RTGWG Working Group
Internet-Draft
Intended status: Standards Track
Expires: 27 October 2025

C. Li
Z. Hu
Huawei Technologies
Y. Zhu
China Telecom
S. Hegde
Juniper Networks Inc.

25 April 2025

# Enhanced Topology Independent Loop-free Alternate Fast Re-route
# draft-li-rtgwg-enhanced-ti-lfa-12

## Abstract

Topology Independent Loop-free Alternate Fast Re-route (TI-LFA) aims at providing protection of node and adjacency segments within the Segment Routing (SR) framework. A key aspect of TI-LFA is the FRR path selection approach establishing protection over the expected post-convergence paths from the point of local repair. However, the TI-LFA FRR path may skip the node even if it is specified in the SID list to be traveled.

This document defines Enhanced TI-LFA(TI-LFA+) by adding a No-bypass indicator for segments to ensure that the FRR route will not bypass the specific node, such as firewall. Also, this document defines No-bypass flag and No-FRR flag in SRH to indicate not to bypass nodes and not to perform FRR on all the nodes along the SRv6 path, respectively.

## 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 27 October 2025.

Table of Contents

1. Introduction . . . . . 2
2. Terminology . . . . . 3
2.1. Requirements Language . . . . . 3
3. Overview of Enhanced TI-LFA . . . . . 3
4. IGP Protocol Extensions . . . . . 4
4.1. IS-IS . . . . . 4
4.2. OSPF . . . . . 6
5. Flags in SRH . . . . . 8
5.1. No-bypass Flag in SRH . . . . . 8
5.2. No-FRR Flag in SRH . . . . . 9
6. IANA Considerations . . . . . 9
7. Security Considerations . . . . . 9
8. References . . . . . 9
8.1. Normative References . . . . . 9
8.2. Informative References . . . . . 10
Authors' Addresses . . . . . 11

## 1. Introduction

Segment Routing [RFC8402] enables to steer packets by explicitly encoding instructions in the data packets at the source node to support services like traffic engineer. Relying on SR, [I-D.ietf-rtgwg-segment-routing-ti-lfa] defines Topology Independent Loop-free Alternate Fast Re-route (TI-LFA), a local repair mechanism for IGP shortest path that capable of restoring end-to-end connectivity in the case of a sudden directly connected failure of a network component.

TI-LFA supports to establish a loop free backup path over the expected post-convergence paths from the point of local repair irrespective of the topologies used in the network, which provides a major improvment compared to LFA [RFC5286], and remote LFA [RFC7490] which cannot be applicable in some topologies [RFC6571].

However, the TI-LFA path may skip the node that the active SID points to when protecting [Adjacency, Node] segment lists. For instance, the node that a adjacency SID points to is a very important node and can not be skipped, such as a firewall node. When the link between the local repair node and firewall node fails, the packets should be steered back to the firewall and then forwarding. But in TI-LFA, if the next SID in the SID list is a node SID, the TI-LFA FRR path MAY bypass the node that the active segment points to. Also, if the firewall node is down, the packets should be dropped instead for fast reroute to bypass the node. Bypassing nodes like firewall in FRR brings issues of network security and reliability.

To enhance the security and reliability of networks, this document defines an Enhanced Topology Independent Loop-free Alternate Fast Re-route (TI-LFA+) based on TI-LFA by adding a No-bypass flag for segments to explicitly specify what node can not be bypassed. Also, this document defines No-bypass flag and No-FRR flag in SRH to indicate not to bypass nodes and not to perform FRR on all the nodes along the SRv6 path, respectively.

## 2. Terminology

This document makes use of the terms defined in [I-D.ietf-rtgwg-segment-routing-ti-lfa] and [RFC8402]. The reader is assumed to be familiar with the terminology defined in [I-D.ietf-rtgwg-segment-routing-ti-lfa] and [RFC8402].

### 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. Overview of Enhanced TI-LFA

Enhanced Topology Independent Loop-free Alternate Fast Re-route (TI-LFA+) is an enhancement of TI-LFA to explicitly indicate whether a node that segment points to can not be bypassed in FRR scenarios.

TI-LFA+ will not change the main process and algorithm of TI-LFA. Instead, in TI-LFA+, when generating repair SID list for a SID, the node should consider whether the SID endpoint can be baseed or not, which is explicitly encoded in IGP messages. If the node that segment points to can not be bypassed, then the repair SID MUST lead the packets to that node. This document defines a No-bypass flag for segments in IS-IS and OSPF. Details will be discussed in section 4.

A node should advertise two kinds of segment to meet various service policy requirements.

* Bypassing capable segment with No-bypass flag unset

* No-bypassing segment with No-bypass flag set.

A controller or control plane should choose specific segment according to the service policy.

[Editors' note] If the TI-LFA result is generated based on Locator route instead of SIDs, then the No-bypass Flag can be applied to the Locator.

Also, this document defines No-bypass flag and No-FRR flag in SRH to indicate not to bypass nodes and not to perform FRR on all the nodes along the SRv6 path, respectively. Details will be discussed in section 5.

# 4. IGP Protocol Extensions

## 4.1. IS-IS

[RFC8667] describes the necessary IS-IS extensions that need to be introduced for Segment Routing.[RFC9352] defines the IS-IS extensions required to support Segment Routing over an IPv6 data plane. This documment defines a No-bypass flag in flag filed of the following IS-IS sub-TLV/TLV.

* Prefix Segment Identifier sub-TLV (Prefix-SID sub-TLV) [RFC8667]

* Adjacency Segment Identifier sub- TLV (Adj-SID sub-TLV).[RFC8667]

* Locator entry in SRv6 Locator TLV [RFC9352]

The following figures are included here for reference and will be deleted in the future version.

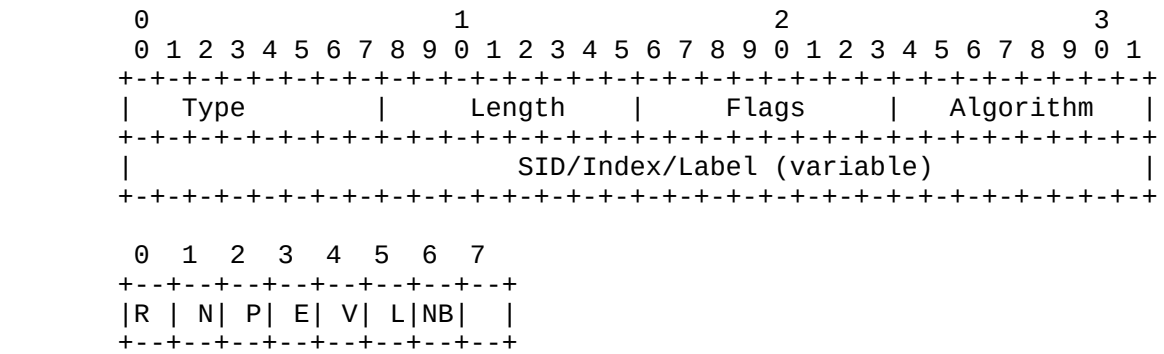



Figure 1. Prefix-SID sub-TLV and No-bypass Flag

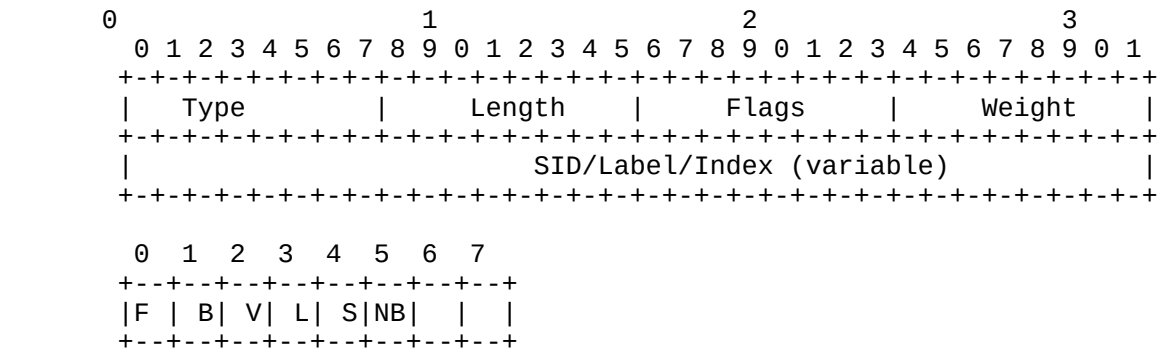



Figure 2. Adj-SID sub-TLV and No-bypass Flag

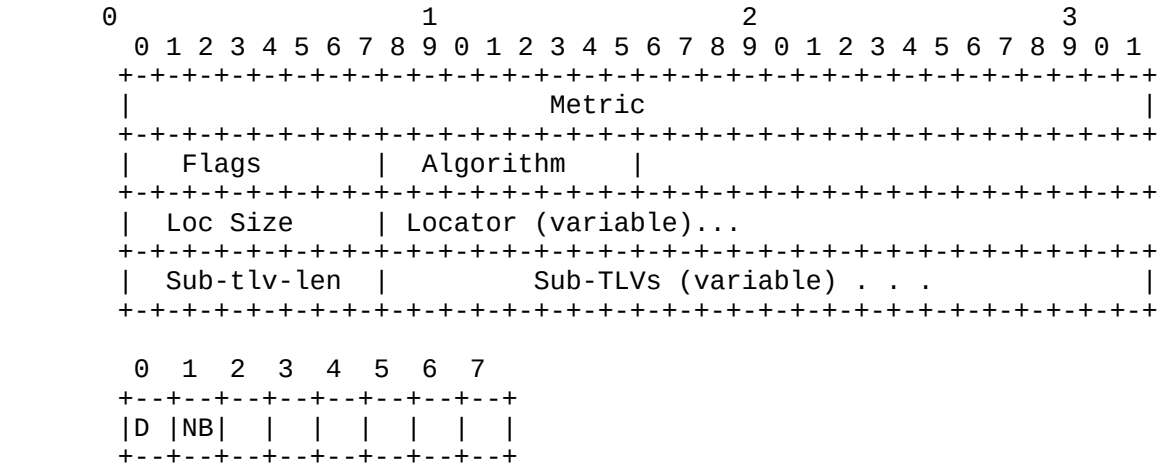



Figure 3. SRv6 Locator Entry and No-bypass Flag

If the No-bypass(NB) flag is set, means the node that the SID/Label/ Locator points to can not be bypassed. Oterwise, the node can be bypassed.

## 4.2. OSPF

[RFC8665] describes the necessary OSPF extensions that need to be introduced for Segment Routing.[RFC9513] defines the OSPF extensions required to support Segment Routing over an IPv6 data plane. This documment defines a No-bypass flag in flag filed of the following OSPF sub-TLV/TLV.

* Prefix SID Sub-TLV [RFC8665]
* Adj-SID sub-TLV [RFC8665]
* SRv6 Node SID TLV [RFC9513]
* SRv6 SID Link Attribute Sub-TLV [RFC9513]

The following figures are included here for reference and will be deleted in the future version.

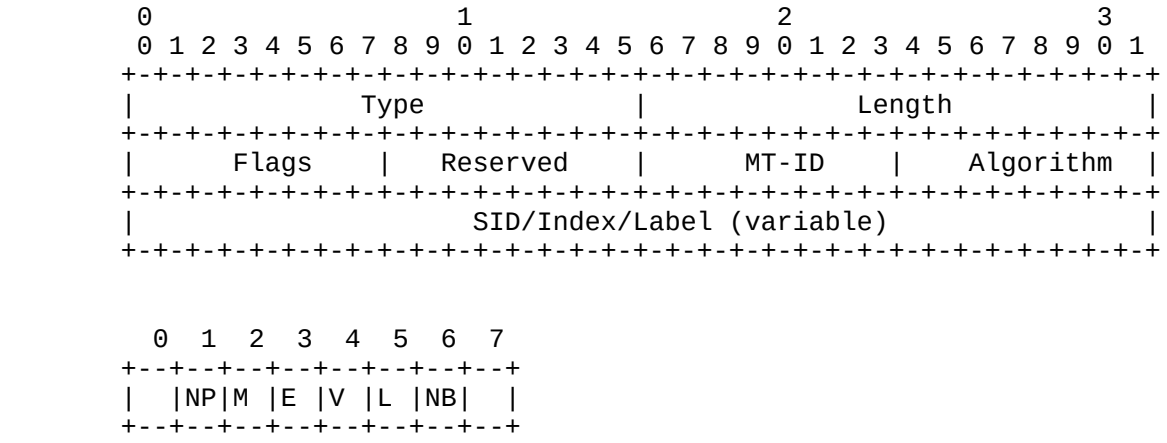
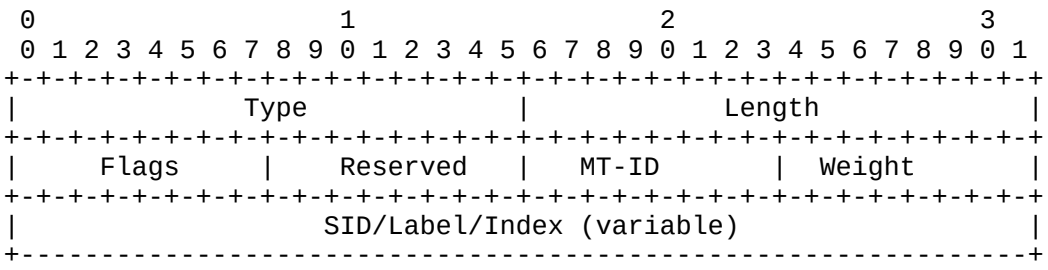



Figure 4. Prefix-SID sub-TLV and No-bypass Flag



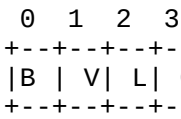
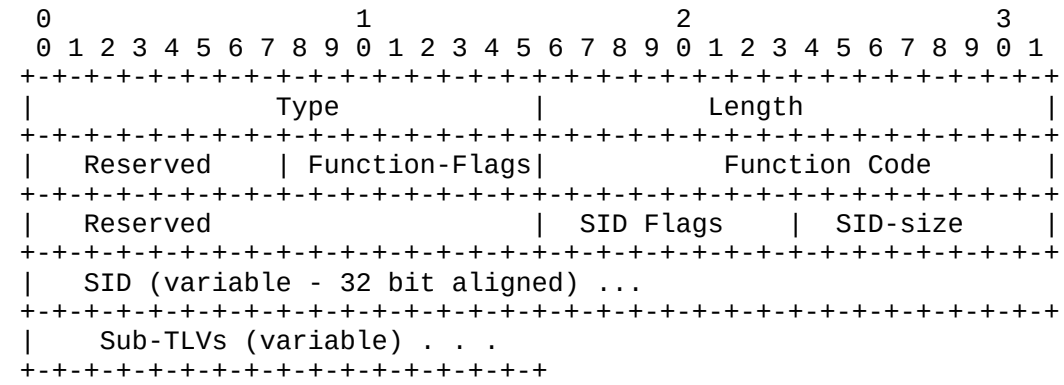




Figure 5. Adj-SID sub-TLV and No-bypass Flag



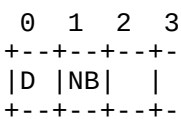
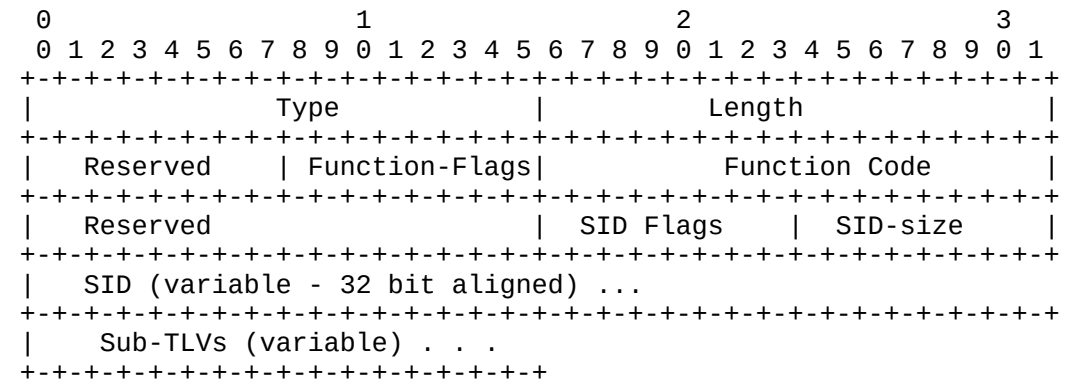




Figure 6. SRv6 Node SID TLV and No-bypass Flag



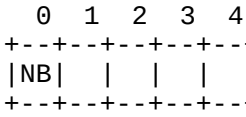




Figure 7. SRv6 Adj-SID TLV and No-bypass Flag

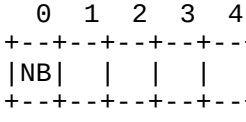
If the No-bypass(NB) flag is set, means the node that the SID/Label/ Locator points to can not be bypassed. Oterwise, the node can be bypassed.

## 5. Flags in SRH

This section describes two flags in SRH.

### 5.1. No-bypass Flag in SRH

This document defines a No-bypass Flag in SRH [RFC8754].

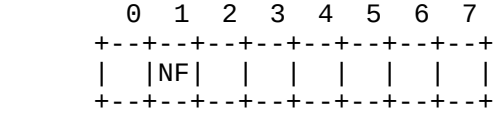



* NB Flag: No-Bypass flag, when the flag is set, the repair segment endpoint nodes MUST NOT bypass any nodes when link or node failures occur. When a link is down, the packet MUST be forwarded to the next segment endpoint node through the repair path. When the node identified by the active SID in IPv6 destination address is down, the SID can not be skipped, and the traffic MUST be forwarded to the node.

The flag can be set when the SID list containing service SIDs like firewall SID, so that the traffic will not bypass the service nodes.

### 5.2. No-FRR Flag in SRH

This document defines a No-FRR Flag in SRH [RFC8754].




* NF Flag: No-FRR flag, when the flag is set, the FRR is disable for the packet, thus the packet will not be protected by the Local protection mechanism, such as TI-LFA.

The flag can be set when the SID list containing service SIDs like firewall SID, so that the traffic will not bypass the service nodes. In this case, E2E protection mechanism should be deployed.

## 6. IANA Considerations

TBD.

## 7. Security Considerations

TBD.

## 8. References

### 8.1. 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>.

[RFC5286] Atlas, A., Ed. and A. Zinin, Ed., "Basic Specification for IP Fast Reroute: Loop-Free Alternates", RFC 5286, DOI 10.17487/RFC5286, September 2008, <https://www.rfc-editor.org/info/rfc5286>.

[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>.

[RFC7490] Bryant, S., Filsfils, C., Previdi, S., Shand, M., and N. So, "Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)", RFC 7490, DOI 10.17487/RFC7490, April 2015, <https://www.rfc-editor.org/info/rfc7490>.

[RFC6571] Filsfils, C., Ed., Francois, P., Ed., Shand, M., Decraene, B., Uttaro, J., Leymann, N., and M. Horneffer, "Loop-Free Alternate (LFA) Applicability in Service Provider (SP) Networks", RFC 6571, DOI 10.17487/RFC6571, June 2012, <https://www.rfc-editor.org/info/rfc6571>.

[I-D.ietf-rtgwg-segment-routing-ti-lfa] Bashandy, A., Litkowski, S., Filsfils, C., Francois, P., Decraene, B., and D. Voyer, "Topology Independent Fast Reroute using Segment Routing", Work in Progress, Internet-Draft, draft-ietf-rtgwg-segment-routing-ti-lfa-21, 12 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rtgwg-segment-routing-ti-lfa-21>.

[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>.

## 8.2. Informative References

[RFC4657] Ash, J., Ed. and J.L. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol Generic Requirements", RFC 4657, DOI 10.17487/RFC4657, September 2006, <https://www.rfc-editor.org/info/rfc4657>.

[RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)", RFC 8253, DOI 10.17487/RFC8253, October 2017, <https://www.rfc-editor.org/info/rfc8253>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

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

[RFC8665] Psenak, P., Ed., Previdi, S., Ed., Filsfils, C., Gredler, H., Shakir, R., Henderickx, W., and J. Tantsura, "OSPF Extensions for Segment Routing", RFC 8665, DOI 10.17487/RFC8665, December 2019, <https://www.rfc-editor.org/info/rfc8665>.

[RFC9513] Li, Z., Hu, Z., Talaulikar, K., Ed., and P. Psenak, "OSPFv3 Extensions for Segment Routing over IPv6 (SRv6)", RFC 9513, DOI 10.17487/RFC9513, December 2023, <https://www.rfc-editor.org/info/rfc9513>.

[RFC9352] Psenak, P., Ed., Filsfils, C., Bashandy, A., Decraene, B., and Z. Hu, "IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane", RFC 9352, DOI 10.17487/RFC9352, February 2023, <https://www.rfc-editor.org/info/rfc9352>.

## Authors' Addresses

Cheng Li
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing
100095
China
Email: c.l@huawei.com

Zhibo Hu
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing
100095
China
Email: huzhibo@huawei.com

Yongqing Zhu
China Telecom
Email: zhuyq8@chinatelecom.cn

Shraddha Hegde
Juniper Networks Inc.
India
Email: shraddha@juniper.net