

MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 14 November 2025

T. Li
Juniper Networks
J. Drake

V. P. Beeram
Juniper Networks
T. Saad
Cisco Systems
I. Meilik
Broadcom
13 May 2025

MPLS Network Actions for Network Resource Partition Selector
draft-ietf-mpls-mna-nrp-selector-00

Abstract

An IETF Network Slice service provides connectivity coupled with a set of network resource commitments and is expressed in terms of one or more connectivity constructs. A Network Resource Partition (NRP) is a collection of resources identified in the underlay network to support IETF Network Slice services. A Slice-Flow Aggregate refers to the set of traffic streams from one or more connectivity constructs belonging to one or more IETF Network Slices that are mapped to a specific NRP and provided the same forwarding treatment. The packets associated with a Slice-Flow Aggregate may carry a marking in the packet's network layer header to identify this association and this marking is referred to as NRP Selector. The NRP Selector is used to map the packet to the associated NRP and provide the corresponding forwarding treatment to the packet.

MPLS Network Actions (MNA) technologies are used to indicate actions for Label Switched Paths (LSPs) and/or MPLS packets and to transfer data needed for these actions. This document discusses options for using MPLS Network Actions (MNAs) to carry the NRP Selector in MPLS packets.

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 14 November 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	2
1.1. Requirements Language	3
2. MPLS Network Actions	3
2.1. 13-bit NRP Selector (NRPS13) Action	4
2.2. 20-bit NRP Selector (NRPS20) Action	4
2.3. 20-bit Entropy and NRP Selector (ENRPS20) Action	5
3. IANA Considerations	5
3.1. 13-bit NRP Selector Action	5
3.2. 20-bit NRP Selector Action	6
3.3. 20-bit Entropy and NRP Selector Action	6
4. Security Considerations	6
5. Contributors	6
6. References	6
6.1. Normative References	6
6.2. Informative References	7
Authors' Addresses	8

1. Introduction

An IETF Network Slice [RFC9543] service provides connectivity coupled with a set of specific commitments of network resources between a number of endpoints over a shared underlay network. The IETF Network Slice service is expressed in terms of one or more connectivity constructs. A Network Resource Partition (NRP) [RFC9543] is a collection of resources identified in the underlay network to support

IETF Network Slice services (or any other services that need logical network structures with required characteristics to be created). An NRP Policy [I-D.ietf-teas-ns-ip-mpls] is a policy construct that enables instantiation of mechanisms in support of service specific control and data plane behaviors on select topological elements associated with the NRP.

A Slice-Flow Aggregate refers to the set of traffic streams from one or more connectivity constructs belonging to one or more IETF Network Slices that are mapped to a specific NRP and are provided the same forwarding treatment. The NRP policy dictates the identification of the flow aggregate that the packet belongs to and the corresponding forwarding treatment that needs to be applied to the packet. The packets associated with a Slice-Flow Aggregate may carry a marking in the packet's network layer header to identify this association and this marking is referred to as NRP Selector (NRPS).

[I-D.ietf-teas-ns-ip-mpls] discusses a few options for carrying the NRP Selector in MPLS packets, including overloading the semantics of forwarding/service labels and using a dedicated identifier field.

[I-D.ietf-mpls-mna-fwk] specifies an architectural framework for the MPLS Network Actions (MNA) technologies. MNA technologies are used to indicate actions for Label Switched Paths (LSPs) and/or MPLS packets and to transfer data needed for these actions. The MNA architecture can facilitate carrying the dedicated identifier based NRP Selector in the MPLS label stack. This document discusses a few options for using MPLS network actions to carry the NRP Selector. The proposed encodings are compliant with the MNA header encoding formats defined in [I-D.ietf-mpls-mna-hdr].

The reader is expected to be familiar with terminology specified in [I-D.ietf-mpls-mna-fwk] and MNA header encoding formats defined in [I-D.ietf-mpls-mna-hdr].

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. These words may also appear in this document in lower case as plain English words, absent their normative meanings.

2. MPLS Network Actions

2.1. 13-bit NRP Selector (NRPS13) Action

The format of the 13-bit NRP Selector (NRPS13) Action (when encoded in the second label stack entry in the Network Action Sub-Stack):

```

 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Opcode=TBA1 |           NRPS                |R|IHS|S| Res |U|  NASL |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- * Name: 13-bit NRP Selector (NRPS13) Action
- * Network Action Indication: The NRPS13 Action indication is opcode TBA1.
- * Scope: The NRPS13 Action is valid in all scopes.
- * In-Stack Data: The NRPS13 Action carries 13 bits of ancillary data. The NRPS is encoded in the 13 bits. The packet carrying the NRPS13 action should be given the forwarding treatment specified by the associated policy.
- * LSE Format: B.
- * Post-Stack Data: None.

2.2. 20-bit NRP Selector (NRPS20) Action

The format of the 20-bit NRP Selector (NRPS20) Action:

```

 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Opcode=TBA2 |           NRPS                |S| NRPS |  NAL  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- * Name: 20-bit NRP Selector (NRPS20) Action
- * Network Action Indication: The NRPS20 Action indication is opcode TBA2.
- * Scope: The NRPS20 Action is valid in all scopes.
- * In-Stack Data: The NRPS20 Action carries 20 bits of ancillary data. The NRPS is encoded in the 20 bits. The packet carrying the NRPS20 action should be given the forwarding treatment specified by the associated policy.

- * LSE Format: C. The Network Action Length (NAL) field SHOULD be transmitted as zero.
- * Post-Stack Data: None.

2.3. 20-bit Entropy and NRP Selector (ENRPS20) Action

The format of the 20-bit Entropy and NRP Selector (ENRPS20) Action:

```

 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Opcode=TBA3|          Entropy          | NRPS |S| NRPS |  NAL  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

- * Name: 20-bit Entropy and NRP Selector (ENRPS20) Action
- * Network Action Indication: The ENRPS20 Action indication is opcode TBA3.
- * Scope: The ENRPS20 Action is valid in all scopes.
- * In-Stack Data: The ENRPS20 Action carries 20 bits of ancillary data. The most significant 12 bits of ancillary data is the Entropy Value. The least significant 8 bits of ancillary data is the NRPS. The Entropy Value has semantics consistent with the Entropy Label [RFC6790]. While the RFC 6790 Entropy Label has some restrictions to avoid collisions with the reserved label space (0-15) [RFC3032], those restrictions are not necessary for the Entropy Value and do not apply. The packet carrying the ENRPS20 action should be given the forwarding treatment specified by the associated policy.
- * LSE Format: C. The Network Action Length (NAL) field SHOULD be transmitted as zero.
- * Post-Stack Data: None.

3. IANA Considerations

3.1. 13-bit NRP Selector Action

This document requests that IANA allocate a codepoint (TBA1) from the "Multiprotocol Label Switching Architecture (MPLS)"/"MPLS Network Actions Parameters"/"Network Action Opcodes" registry for the 13-bit NRP Selector Action. The allocation should reference this document.

3.2. 20-bit NRP Selector Action

This document requests that IANA allocate a codepoint (TBA2) from the "Multiprotocol Label Switching Architecture (MPLS)"/"MPLS Network Actions Parameters"/"Network Action Opcodes" registry for the 20-bit NRP Selector Action. The allocation should reference this document.

3.3. 20-bit Entropy and NRP Selector Action

This document requests that IANA allocate a codepoint (TBA3) from the "Multiprotocol Label Switching Architecture (MPLS)"/"MPLS Network Actions Parameters"/"Network Action Opcodes" registry for the 20-bit Entropy and NRP Selector Action. The allocation should reference this document.

4. Security Considerations

The forwarding plane is insecure. If an adversary can affect the forwarding plane, then they can inject data, remove data, corrupt data, or modify data. MNA additionally allows an adversary to make packets perform arbitrary network actions.

Link-level security mechanisms can help mitigate some on-link attacks, but does nothing to preclude hostile nodes.

5. Contributors

The following individuals contributed to this document:

Colby Barth
Juniper Networks
Email: cbarth@juniper.net

Srihari R. Sangli
Juniper Networks
Email: ssangli@juniper.net

Chandra Ramachandran
Juniper Networks
Email: csekar@juniper.net

Kireeti Kompella
Juniper Networks
Email: kireeti@juniper.net

6. References

6.1. Normative References

[I-D.ietf-mppls-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-mppls-mna-hdr-12, 3 March 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-mppls-mna-hdr-12>>.

- [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>>.

- [RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, DOI 10.17487/RFC3032, January 2001, <<https://www.rfc-editor.org/info/rfc3032>>.

- [RFC6790] Kompella, K., Drake, J., Amante, S., Henderickx, W., and L. Yong, "The Use of Entropy Labels in MPLS Forwarding", RFC 6790, DOI 10.17487/RFC6790, November 2012, <<https://www.rfc-editor.org/info/rfc6790>>.

- [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>>.

6.2. Informative References

[I-D.ietf-mppls-mna-fwk]

Andersson, L., Bryant, S., Bocci, M., and T. Li, "MPLS Network Actions (MNA) Framework", Work in Progress, Internet-Draft, draft-ietf-mppls-mna-fwk-15, 27 December 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-mppls-mna-fwk-15>>.

- [RFC9543] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "A Framework for Network Slices in Networks Built from IETF Technologies", RFC 9543, DOI 10.17487/RFC9543, March 2024, <<https://www.rfc-editor.org/info/rfc9543>>.

[I-D.ietf-teas-ns-ip-mppls]

Saad, T., Beeram, V. P., Dong, J., Halpern, J. M., and S. Peng, "Realizing Network Slices in IP/MPLS Networks", Work in Progress, Internet-Draft, draft-ietf-teas-ns-ip-mppls-05, 2 March 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-teas-ns-ip-mppls-05>>.

Authors' Addresses

Tony Li
Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
United States
Email: tony.li@tony.li

John Drake
Email: je_drake@yahoo.com

Vishnu Pavan Beeram
Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
United States
Email: vbeeram@juniper.net

Tarek Saad
Cisco Systems
Email: tsaad.net@gmail.com

Israel Meilik
Broadcom
Email: israel.meilik@broadcom.com