Multiprotocol Label Switching
Internet-Draft
Intended status: Standards Track
Expires: 15 December 2025

F. Ihle
M. Menth
University of Tuebingen

13 June 2025

Stateless MNA-based Egress Protection (SMEP)
draft-ihle-mpls-mna-stateless-egress-protection-01

Abstract

The MPLS Egress Protection Framework specifies a fast reroute framework for protecting IP/MPLS services. To that end, bypass tunnels have to be signaled to the Point of Local Repair (PLR). Further, the PLR must maintain the bypass forwarding state on a per-transport-tunnel basis. This document presents the concept of Stateless MNA-based Egress Protection (SMEP). SMEP protects egress routers by providing alternative MPLS egress labels in-stack. This mechanism does not require a bypass forwarding state in PLRs. An example for the application of SMEP is given using a MPLS network action for stack management.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://uni-tue-kn.github.io/mpls-mna-stateless-egress-protection/draft-ihle-mpls-mna-stateless-egress-protection.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ihle-mpls-mna-stateless-egress-protection/.

Discussion of this document takes place on the Multiprotocol Label Switching Working Group mailing list (mailto:mpls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/mpls/. Subscribe at https://www.ietf.org/mailman/listinfo/mpls/.

Source for this draft and an issue tracker can be found at https://github.com/uni-tue-kn/mpls-mna-stateless-egress-protection.

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 15 December 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The MPLS egress protection framework in [RFC8679] establishes bypass tunnels for egress routers on an egress failure, i.e., on a node or a link failure. This is referred to as egress protection. The protection mechanism relies on a Point of Local Repair (PLR) to perform local failure detection and local repair. Typically, this PLR is the penultimate router. When an egress failure occurs, packets are rerouted to an alternative egress router. The PLR node maintains the bypass forwarding state, which is a mapping of specific labels to bypass tunnels. The bypass tunnels are signaled using existing mechanisms, i.e., via an IGP, or topology-driven label distribution protocols such as LDP.

This document defines the concept of Stateless MNA-based Egress Protection (SMEP). SMEP provides an alternative to the rerouting mechanism defined for the PLR, allowing the PLR to be stateless.

1.1. Terminology

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.

1.1.1. Abbreviations

This document makes use of the terms defined in [RFC8679] and in [I-D.ietf-mpls-mna-hdr].

Further abbreviations used in this document:

Abbreviation	Meaning	Reference
BML	Bypass MPLS Label	This document
SMEP	Stateless MNA-based Egress Protection	This document

Table 1: Abbreviations.

2. Concept of SMEP

With SMEP, the egress bypass tunnel is indicated by one or multiple alternative MPLS forwarding labels which are located at the bottom of stack. We call those labels Bypass MPLS Labels (BMLs). On an egress failure, SMEP uses the BMLs in the stack to protect the egress tunnel. The PLR node is required to install the MPLS forwarding entries for the bypass tunnels using the BMLs. However, it does not need to maintain a table that maps transport tunnels to backup paths. Likewise, the PLR is not involved in the signaling of such information. Instead, this information is supplied in the MPLS stack from the ingress node to the PLR. Signaling is only needed between ingress, egress, and the protector, but not with the PLR anymore. Details of the signaling are not contained in this draft. The general concepts and mechanisms described in [RFC8679] still apply.

3. Stack Management with POP-N-LSE Operation Network Action for SMEP

The MPLS Network Action (MNA) framework encodes network actions and their data for processing by MPLS nodes. [I-D.ietf-mpls-mna-hdr] defines the encoding of such network actions and their data in so-called Network Action Substacks (NAS) in the MPLS stack.

[I-D.ihle-mpls-mna-stack-management-00] introduces a network action for stack management. It features a POP-N-LSE operation that pops a number POP-N of LSEs below the NAS. The POP-N-LSE operation facilitates the application of SMEP. To that end, the POP-N-LSE operation is added directly above the BMLs where POP-N is the number of labels in the bypass tunnel. The processing at the PLR is as follows:

1. If the PLR does not detect an egress failure
    * The PLR executes the POP-N-LSE action and pops all BMLs.
    * The packet is forwarded as usual to the egress node.
2. If the PLR detects an egress failure
    * The POP-N-LSE action is ignored and is popped along with the top-of-stack label.
    * The BML is now the top-of-stack label. The packet is forwarded to the protector based on the BML.

4. Example

A simple example topology using MNA-based egress protection with an SR bypass tunnel is shown in Figure 1. The example network contains an LSP R1-R2-R3 and a bypass tunnel R2-R3'-R3''.

The MPLS stack using SMEP pushed by the ingress LER for the example topology is shown in Figure 2. The label stack contains the forwarding labels L1, L2, L3, L3', and L3'', and the POP-N-LSE operation destined for the PLR. Since there are two BMLs to reach the protector, POP-N = 2. Labels L1 and L2 are used to forward to the penultimate router. Label L3 is used to route to the egress node, and labels L3' and L3'' are used to route to the protector. If the egress link or router R3 fails, the PLR can use the bypass tunnel of router R3' and R3''.

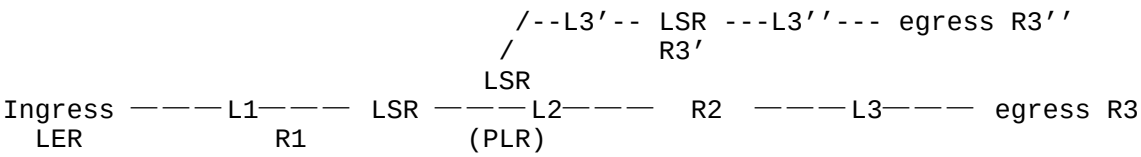

Figure 1: Example using the POP-N-LSE operation for SMEP.

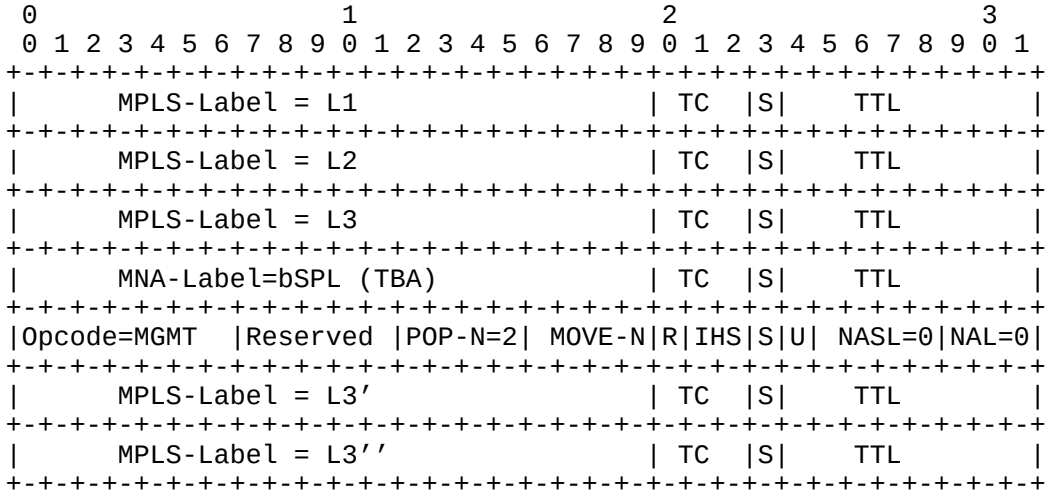

Figure 2: MPLS stack pushed by the ingress LER.

If there is no egress failure, the LSR R2 executes the POP-N-LSE action with POP-N = 2 and pops the BMLs L3' and L3''. R2 pops the top-of-stack label L3 and forwards the packet as usual to the egress.

If the LSR R2 detects an egress failure, it becomes the PLR. The POP-N-LSE action is ignored and the NAS is popped along with the top-of-stack label. This stack is shown in Figure 1. This time, the BMLs L3' and L3'' are at the top-of-stack. The packet is forwarded according to those labels to the alternative egress node R3''.

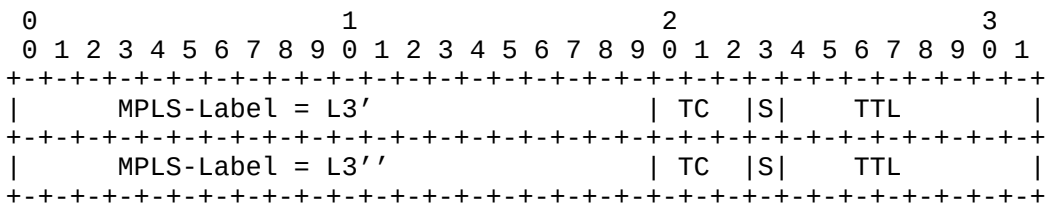

Figure 3: MPLS stack at the PLR on egress failure.

5. Security Considerations

The security issues discussed in [I-D.ietf-mpls-mna-hdr] and in [RFC8679] apply to this document.

6. IANA Considerations

This document makes no request of IANA.

7. References

7.1. 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/rfc/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/rfc/rfc8174>.

7.2. Informative References

[I-D.ietf-mpls-mna-hdr] Rajamanickam, J., Gandhi, R., Zigler, R., Song, H., and K. Kompella, "MPLS Network Action (MNA) Sub-Stack Solution", Work in Progress, Internet-Draft, draft-ietf-mpls-mna-hdr-12, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-mna-hdr-12>.

[I-D.ihle-mpls-mna-stack-management-00]
Ihle, F. and M. Menth, "MPLS Network Action for Stack Management", Work in Progress, Internet-Draft, draft-ihle-mpls-mna-stack-management-00, 13 June 2025, <https://datatracker.ietf.org/doc/html/draft-ihle-mpls-mna-stack-management-00>.

[RFC8679] Shen, Y., Jeganathan, M., Decraene, B., Gredler, H., Michel, C., and H. Chen, "MPLS Egress Protection Framework", RFC 8679, DOI 10.17487/RFC8679, December 2019, <https://www.rfc-editor.org/rfc/rfc8679>.

Authors' Addresses

Fabian Ihle
University of Tuebingen
Tuebingen
Germany
Email: fabian.ihle@uni-tuebingen.de

Michael Menth
University of Tuebingen
Tuebingen
Germany
Email: michael.menth@uni-tuebingen.de