Stream:	Internet Engineering Task Force (IETF)		
RFC:	9613		
Category:	Informational		
Published:	August 2024		
ISSN:	2070-1721		
Authors:	M. Bocci, Ed.	S. Bryant	J. Drake
	Nokia	*University of Surrey ICS*	*Independent*

RFC 9613
Requirements for Solutions that Support MPLS Network Actions (MNAs)

Abstract

This document specifies requirements for the development of MPLS Network Actions (MNAs) that affect the forwarding or other processing of MPLS packets. These requirements are informed by a number of proposals for additions to the MPLS information in the labeled packet to allow such actions to be performed, either by a transit or terminating Label Switching Router (i.e., the Label Edge Router - LER).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9613.

Copyright Notice

Table of Contents

1. Introduction

There is significant interest in developing the MPLS data plane to address the requirements of new use cases [MNA-USECASES]. This requires a general mechanism, termed MPLS Network Actions (MNAs), to allow the network to make a forwarding or processing decision based on information other than the top label and Traffic Class (TC) bits, and to also make use of the Network Action Indicator (NAI) and ancillary data (MNA information). These use cases require the definition of extensions to the MPLS architecture and label-stack operations that can be used across these use cases in order to minimize implementation complexity and promote interoperability and extensibility. These protocol extensions need to conform to the existing MPLS architecture as specified by [RFC3031], [RFC3032], and [RFC6790].

Note that the MPLS architecture specified in [RFC3031] describes a mechanism for forwarding MPLS packets through a network without requiring any analysis of the MPLS packet payload's network layer header by intermediate nodes (Label Switching Routers - LSRs). Formally, inspection may only occur at network ingress (the Label Edge Router - LER) where the MPLS packet is assigned to a Forwarding Equivalence Class (FEC).

This document specifies the requirements for solutions that encode MNAs and ancillary data that may be needed to process those actions. These requirements are informed by a number of proposals to allow additions to the MPLS information in the labeled packet so that such actions can be performed, either by a transit or terminating LSR. It is anticipated that these will result in two types of solution specifications:

MNA solution specification: A specification that describes a common protocol that supports all forms of MNAs.

Network Action solution specifications: One or more specifications describing the protocol extensions for the MNA solution to address a use case.

The term 'solutions', in isolation, refers to both MNA and Network Action solutions. The requirements constrain the MNA solution design to enable interoperability between implementations.

1.1. Terminology

Network Action (NA): An operation to be performed on an MPLS packet or as a consequence of an MPLS packet being processed by a router. An NA may affect router state or MPLS packet forwarding, or it may affect the MPLS packet in some other way.

Network Action Indicator (NAI): An indication in the MPLS packet that a certain NA is to be performed.

Ancillary Data (AD): Data in an MPLS packet associated with a given NA that may be used as input to process the NA or may result from processing the NA. Ancillary data may be associated with:

- Both the control or maintenance information and the data traffic carried by the Label Switched Path (LSP).
- Only the control or maintenance information.
- Only the data traffic carried by the LSP.

In-Stack Data: Ancillary data carried within the MPLS label stack.

Post-Stack Data: Ancillary data carried in an MPLS packet between the bottom of the MPLS label stack and the first octet of the user payload. This document does not prescribe whether post-stack data precedes or follows any other post-stack header such as a Control Word or Associated Channel Header (ACH).

Scope: The set of nodes that should perform a given action.

2. 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.

Although this document is not a protocol specification, this convention is adopted for clarity of description of requirements.

3. MPLS Network Action Requirements

This document specifies requirements on MNAs and the technology to support them in MPLS, such as NAIs, the associated AD, and the alert mechanism to indicate to an LSR that NAIs are present in an MPLS packet.

The requirements are for the behavior of the protocol mechanisms and procedures that constitute building blocks out of which indicators for a NA and associated ancillary data are constructed. It does not specify the detailed actions and processing of any NAs or ancillary data by an LSR or LER.

The size of the ancillary data carried post-stack end to end in an MPLS packet is a matter for agreement between the ingress and egress provider edges (PEs), and is not part of these requirements. Since in-stack ancillary data and per-hop post-stack data need to be parsed and processed by transit LSRs along the Label Switched Path (LSP), requirements on the size of such ancillary data are documented in the following sections.

3.1. General Requirements

1. Any solutions **MUST** maintain the properties of extensibility, flexibility, and efficiency inherent in the split between the control plane context and simple data plane used in MPLS and the specification **SHOULD** describe how this is achieved.
2. Any solutions to these requirements **MUST** be based on and **MUST NOT** restrict the generality of the MPLS architecture [RFC3031] [RFC3032] [RFC5331].
3. If extensions to the MPLS data plane are required, they **MUST** be consistent with the MPLS architecture [RFC3031] [RFC3032] [RFC5331].
4. Solutions meeting the requirements set out in this document **MUST** be able to coexist with existing MPLS mechanisms.
5. Subject to the constraints in these requirements, a Network Action solution **MAY** carry MNA information in-stack, post-stack, or both in-stack and post-stack.
6. Solution specifications **MUST NOT** require an implementation to support in-stack ancillary data, unless the implementation chooses to support an NA that uses in-stack ancillary data.

7. Solution specifications **MUST NOT** require an implementation to support post-stack ancillary data, unless the implementation chooses to support an NA that uses post-stack ancillary data.
8. The design of any MNA solution **MUST** minimize the amount of processing required to parse the label stack at an LSR.
9. Solutions **MUST** minimize any additions to the size of the MPLS label stack.
10. Solution specifications that increase the size of the MPLS label stack in a way that is not controlled by the ingress LER **MUST** discuss the consequences.
11. Solution specifications **MUST** discuss the ECMP consequences of the design.
12. A Network Action solution **MUST NOT** expose information to the LSRs that is not already exposed to the LER.
13. The design of any NA **MUST NOT** expose any information that a user of any service using the LSP considers confidential [RFC6973] [RFC3552].
14. Solution specifications **MUST** document any new security considerations that they introduce.
15. An MNA solution **MUST** allow MPLS packets carrying NAI and ancillary data (where it exists) to coexist with MPLS packets that do not carry this information on the same LSP.

3.2. Requirements on the MNA Alert Mechanism

16. An MNA solution specification **MUST** define how a node determines whether NAIs are present in the MPLS packet.
17. Special Purpose Labels (SPLs) are a mechanism of last resort; therefore, an MNA solution specification that defines their use **MUST** minimize the number of new SPLs that are allocated.

3.3. Requirements on Network Actions

18. It is **RECOMMENDED** that an MNA solution include support for NAs for Private Use (see Section 4.1 of [RFC8126]).
19. Network Action solution specifications **MUST** define if the NA needs to be processed as a part of the immediate forwarding operation and whether MPLS packet misordering is allowed to occur as a result of the time taken to process the NA.
20. If a Network Action solution specification allows more than one scope for an NA, it **MUST** define a mechanism to indicate the precedence of the scopes or any combination of the scopes.
21. If a network action requires an NAI with in-stack ancillary data that needs to be imposed at an LSR on an LSP, then the Network Action solution **MUST** specify how this is achieved in all circumstances.
22. If a network action requires an NAI with post-stack ancillary data to be imposed at an LSR on an LSP, then the Network Action solution specification **MUST** describe how this is achieved in all circumstances.

3.4. Requirements on Network Action Indicators

23. Insertion, parsing, processing, and disposition of NAIs **SHOULD** make use of existing MPLS data plane operations.
24. Without constraining the mechanism, an MNA solution **MUST** enable a node inserting or modifying NAIs to determine if the target of the NAI, or any other LSR that may expose the NAI, can accept and process an MPLS packet containing the NAI.
25. An NAI **MUST NOT** be imposed for delivery to a node unless it is known that the node supports processing the NAI.
26. The NAI design **MUST** support setting the scope of network actions.
27. A given Network Action solution specification **MUST** define which scope or scopes are applicable to the associated NAI.
28. An MNA solution specification **SHOULD** define the support of NAIs for both Point-to-Point (P2P) and Point-to-Multipoint (P2MP) paths, but the Network Action solution specification **MAY** limit a specific NAI to only one of these path types if there is a clear reason to do so.
29. An MNA solution specification defining data plane mechanisms for NAIs **MUST** be consistent across different control plane protocols.
30. An MNA solution **MUST** allow the deployed MPLS control and management planes to determine the ability of downstream LSRs to accept and/or process a given NAI.
31. An MNA solution **MUST** allow indicators for multiple network actions in the same MPLS packet.
32. An MNA solution specification **MUST NOT** require an implementation to process all NAIs present in an MPLS packet.
33. NAIs **MUST** only be inserted at LSRs that push a label onto the stack, but they can be processed by LSRs along the path of the LSP. Two examples of LSRs that push a label onto the stack are head-end LSRs and points of local repair (PLRs).
34. If a network action requires in-stack ancillary data, the NAI that indicates this network action **MUST** be present in the label stack.
35. All NAIs **MUST** be encoded in a manner consistent with [RFC3031].
36. If there is post-stack ancillary data for an NAI that is present in the label stack, it **MUST** be possible to infer the presence of the ancillary data without having to parse below the bottom of the label stack.
37. Any processing that removes an NAI from the label stack **MUST** also remove all associated ancillary data from the MPLS packet unless the ancillary data is required by any remaining NAIs.
38. MNA solution specifications **MUST** request that IANA create registries and make allocations from those registries for NAIs as necessary to ensure unambiguous identification of standardized network actions. An MNA solution specification **MAY** request that IANA reserve a range of a registry for Private Use.
39. A Network Action solution specification **MUST** state where the NAIs are to be placed in the MPLS packet, that is whether they are placed in-stack or post-stack.

3.5. Requirements on Ancillary Data

40. Network Action solution specifications **MUST** state whether ancillary data is required to fulfill the action and whether it is in-stack and/or post-stack.
41. Network Action solution specifications **MUST** state if in-stack or post-stack ancillary data that is already present in the MPLS packet **MAY** be rewritten by an LSR.
42. Solutions for in-stack ancillary data **MUST** be able to coexist with and **MUST NOT** obsolete existing MPLS mechanisms. Such solutions **MUST** be described in a Standards Track RFC.
43. Network Action solutions **MUST** take care to limit the quantity of in-stack ancillary data to the minimum amount required.
44. A Network Action solution **SHOULD NOT** use post-stack ancillary data unless the size of that ancillary data could prevent the coexistence of the network action with other in-use MPLS network functions if it were inserted into the label stack.
45. The structure of the NAI and any associated ancillary data **MUST** enable skipping of unknown NAIs and any associated AD.
46. Any MNA solution specification **MUST** describe whether the solution can coexist with existing post-stack data mechanisms (e.g., control words and the Generic Associated Channel Header [RFC5586]), and if so how coexistence operates.
47. An MNA solution **MUST** allow an LER that inserts ancillary data to determine whether each node that needs to process the ancillary data can read the required distance into the MPLS packet at that node (compare with the mechanism in [RFC9088]).
48. For scoped in-stack or post-stack ancillary data, any MNA solution **MUST** allow an LER inserting NAIs whose network actions make use of that ancillary data to determine if the NAI and ancillary data will be processed by LSRs within the scope along the path. Such a solution may need to determine if LSRs along the path can process a specific type of AD implied by the NAI at the depth in the stack that it will be presented to the LSR.
49. A mechanism **MUST** exist to notify an egress LER of the presence of ancillary data so that it can dispose of it appropriately.
50. In-stack ancillary data **MUST** only be inserted in conjunction with an operation conforming with [RFC3031].
51. Post-stack ancillary data **MUST** only be inserted in conjunction with an operation conforming with [RFC3031].
52. Processing of ancillary data below a swapped label **MAY** include rewriting the ancillary data.
53. If a Network Action solution needs to change the size of the ancillary data, its specification **MUST** analyze the implications on MPLS packet forwarding and specify how these are addressed.
54. Not more than one Standards Track solution specification **SHOULD** be defined for encoding in-stack ancillary data.
55. Not more than one Standards Track solution specification **SHOULD** be defined for encoding post-stack ancillary data.

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

Solutions designed according to the requirements in this document may introduce new security considerations to MPLS, whose forwarding plane on its own does not provide any built-in security mechanisms [RFC5920].

In particular, such solutions may embed information derived from the MPLS payload in the MPLS headers. This may expose data that a user of the MPLS-based service might otherwise assume is opaque to the MPLS network. Furthermore, an LSR may insert information into the labeled packet such that the forwarding behavior is no longer purely a function of the top label or another label with forwarding context. Instead, the forwarding behavior may be the result of a more complex heuristic. This creates an implicit trust relationship between the LSR whose forwarding behavior is being changed and the upstream LSR inserting the data causing that change.

Several requirements above address some of these considerations. The MNA framework [MNA-FRAMEWORK] also provides security considerations resulting from any extensions to the MPLS architecture, and these **SHOULD** be taken together with the security considerations herein.

Individual solution specifications meeting the requirements in this document **MUST** address any security considerations introduced by the MNA design.

6. Acknowledgements

The authors gratefully acknowledge the contributions from Joel Halpern, Greg Mirsky, Yingzhen Qu, Haoyu Song, Tarek Saad, Loa Andersson, Tony Li, Adrian Farrel, Jie Dong, Bruno Decraene, and participants in the MPLS Working Group who have provided comments.

The authors also gratefully acknowledge the input of the members of the MPLS Open Design Team.

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/info/rfc2119>.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, DOI 10.17487/RFC3031, January 2001, <https://www.rfc-editor.org/info/rfc3031>.

[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>.

[RFC5331] Aggarwal, R., Rekhter, Y., and E. Rosen, "MPLS Upstream Label Assignment and Context-Specific Label Space", RFC 5331, DOI 10.17487/RFC5331, August 2008, <https://www.rfc-editor.org/info/rfc5331>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

7.2. Informative References

[MNA-FRAMEWORK] Andersson, L., Bryant, S., Bocci, M., and T. Li, "MPLS Network Actions (MNA) Framework", Work in Progress, Internet-Draft, draft-ietf-mpls-mna-fwk-10, 6 August 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-mna-fwk-10>.

[MNA-USECASES] Saad, T., Makhijani, K., Song, H., and G. Mirsky, "Use Cases for MPLS Network Action Indicators and MPLS Ancillary Data", Work in Progress, Internet-Draft, draft-ietf-mpls-mna-usecases-10, 20 June 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-mna-usecases-10>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC5586] Bocci, M., Ed., Vigoureux, M., Ed., and S. Bryant, Ed., "MPLS Generic Associated Channel", RFC 5586, DOI 10.17487/RFC5586, June 2009, <https://www.rfc-editor.org/info/rfc5586>.

[RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS Networks", RFC 5920, DOI 10.17487/RFC5920, July 2010, <https://www.rfc-editor.org/info/rfc5920>.

[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>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC9088] Xu, X., Kini, S., Psenak, P., Filsfils, C., Litkowski, S., and M. Bocci, "Signaling Entropy Label Capability and Entropy Readable Label Depth Using IS-IS", RFC 9088, DOI 10.17487/RFC9088, August 2021, <https://www.rfc-editor.org/info/rfc9088>.

Authors' Addresses

Matthew Bocci (EDITOR)
Nokia
Email: matthew.bocci@nokia.com

Stewart Bryant
University of Surrey ICS
Email: sb@stewartbryant.com

John Drake
Independent
Email: je_drake@yahoo.com