MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 6 November 2026

T. Li
V. P. Beeram
HPE
J. Drake

T. Saad
Cisco Systems
I. Meilik
Broadcom

5 May 2026

MPLS Network Actions for Network Resource Partition Selector
draft-ietf-mpls-mna-nrp-selector-06

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 provide the same forwarding treatment. The packets associated with a Slice-Flow Aggregate may carry markings in the packet’s network layer header to identify this association and each is referred to as NRP Selector. The NRP Selector is used to map the packet to the associated NRP and provides 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 specifies 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/.

Copyright Notice

Table of Contents

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], Section 7) 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 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. This is also discussed in [I-D.ietf-teas-ns-ip-mpls].

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 markings in the packet’s network layer header to identify this association and each 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.

[RFC9789] 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. These 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 the terminology specified in [RFC9789] 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

The MNA Label Stack Entries (LSEs) in the following subsections use the format and fields defined in [I-D.ietf-mpls-mna-hdr], Section 4, with no change to their meanings. Only the Ancillary Data is modified to carry the NRPS Selector as described in each of the subsections.

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) is:

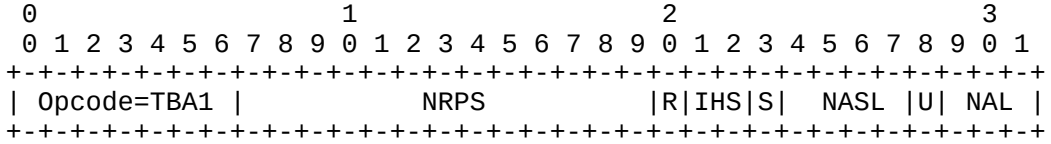

Figure 1: A 13-bit NRP Selector in a Format B LSE

This complies with MNA LSE Format B ([I-D.ietf-mpls-mna-hdr], Section 4.2). The fields are:

* Opcode: The MNA Opcode (TBA1). See [I-D.ietf-mpls-mna-hdr], Section 5.1.

* NRPS: Network Resource Partition Selector. If this is the top-most NRPS in the label stack, the packet carrying the NRPS13 action is to be given the forwarding treatment specified by the associated NRP policy. See [I-D.ietf-teas-ns-ip-mpls], Section 5.1.1.

* R: Reserved. See [I-D.ietf-mpls-mna-hdr], Section 4.2.

* IHS: The Scope of the NAS. See [I-D.ietf-mpls-mna-hdr], Section 5.3.

* S: The Bottom of Stack. [RFC3032]

* NASL: The Network Action Sub-Stack Length (NASL). See [I-D.ietf-mpls-mna-hdr], Section 4.2.

* U: Unknown Network Action Handling. See [I-D.ietf-mpls-mna-hdr], Section 5.4.

* NAL: Network Action Length. See [I-D.ietf-mpls-mna-hdr], Section 4.2.

Each Network Action is required to specify the following by [I-D.ietf-mpls-mna-hdr]:

* Format: LSE Format B

* Scope: The NRPS13 Action is valid in all scopes.

* Ancillary Data: The NRPS13 Action carries 13 bits of ancillary data. The NRPS is encoded in 13 bits.

* Processing: If this is the top-most NRPS in the label stack, the packet carrying the NRPS13 action is to be given the forwarding treatment specified by the associated NRP policy.

* Interactions: None

2.2. 20-bit NRP Selector (NRPS20) Action

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

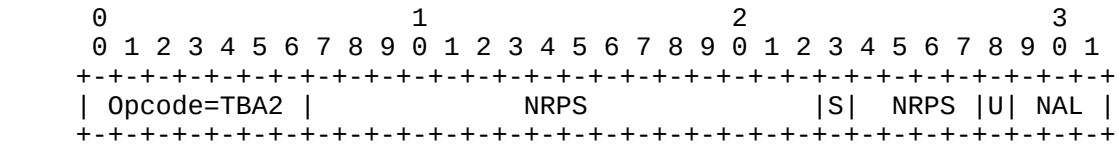

Figure 2: A 20-bit NRP Selector in a Format C LSE

This complies with MNA LSE Format C ([I-D.ietf-mpls-mna-hdr], Section 4.3). The fields are:

* Opcode: The MNA Opcode (TBA2). See [I-D.ietf-mpls-mna-hdr], Section 5.1.

* NRPS: Network Resource Partition Selector. This field is intentionally split across the S bit. If this is the top-most NRPS in the label stack, the packet carrying the NRPS20 action is

to be given the forwarding treatment specified by the associated NRP policy. See [I-D.ietf-mpls-mna-hdr], Section 4.3 and [I-D.ietf-teas-ns-ip-mpls], Section 5.1.1.

* S: The Bottom of Stack. [RFC3032]

* U: Unknown Network Action Handling. See [I-D.ietf-mpls-mna-hdr], Section 5.4.

* NAL: Network Action Length. See [I-D.ietf-mpls-mna-hdr], Section 4.3.

Each Network Action is required to specify the following by [I-D.ietf-mpls-mna-hdr]:

* Format: LSE Format C

* Scope: The NRPS20 Action is valid in all scopes.

* Ancillary Data: The NRPS20 Action carries 20 bits of ancillary data. The NRPS is encoded in the 20 bits.

* Processing: If this is the top-most NRPS in the label stack, the packet carrying the NRPS20 action is to be given the forwarding treatment specified by the associated NRP policy.

* Interactions: None

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

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

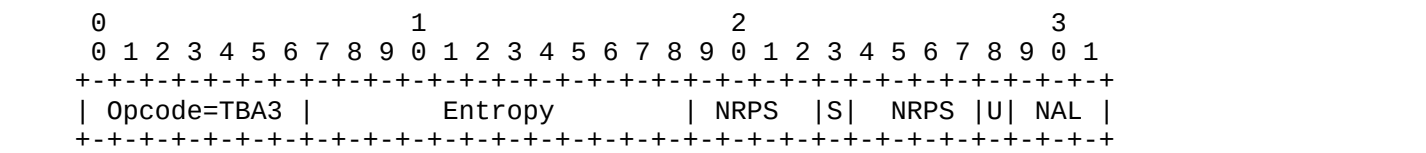

Figure 3: A 12-bit Entropy Value and an 8-bit NRP Selector in a Format C LSE

This complies with MNA LSE Format C ([I-D.ietf-mpls-mna-hdr], Section 4.3). The fields are:

* Opcode: The MNA Opcode (TBA3). See [I-D.ietf-mpls-mna-hdr], Section 5.1.

* Entropy: A 12-bit Entropy Value. 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 selection of the Opcode ensures that this cannot be mistaken for a reserved label.

* NRPS: Network Resource Partition Selector. This field is intentionally split across the S bit. If this is the top-most NRPS in the label stack, the packet carrying the ENRPS20 action is to be given the forwarding treatment specified by the associated NRP policy. See [I-D.ietf-mpls-mna-hdr], Section 4.3 and [I-D.ietf-teas-ns-ip-mpls], Section 5.1.1.

* S: The Bottom of Stack. [RFC3032]

* U: Unknown Network Action Handling. See [I-D.ietf-mpls-mna-hdr], Section 5.4.

* NAL: Network Action Length. See [I-D.ietf-mpls-mna-hdr], Section 4.3.

Each Network Action is required to specify the following by [I-D.ietf-mpls-mna-hdr]:

* Format: LSE Format C

* Scope: The ENRPS20 Action is valid in all scopes.

* Ancillary 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.

* Processing: 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 selection of the Opcode ensures that this cannot be mistaken for a reserved label. If this is the top-most NRPS in the label stack, the packet carrying the ENRPS20 action is to be given the forwarding treatment specified by the associated NRP policy.

* Interactions: None

2.4. Top-most NRPS Action

Multiple NRPS Actions MAY be encoded in a single packet. An implementation MUST use only the top-most NRPS Action to determine the packet's forwarding treatment. An implementation that finds a subsequent opcode of any of the three NRPS Actions in the label stack MUST ignore it. The specific scenarios where multiple NRPS Actions are present in the label stack are outside the scope of this document. See [I-D.ietf-teas-ns-ip-mpls].

2.5. Unknown NRPS

An NRP-capable node SHOULD drop a packet by default if the encoded NRPS cannot be mapped to a known NRP. This requirement MAY be overridden by an operator-specified policy, the specification of which is outside the scope of this document. See [I-D.ietf-teas-ns-ip-mpls] for more details.

3. Operational Considerations

MNA In-stack operational considerations are discussed in [I-D.ietf-mpls-mna-hdr], Section 13.

The choice of the number of bits to encode an NRP Selector is a network-wide deployment decision. This decision may be constrained by implementations.

The choice of which Action to use when the NRP Selector could fit in multiple Actions is open, but it is RECOMMENDED to use NRPS13 where possible unless Entropy is also to be carried and it is possible to use ENRPS20.

4. IANA Considerations

4.1. 13-bit NRP Selector Action

This document requests that IANA allocate a codepoint (TBA1) from the "Network Action Opcodes" registry in the "MPLS Network Actions" group [NAO] for the 13-bit NRP Selector Action. The allocation should reference this document with the description " 13-bit NRP Selector".

4.2. 20-bit NRP Selector Action

This document requests that IANA allocate a codepoint (TBA2) from the "Network Action Opcodes" registry in the "MPLS Network Actions" group [NAO] for the 20-bit NRP Selector Action. The allocation should reference this document with the description "20-bit NRP Selector".

4.3. 20-bit Entropy and NRP Selector Action

This document requests that IANA allocate a codepoint (TBA3) from the "Network Action Opcodes" registry in the "MPLS Network Actions" group [NAO] for the 20-bit Entropy and NRP Selector Action. The allocation should reference this document with the description "20-bit Entropy and NRP Selector".

5. 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.

Unauthorized use of an NRPS can lead to traffic receiving unintended resource treatment and/or disclosure of network policies.

Further security considerations can be found in [I-D.ietf-teas-ns-ip-mpls], [I-D.ietf-mpls-mna-hdr], Section 12 and [RFC9789], Section 7.

6. 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

7. References

7.1. Normative References

[I-D.ietf-mpls-mna-hdr]
Rajamanickam, J., Gandhi, R., Zigler, R., Song, H., and K. Kompella, "MPLS Network Action (MNA) Sub-Stack Specification including In-Stack Network Actions and Data", Work in Progress, Internet-Draft, draft-ietf-mpls-mna-hdr-21, 24 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-mna-hdr-21>.

[I-D.ietf-teas-ns-ip-mpls]
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-mpls-07, 28 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ns-ip-mpls-07>.

[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>.

[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>.

[RFC9789] Andersson, L., Bryant, S., Bocci, M., and T. Li, "MPLS Network Actions (MNAs) Framework", RFC 9789, DOI 10.17487/RFC9789, July 2025, <https://www.rfc-editor.org/info/rfc9789>.

7.2. Informative References

[NAO] "MPLS Network Actions, Network Action Opcodes", May 2026, <https://www.iana.org/assignments/mpls-network-actions/mpls-network-actions.xhtml#network-action-opcodes>.

Authors' Addresses

Tony Li
HPE
1701 E Mossy Oaks Rd.
Spring, TX 77389
United States
Email: tony.li@tony.li

Vishnu Pavan Beeram
HPE
1701 E Mossy Oaks Rd.
Spring, TX 77389
United States
Email: vbeeram@juniper.net

John Drake
Email: je_drake@yahoo.com

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

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