MUST conform to standard BGP advertisement and propagation rules (iBGP, eBGP, Route-Reflectors, Confederations).

10. Security Considerations

[RFC7752] defines BGP-LS NLRIs and their associated security aspects.

[I-D.ietf-idr-bgpls-segment-routing-epe] defines the BGP-LS extensions required by the BGP-EPE mechanisms described in this document. BGP-EPE BGP-LS extensions also include the related security.

11. Contributors

Daniel Ginsburg substantially contributed to the content of this document.

12. Acknowledgements

The authors would like to thank Acee Lindem for his comments and contribution.

13. References

13.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3107] Rekhter, Y. and E. Rosen, "Carrying Label Information in BGP-4", RFC 3107, DOI 10.17487/RFC3107, May 2001, <http://www.rfc-editor.org/info/rfc3107>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <http://www.rfc-editor.org/info/rfc5575>.

[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, <http://www.rfc-editor.org/info/rfc6241>.

13.2. Informative References

[I-D.ietf-idr-bgpls-segment-routing-epe] Previdi, S., Filsfils, C., Patel, K., Ray, S., Dong, J., and M. Chen, "Segment Routing BGP Egress Peer Engineering BGP-LS Extensions", draft-ietf-idr-bgpls-segment-routing-epe-09 (work in progress), February 2017.

[I-D.ietf-idr-te-pm-bgp] Previdi, S., Wu, Q., Gredler, H., Ray, S., jefftant@gmail.com, j., Filsfils, C., and L. Ginsberg, "BGP-LS Advertisement of IGP Traffic Engineering Performance Metric Extensions", draft-ietf-idr-te-pm-bgp-04 (work in progress), October 2016.

[I-D.ietf-isis-segment-routing-extensions] Previdi, S., Filsfils, C., Bashandy, A., Gredler, H., Litkowski, S., Decraene, B., and j. jefftant@gmail.com, "IS-IS Extensions for Segment Routing", draft-ietf-isis-segment-routing-extensions-09 (work in progress), October 2016.

[I-D.ietf-ospf-ospfv3-segment-routing-extensions]
Psenak, P., Previdi, S., Filsfils, C., Gredler, H., Shakir, R., Henderickx, W., and J. Tantsura, "OSPFv3 Extensions for Segment Routing", draft-ietf-ospf-ospfv3-segment-routing-extensions-07 (work in progress), October 2016.

[I-D.ietf-ospf-segment-routing-extensions]
Psenak, P., Previdi, S., Filsfils, C., Gredler, H., Shakir, R., Henderickx, W., and J. Tantsura, "OSPF Extensions for Segment Routing", draft-ietf-ospf-segment-routing-extensions-10 (work in progress), October 2016.

[I-D.ietf-pce-pce-initiated-lsp]
Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model", draft-ietf-pce-pce-initiated-lsp-07 (work in progress), July 2016.

[I-D.ietf-pce-segment-routing]
Sivabalan, S., Medved, J., Filsfils, C., Crabbe, E., Raszuk, R., Lopez, V., Tantsura, J., Henderickx, W., and J. Hardwick, "PCEP Extensions for Segment Routing", draft-ietf-pce-segment-routing-08 (work in progress), October 2016.

[I-D.ietf-spring-segment-routing]
Filsfils, C., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", draft-ietf-spring-segment-routing-10 (work in progress), November 2016.

[I-D.ietf-spring-segment-routing-mpls]
Filsfils, C., Previdi, S., Bashandy, A., Decraene, B., Litkowski, S., Horneffer, M., Shakir, R., jefftant@gmail.com, j., and E. Crabbe, "Segment Routing with MPLS data plane", draft-ietf-spring-segment-routing-mpls-07 (work in progress), February 2017.

[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, <http://www.rfc-editor.org/info/rfc7752>.

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

[RFC7855] Previdi, S., Ed., Filsfils, C., Ed., Decraene, B., Litkowski, S., Horneffer, M., and R. Shakir, "Source Packet Routing in Networking (SPRING) Problem Statement and Requirements", RFC 7855, DOI 10.17487/RFC7855, May 2016, <http://www.rfc-editor.org/info/rfc7855>.

Authors' Addresses

Clarence Filsfils (editor)
Cisco Systems, Inc.
Brussels
BE

Email: cfilsfil@cisco.com

Stefano Previdi (editor)
Cisco Systems, Inc.
Via Del Serafico, 200
Rome 00142
Italy

Email: sprevidi@cisco.com

Ebben Aries
Juniper Networks
1133 Innovation Way
Sunnyvale CA 94089
US

Email: exa@juniper.net

Dmitry Afanasiev
Yandex
RU

Email: fl0w@yandex-team.ru