Inter-Domain Routing
Internet-Draft
Intended status: Standards Track
Expires: 19 August 2026

Z. Li, Ed.
S. Liu, Ed.
China Mobile

15 February 2026

BGP SR Policy Extensions for BFD Configuration
draft-li-idr-bgp-sr-policy-bfd-extension-01

Abstract

Segment Routing (SR) Policies require fast failure detection for Candidate Paths (CPs) to enable rapid rerouting and high availability. Currently, the provisioning of SR Policies and the configuration of associated Bidirectional Forwarding Detection (BFD) or Seamless BFD (S-BFD) sessions are performed independently. This often necessitates separate mechanisms (e.g., manual configuration, NETCONF, or additional signaling) to associate BFD/S-BFD sessions with the SR Policies, resulting in complex and error-prone operations

This document defines extensions to BGP SR Policy for the simultaneous provisioning of SR Policy CPs and their BFD/S-BFD configuration parameters during policy advertisement. The extensions include optional sub-TLVs within the Tunnel Encapsulation Attribute to carry BFD/S-BFD configuration parameters (e.g., discriminators, intervals, multipliers).

These extensions simplify deployment in distributed or controller-based environments, reduce configuration overhead, and enhance operational efficiency for SR-based traffic engineering.

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 https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 August 2026.

Table of Contents

1. Introduction

Segment Routing (SR) [RFC8402] enables source routing by allowing a headend node to steer packet flows along specific paths using an ordered list of segments, eliminating intermediate per-path states. An SR Policy [RFC9256] defines such paths as one or more Candidate Paths (CPs), each comprising one or more segment lists.

To ensure high availability and fast failure detection in SR networks, Bidirectional Forwarding Detection (BFD) [RFC5880] or Seamless BFD (S-BFD) [RFC7880] is commonly used to monitor SR Policy path liveliness. However, current deployments configure SR Policies and BFD/S-BFD sessions independently. Typically, an SR Policy Controller [RFC9256] defines the set of policies and advertises them to SR Policy headend routers (typically ingress routers) via BGP SR Policy [RFC9830], or PCEP [RFC8664][RFC9603]. After SR Policies are advertised and installed, separate mechanisms (e.g., manual

configuration, NETCONF/YANG, or additional signaling) are required to associate BFD/S-BFD parameters with the paths. This leads to increased operational complexity, longer provisioning times, and potential inconsistencies.

[I-D.ietf-pce-pcep-bfd-parameters] extends PCEP [RFC5440] to carry S-BFD parameters, which can be used together with [RFC8664] or [RFC9603] to complete S-BFD configuration while distributing SR Policies.

This document extends BGP SR Policy [RFC9830] to carry BFD/S-BFD parameters. These extensions enable simultaneous provisioning of SR Policies and their monitoring sessions, reducing separate configuration steps.

BGP itself does not install SR Policy CPs or BFD/S-BFD sessions into the data plane; these actions remain the responsibility of the SR Policy Module (SRPM) on the headend node.

The relationship between this document and existing BFD signaling mechanisms in BGP is discussed in Section 1.2.

1.1. 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.

1.2. Relationship to Existing BFD Mechanisms

[RFC9026] defines a BGP Path Attribute that enables BFD-based liveliness detection for BGP forwarding paths by associating a BFD session with a BGP path. While this mechanism is relevant to the general problem space of BFD-based liveness detection, it is primarily intended to validate BGP next-hop reachability and influence BGP path usability.

An SR Policy Candidate Path is not a BGP path and does not participate in the BGP best-path selection process. An SR Policy may consist of multiple Candidate Paths with distinct segment lists and traffic engineering characteristics. The liveness of these Candidate Paths is evaluated and acted upon by the SR Policy Module (SRPM) on the headend node, rather than by the BGP decision process.

Furthermore, SR Policy deployments often require distinct BFD or S-BFD sessions for individual Candidate Paths of the same SR Policy, possibly with different parameters. The BGP Path Attribute defined in [RFC9026] does not provide a mechanism to express such per-Candidate-Path BFD or S-BFD configuration. Therefore, the mechanism defined in [RFC9026] alone is not sufficient to support SR Policy Candidate Path-level liveliness monitoring, and this document defines extensions to BGP SR Policy to carry BFD and S-BFD configuration parameters at the Candidate Path level.

2. BGP SR Policy Extensions for BFD/S-BFD Configuration

This section defines extensions to BGP SR Policy that allow an SR Policy Candidate Path (CP) to be advertised together with the configuration parameters required to establish BFD [RFC5880] or S-BFD [RFC7880] sessions for monitoring the liveness of the path. The extensions are designed to be carried within the existing BGP SR Policy SAFI (73) and the Tunnel Encapsulation Attribute as specified in [RFC9830].

The BFD and S-BFD configuration parameters are carried in new optional sub-TLVs of the Tunnel Encapsulation Attribute [RFC9012]. These sub-TLVs are applicable only for the SR Policy SAFI (AFI/SAFI 1/73 or 2/73). They MAY appear at most once in a given Tunnel Encapsulation Attribute; if multiple instances of the same sub-TLV are present, only the first instance is processed and subsequent instances MUST be ignored. The Extended BGP SR Policy Encoding structure is as follows.

```
SR Policy SAFI NLRl: <Distinguisher, Color, Endpoint>
Attributes:
    Tunnel Encapsulation Attribute (23)
        Tunnel Type: SR Policy (15)
            Binding SID
            Preference
            Priority
            BFD Parameters (This Document)
            S-BFD Parameters (This Document)
            SR Policy Name
            SR Policy Candidate Path Name
            Explicit NULL Label Policy (ENLP)
            Segment List
                Weight
                Segment
                Segment
                ...
            ...
```

Figure 1: Extended BGP SR Policy Encoding

The introduced sub-TLVs in this document are not used by the BGP path selection process. They are passed unchanged to the SRPM on the headend node, which is responsible for validating the parameters and instantiating the corresponding BFD/S-BFD sessions.

2.1. BFD Parameters Sub-TLV

The BFD Parameters sub-TLV carries the configuration parameters needed to establish a classic BFD session for monitoring the SR Policy CP. The format of this BFD Parameters Sub-TLV is as follows.

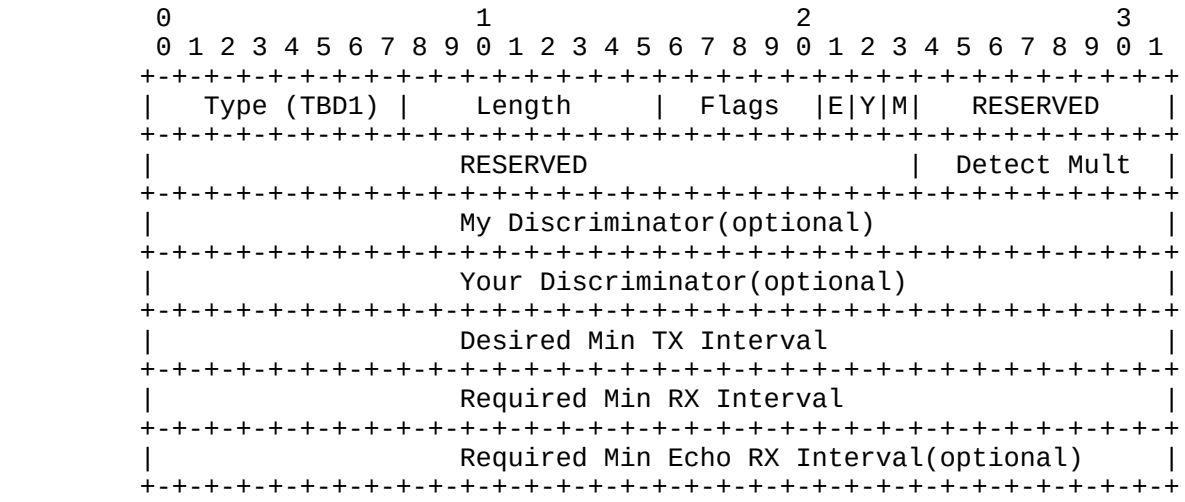

Figure 2: BFD Parameters Sub-TLV Format

Type: 1 octet. To be assigned by IANA from the "BGP Tunnel Encapsulation Attribute Sub-TLVs" registry (suggested value 21).

Length: 1 octet. Length of the value field in octets. The Length field reflects the total size of all fields following the Flags field, including any optional parameters that are present.

Flags: 1 octet. The Flags field indicates the presence of optional parameters in the BFD Parameters Sub-TLV. The following bits are defined:

M bit: Bit 0, When set, My Discriminator field is present in this Sub-TLV.

Y bit: Bit 1, When set, Your Discriminator field is present in this Sub-TLV.

E bit: Bit 2, When set, Required Min Echo RX Interval field is present in this Sub-TLV.

Bits 3 through 7 are reserved for future use. These bits SHOULD be set to zero on transmission and MUST be ignored on receipt.

RESERVED: reserved for future use. RESERVED field SHOULD be set to zero on transmission and MUST be ignored on receipt.

Other parameters have the same meaning as defined in [RFC5880].

If present, optional parameters MUST appear in the order shown in the BFD Parameters Sub-TLV format.

2.2. S-BFD Parameters Sub-TLV

The S-BFD Parameters sub-TLV carries the configuration parameters needed to establish a S-BFD session for monitoring the SR Policy CP. The format of this S-BFD Parameters Sub-TLV is as follows.

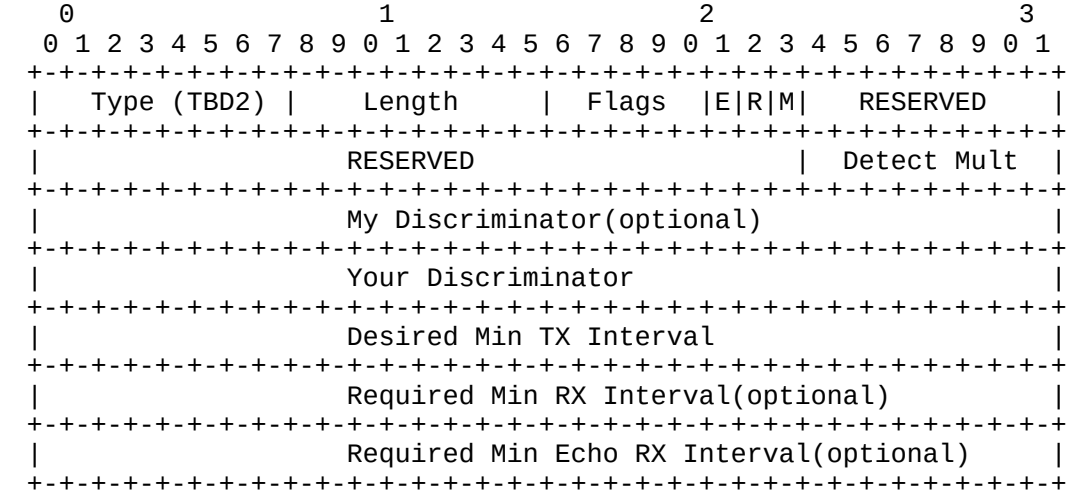

Figure 3: S-BFD Parameters Sub-TLV Format

Type: 1 octet. To be assigned by IANA from the "BGP Tunnel Encapsulation Attribute Sub-TLVs" registry (suggested value 22).

Length: 1 octet. Length of the value field in octets. The Length field reflects the total size of all fields following the Flags field, including any optional parameters that are present.

Flags: 1 octet. The Flags field indicates the presence of optional parameters in the S-BFD Parameters Sub-TLV. The following bits are defined:

M bit: Bit 0, When set, My Discriminator field is present in this Sub-TLV.

R bit: Bit 1, When set, Required Min RX Interval field is present in this Sub-TLV.

E bit: Bit 2, When set, Required Min Echo RX Interval field is present in this Sub-TLV.

Bits 3 through 7 are reserved for future use. These bits SHOULD be set to zero on transmission and MUST be ignored on receipt.

RESERVED: reserved for future use. RESERVED field SHOULD be set to zero on transmission and MUST be ignored on receipt.

Other parameters have the same meaning as defined in [RFC7880].

If present, optional parameters MUST appear in the order shown in the S-BFD Parameters Sub-TLV format.

When establishing an S-BFD session, the headend of the SR Policy acts as the S-BFD initiator and the endpoint of the SR Policy acts as the S-BFD reflector, as described in Section 3 of [RFC7880]. The Your Discriminator field identifies the S-BFD reflector instance associated with the monitored Candidate Path.

3. BGP SR Policy Speaker Behavior

A BGP SR Policy speaker that receives an SR Policy UPDATE containing BFD/S-BFD sub-TLVs MUST perform the following steps:

1. If the BFD/S-BFD sub-TLVs are malformed (e.g., length inconsistent, reserved fields non-zero), the UPDATE MUST be handled according to the "treat-as-withdraw" strategy [RFC7606].

2. If multiple BFD-related sub-TLVs (BFD Parameters, S-BFD Parameters) are present in the same UPDATE, only the first one is processed and subsequent ones MUST be ignored.

3. If the sub-TLVs are syntactically valid, the speaker MUST pass them unchanged to the SRPM together with the rest of the SR Policy CP information.

The SRPM on the headend node is responsible for interpreting the BFD/S-BFD parameters and instantiating the corresponding monitoring sessions in the data plane. If the SRPM cannot support a requested parameter (e.g., an interval value below its hardware capability), it SHOULD log an error and MAY fall back to locally configured defaults or disable BFD/S-BFD for that CP.

4. IANA Considerations

This document defines new Sub-TLVs for the BGP Tunnel Encapsulation Attribute that enable BFD/S-BFD configuration to be advertised along with SR Policy Candidate Paths.

IANA is requested to allocate two new code points in the "BGP Tunnel Encapsulation Attribute Sub-TLVs" registry:

Code Point	Description	Reference
TBD1	BFD Parameters Sub-TLV	This document
TBD2	S-BFD Parameters Sub-TLV	This document

Table 1: BGP Tunnel Encapsulation Attribute Sub-TLV Values

The suggested values are 21 for BFD Parameters Sub-TLV, 22 for S-BFD Parameters Sub-TLV.

5. Security Considerations

The security considerations of BGP [RFC4271], BGP SR Policy [RFC9830], BFD [RFC5880], and S-BFD [RFC7880] apply to this document.

Advertisements of BFD/S-BFD parameters via BGP SR Policy may expose sensitive network information, such as failure detection capabilities, session intervals, and discriminator values. These advertisements should be confined within trusted administrative domains to prevent information disclosure.

Malicious modification of BFD/S-BFD parameters in BGP SR Policy advertisements could lead to denial of service or reduced monitoring effectiveness. For example, setting extremely short intervals might

overwhelm network resources, while setting inappropriate discriminators could prevent session establishment. Implementations should validate received parameters against acceptable ranges before applying them.

Unauthorized configuration of BFD/S-BFD sessions could be used to create false failure indications or hide actual failures. Network operators should ensure that BGP SR Policy sessions carrying BFD/S-BFD configuration parameters are properly authenticated and authorized.

For BFD/S-BFD sessions established based on the parameters advertised via BGP SR Policy, the security mechanisms defined in [RFC5880] and [RFC7880] should be used to protect against session spoofing and unauthorized access. This includes using authentication where appropriate.

6. References

6.1. 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>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC7880] Pignataro, C., Ward, D., Akiya, N., Bhatia, M., and S. Pallagatti, "Seamless Bidirectional Forwarding Detection (S-BFD)", RFC 7880, DOI 10.17487/RFC7880, July 2016, <https://www.rfc-editor.org/info/rfc7880>.

[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>.

[RFC9012] Patel, K., Van de Velde, G., Sangli, S., and J. Scudder, "The BGP Tunnel Encapsulation Attribute", RFC 9012, DOI 10.17487/RFC9012, April 2021, <https://www.rfc-editor.org/info/rfc9012>.

[RFC9830] Previdi, S., Filsfils, C., Talaulikar, K., Ed., Mattes, P., and D. Jain, "Advertising Segment Routing Policies in BGP", RFC 9830, DOI 10.17487/RFC9830, September 2025, <https://www.rfc-editor.org/info/rfc9830>.

6.2. Informative References

[I-D.ietf-pce-pcep-bfd-parameters]
Fizgeer, M. and O. Bachar, "PCEP Extensions to support BFD parameters", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-bfd-parameters-01, 20 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-pcep-bfd-parameters-01>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", RFC 7606, DOI 10.17487/RFC7606, August 2015, <https://www.rfc-editor.org/info/rfc7606>.

[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>.

[RFC8664] Sivabalan, S., Filsfils, C., Tantsura, J., Henderickx, W., and J. Hardwick, "Path Computation Element Communication Protocol (PCEP) Extensions for Segment Routing", RFC 8664, DOI 10.17487/RFC8664, December 2019, <https://www.rfc-editor.org/info/rfc8664>.

[RFC9026] Morin, T., Ed., Kebler, R., Ed., and G. Mirsky, Ed., "Multicast VPN Fast Upstream Failover", RFC 9026, DOI 10.17487/RFC9026, April 2021, <https://www.rfc-editor.org/info/rfc9026>.

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

[RFC9603] Li, C., Ed., Kaladharan, P., Sivabalan, S., Koldychev, M., and Y. Zhu, "Path Computation Element Communication Protocol (PCEP) Extensions for IPv6 Segment Routing", RFC 9603, DOI 10.17487/RFC9603, July 2024, <https://www.rfc-editor.org/info/rfc9603>.

Acknowledgements

The authors would like to thank Jeffrey Haas for his helpful comments during the development of this document. The authors would also like to thank Changwang Lin from New H3C Technologies, as well as Xuhui Cai and Yunyang Lu from China Unitechs, and Zhibo Hu from Huawei, for their valuable comments and constructive suggestions that helped improve and refine this document.

Authors' Addresses

Zhenqiang Li (editor)
China Mobile
29 Finance Avenue, Xicheng District
Beijing
China
Email: lizhenqiang@chinamobile.com

Song Liu (editor)
China Mobile
10 Manbai Road, Changping District
Beijing
China
Email: liusongwl@chinamobile.com