Workgroup: MPLS Working Group
Internet-Draft: draft-ietf-mpls-mna-fwk-05
Published: 19 October 2023
Intended Status: Informational
Expires: 21 April 2024
Authors: L. Andersson, Huawei Technologies
S. Bryant, University of Surrey 5GIC
M. Bocci, Nokia
T. Li, Juniper Networks

MPLS Network Actions Framework

Abstract

This document 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 document provides the foundation for the development of a common set of network actions and information elements supporting additional operational models and capabilities of MPLS networks. Some of these actions are defined in existing MPLS specifications, while others require extensions to existing specifications to meet the requirements found in "Requirements for MPLS Network Actions".

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document specifies an architectural framework for the MPLS Network Actions (MNA) technologies. MNA technologies are used to indicate actions for LSPs and/or MPLS packets and to transfer data needed for these actions.

The document provides the foundation for the development of a common set network actions and information elements supporting additional operational models and capabilities of MPLS networks. Some of these actions are defined in existing MPLS specifications, while others require extensions to existing specifications to meet the requirements found in [I-D.ietf-mpls-mna-requirements].

Forwarding actions are instructions to MPLS routers to apply additional actions when forwarding a packet. These might include load-balancing a packet given its entropy, whether or not to perform fast reroute on a failure, and whether or not a packet has metadata relevant to the forwarding decisions along the path.

This document generalizes the concept of "forwarding actions" into "network actions" to include any action that an MPLS router is requested to take on the packet. That includes any forwarding action, but may include other operations (such as security functions, OAM procedures, etc.) that are not directly related to forwarding of the packet.

MNA technologies may use the TC and TTL fields in an MPLS LSE for an alternative purpose.

1.1. Requirement 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.

1.2. Terminology

1.2.1. Normative Definitions

This document adopts the definitions of the following terms and abbreviations from [I-D.ietf-mpls-mna-requirements] as normative: "Network Action", "Network Action Indication (NAI)", "Ancillary Data (AD)", and "Scope".

In addition, this document also defines the following terms:

* Network Action Sub-Stack (NAS): A set of related, contiguous Label Stack Entries (LSEs) in the MPLS label stack. The TC and TTL values in the LSEs in the NAS may be redefined, but the meaning of the S bit is unchanged.

* Network Action Sub-Stack Indicator (NSI): The first LSE in the NAS contains a special label that indicates the start of the NAS.

1.2.2. Abbreviations

Abbreviation	Meaning	Reference
AD	Ancillary Data	[I-D.ietf-mpls-mna-requirements]
bSPL	Base Special Purpose Label	[RFC9017]
ECMP	Equal Cost Multipath	
eSPL	Extended Special Purpose Label	[RFC9017]
HBH	Hop by hop	In the MNA context, this document.
I2E	Ingress to Egress	In the MNA context, this document.
ISD	In stack data	[I-D.ietf-mpls-mna-requirements]
LSE	Label Stack Entry	[RFC3032]
MNA	MPLS Network Actions	[I-D.ietf-mpls-mna-requirements]
NAI	Network Action Indicator	[I-D.ietf-mpls-mna-requirements]
NAS	Network Action Sub-Stack	This document
PSD	Post stack data	[I-D.ietf-mpls-mna-requirements] and Section 3.6
RLD	Readable Label Depth	This document
SPL	Special Purpose Label	[RFC9017]

Table 1: Abbreviations

2. Structure

An MNA solution specifies one or more actions to apply to an MPLS packet. These actions and their parameters may be carried in sub-stacks within the MPLS label stack and/or possibly post-stack data. A solution must specify where in the label stack the network actions sub-stacks occur, if and how frequently they should be replicated, and how network action sub-stack and post-stack data are encoded.

A network action sub-stack contains:

* Network Action Sub-Stack Indicator: The first LSE in the NAS contains a label with special semantics, called the MNA label, that is used to indicate the start of a network action sub-stack.

* Network Action Indicators: Optionally, a set of indicators that describes the set of network actions. If the set of indicators is not in the sub-stack, a solution could encode them in post-stack data. A network action is said to be present if there is an indicator in the packet that invokes the action.

* In-Stack Data: A set of zero or more LSEs that carry ancillary data for the present network actions. Indicators are not considered ancillary data.

Each network action present in the network action sub-stack may have zero or more LSEs of in-stack data. The ordering of the in-stack data LSEs corresponds to the ordering of the network action indicators. The encoding of the in-stack data, if any, for a network action must be specified in the document that defines the network action.

Certain network actions may also specify that data is carried after the label stack. This is called post-stack data. The encoding of the post-stack data, if any, for a network action must be specified in the document that defines the network action. If multiple network actions are present and have post-stack data, the ordering of their post-stack data corresponds to the ordering of the network action indicators.

A solution must specify the order that network actions are to be applied to the packet.

2.1. Scopes

A network action may need to be processed by every node along the path, or some subset of the nodes along its path. Some of the scopes that an action may have are:

* Hop-by-hop (HBH): Every node along the path will perform the action.

* Ingress-to-Egress (I2E): Only the last node on the path will perform the action.

* Select: Only specific nodes along the path will perform the action.

If a solution supports the select scope, it must describe how it specifies the set of nodes to perform the actions.

This framework does not place any constraints on the scope or on the ancillary data for a network action. Any network action may appear in any scope or combination of scopes, may have no ancillary data, may require in stack data, and/or post stack data. Some combinations may be sub-optimal, but this framework does not place any limitations on an MNA solution. A specific MNA solution may define such constraints.

2.2. Partial Processing

As described in [RFC3031], legacy devices that do not recognize the MNA label will discard the packet if the top label is the MNA label.

Devices that do recognize the MNA label may not implement all of the present network actions. A solution must specify how unrecognized present network actions should be handled.

One alternative is that an implementation should stop processing network actions when it encounters an unrecognized network action. Subsequent present network actions would not be applied. The result is dependent on the solution's order of operations.

Another alternative is that an implementation should drop any packet that contains any unrecognized present network actions.

A third alternative is that an implementation should perform all recognized present network actions, but ignore all unrecognized present network actions.

Other alternatives may also be possible and should be specified by the solution.

In some solutions an indication MAY be provided in the packet or in the action as to how the forwarder should proceed if it does not recognise the action. Where an action needs to processed at every hop, it is RECOMMENDED that care is taken not to construct an LSP that traverses nodes that do not support that action. It is recognised that in some circumstances it may not be possible to construct an LSP that avoids such nodes. For example where a network is re-converging following a failure or where IPFRR [RFC5714] is taking place.

2.3. Signaling

A node that wishes to make use of MNA and apply network actions to a packet must understand the nodes that the packet will transit and whether or not the nodes support MNA and the network actions that are to be invoked. These capabilities are presumed to be signaled by protocols that are out-of-scope for this document and are presumed to have per-network action granularity. If a solution requires alternate signaling, it must specify so explicitly.

2.3.1. Readable Label Depth

[RFC8662] introduced the concept of Entropy Readable Label Depth (ERLD). Readable Label Depth (RLD) is the same concept, but generalized and not specifically associated with the Entropy Label (EL) or MNA. Readable Label Depth is defined as the number of LSEs, starting from the top of the stack, that a router can read in an incoming MPLS packet with no performance impact.

A node that pushes a NAS onto the label stack is responsible for ensuring that all nodes that are expected to process the NAS will have the entire NAS within their RLD. A node SHOULD use signaling (e.g., [RFC9088], [RFC9089]) to determine this.

Per [RFC8662], a node that does not support EL will advertise a value of zero for its ERLD, so advertising ERLD alone does not suffice in all cases. A node MAY advertise both ERLD and RLD.

RLD is advertised by an IGP MSD-Type value of (TBA) and MAY be advertised as a Node MSD, Link MSD, or both.

An MNA node MUST use the RLD determined by the selecting the first advertised non-zero value from:

* The RLD advertised for the link.

* The RLD advertised for the node.

* The non-zero ERLD for the node.

2.4. State

A network action can affect state in the network. This implies that a packet may affect how subsequent packets are handled.

3. Encoding

Several possibilities to carry NAIs have been discussed in MNA drafts and in the MPLS Open DT [MPLSODT]. In this section, we enumerate the possibilities and some considerations for the various alternatives.

All types of network actions are represented in the MPLS label stack by a set of LSEs termed a network action sub-stack (NAS). An NAS consists of a special label, optionally followed by LSEs that specify which network actions are to be performed on the packet, and the in-stack ancillary data for each indicated network action.

[I-D.ietf-mpls-mna-requirements] requires that a solution not add unnecessary LSEs to the sub-stack (Section 3.1, requirement 7). Accordingly, solutions should also make efficient use of the bits within the sub-stack, as inefficient use of the bits will result in the addition of unnecessary LSEs.

3.1. The MNA Label

The first LSE in a network action sub-stack contains a special label that indicates a network action sub-stack. A solution has several choices for this special label.

3.1.1. Existing Base SPL

A solution may reuse an existing Base SPL (bSPL). If it elects to do so, it must explain how the usage is backwards compatible, including in the case where there is ISD.

If an existing inactive bSPL is selected and its usage would not be backward compatible, then it must first be retired in accordance with [RFC7274] and then reallocated.

3.1.2. New Base SPL

A solution may select a new bSPL.

3.1.3. New Extended SPL

A solution may select a new eSPL. If it elects to do so, it must address the requirement for the minimal number of LSEs.

3.1.4. User-Defined Label

A solution may allow the network operator to define the label that indicates the network action sub-stack. This creates management overhead for the network operator to coordinate the use of this label across all nodes on the path using management or signaling protocols. If a solution elects to use a user-defined label, the solution should justify this overhead.

3.2. TC and TTL

In the first LSE of the network action sub-stack, only the 20 bits of Label Value and the Bottom of Stack bit are significant, the TC field (3 bits) and the TTL (8 bits) are not used. This leaves 11 bits that could be used for other purposes.

3.2.1. TC and TTL retained

If the solution elects to retain the TC and TTL field, then the first LSE of the network action sub-stack would appear as:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Label                   | TC  |S|      TTL      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
              Label:  Label value, 20 bits
              TC:     Traffic Class, 3 bits
              S:      Bottom of Stack, 1 bit
              TTL:    Time To Live
```

Further LSEs would be needed to encode NAIs. If a solution elects to retain these fields, it must address the requirement for the minimal number of LSEs.

3.2.2. TC and TTL Repurposed

If the solution elects to reuse the TC and TTL field, then the first LSE of the network action sub-stack would appear as:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Label                  |x x x|S|x x x x x x x x|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
              Label:  Label value, 20 bits
              x:      Bit available for solution definition
              S:      Bottom of Stack, 1 bit
```

The solution may use more LSEs to contain NAIs.

3.3. Length of the NAS

A solution must have a mechanism to indicate the length of the NAS. This must be easily processed even by implementations that do not understand the full contents of the NAS. Two options are described below, other solutions may be possible.

3.3.1. Last/Continuation Bits

A solution may use a bit per LSE to indicate whether the NAS continues into the next LSE or not. The bit may indicate continuation by being set or by being clear. The overhead of this approach is one bit per LSE and has the advantage that it can effectively encode an arbitrarily sized NAS. This approach is efficient if the NAS is small.

3.3.2. Length Field

A solution may opt to have a fixed size length field at a fixed location within the NAS. The fixed size of the length field may not be large enough to support all possible NAS contents. This approach may be more efficient if the NAS is longer, but not longer than can be described by the length field.

Advice from hardware designers advocates a length field as this minimizes branching in the logic.

3.4. Encoding of Scopes

A solution may choose to explicitly encode the scope of the actions contained in a network action sub-stack. A solution may also choose to have the scope encoded implicitly, based on the actions present in the network action sub-stack. This choice may have performance implications as an implementation might have to parse the network actions that are present in a network action sub-stack only to discover that there are no actions for it to perform.

Solutions need to consider the order of scoped NAIs and their associated AD within individual sub-stacks and the order of per-scope sub-stacks in order that network actions and the AD can be most readily found and not need to processed by nodes that are not required to handle those actions.

3.5. Encoding a Network Action

Two options for encoding NAIs are described below, other solutions may be possible. Any solution should allow encoding of an arbitrary number of NAIs.

3.5.1. Bit Catalogs

A solution may opt to encode the set of network actions as a list of bits, sometimes known as a catalog. The solution must provide a mechanism to determine how many LSEs are devoted to the catalog. A set bit in the catalog would indicate that the corresponding network action is present.

Catalogs are efficient if the number of present network actions is relatively high and if the size of the necessary catalog is small. For example, if the first 16 actions are all present, a catalog can encode this in 16 bits. However, if the number of possible actions is large, then a catalog can become inefficient. Selecting only one action that is the 256th action would require a catalog of 256 bits, which would require more than one LSE.

A solution may include a bit remapping mechanism so that a given domain may optimize for its commonly used actions.

3.5.2. Operation Codes

A solution may opt to encode the set of present network actions as a list of operation codes (opcodes). Each opcode is a fixed number of bits. The size of the opcode bounds the number of network actions that the solution can support.

Opcodes are efficient if there are only one or two active network actions. For example, if an opcode is 8 bits, then two active network actions could be encoded in in 16 bits. However, if there are 16 actions required, then opcodes would consume 128 bits. Opcodes are efficient at encoding a large number of possible actions. If only the 256th action is to be selected, that still requires 8 bits.

3.6. Encoding of Post-Stack Data

A solution may optionally carry some data as PSD.

If there are multiple instances of post-stack data, they should occur in the same order as their relevant network action sub-stacks and then in the same order as their relevant network functions occur within the network action sub-stacks.

3.6.1. First Nibble Considerations

The first nibble after the label stack has been used to convey information in certain cases [RFC4385]. A consolidated view of first nibble uses is provided in [I-D.ietf-mpls-1stnibble].

For example, in [RFC4928] this nibble is investigated to find out if it has the value "4" or "6", if it is not, it is assumed that the packet payload is not IPv4 or IPv6 and Equal Cost Multipath (ECMP) is not performed.

It should be noted that this is an inexact method, for example an Ethernet Pseudowire without a control word might have "4" or "6" in the first nibble and thus will be ECMP'ed.

Nevertheless, the method is implemented and deployed, it is used today and will be for the foreseeable future.

The use of the first nibble for BIER is specified in [RFC8296]. Bier sets the first nibble to 5. The same is true for BIER payload, as for any use of the first nibble, it is not possible from the first nibble itself being set to 5, conclude that the payload is BIER.

However, it achieves the design goal of [RFC8296], to exclude that the payload is IPv4, IPv6 or a pseudowire.

There are possibly more examples, they will be added if we find that they further highlight the issue with using the first nibble.

[RFC4385] allocates 0b0000 for the PW control word and 0b0001 for the PW ACH.

A PSD solution should specify the contents of the first nibble, the actions to be taken for the value, and the interaction with post-stack data used concurrently by other MPLS applications.

4. Semantics

4.1. Order of Evaluation

For MNA to be consistent across implementations and predictable in operational environments, its semantics need to be entirely predictable. An MNA solution MUST specify a deterministic order for processing each of the Network Actions in a packet. Each Network Action must specify how it interacts with all other previously defined Network Actions. Private network actions MUST be included in the ordering of Network Actions, but the interactions of private actions with other actions is outside of the scope of this document.

5. Definition of a Network Action

Network actions should be defined in a document and must contain:

* Name: The name of the network action.

* Network Action Indicator: The bit position or opcode that indicates that the network action is active.

* Scope: The document should specify which nodes should perform the network action. The action may apply to each transit node (HBH), only the egress node that pops the final label off of the label stack, or specific nodes along the label switched path.

* State: The document should specify if the network action can modify state in the network, and if so, the state that may be modified and its side-effects.

* Required/Optional: The document should specify whether a node is required to perform the network action.

* In-Stack Data: The number of LSEs of in-stack data, if any, and its encoding. If this is of a variable length, then the solution

must specify how an implementation can determine this length without implementing the network action.

*Post-Stack Data: The encoding of post-stack data, if any. If this is of a variable length, then the solution must specify how an implementation can determine this length without implementing the network action.

A solution should create an IANA registry for network actions.

6. Management Considerations

Network operators will need to be cognizant of which network actions are supported by which nodes and will need to ensure that this is signalled appropriately. Some solutions may require network-wide configuration to synchronize the use of the labels that indicate the start of an NAS. Solution documents must make clear what management considerations apply to the solutions they are describing. Solutions documents must describe mechanisms for performing network diagnostics in the presence of MNAs.

7. Security Considerations

An analysis of the security of MPLS systems is provided in [RFC5920], which also notes that the MPLS forwarding plane has no built-in security mechanisms.

Some proposals to add encryption to the MPLS forwarding plane have been suggested [I-D.ietf-mpls-opportunistic-encrypt], but no mechanisms have been agreed upon at the time of publication of this document. Additionally, MPLS does not provide any cryptographic integrity protection on the MPLS headers. However, both such mechanisms would significantly complicate the operation of any MNA solution and would likely be significantly deleterious to forwarding performance. This is particularly the case where an MNA solution used an in-stack approach that needed to employ on-path modification of the MNA data.

Central to the security of MPLS networks is operational security of the network; something that operators of MPLS networks are well versed in. The deployment of link-level security (e.g., [MACsec]) prevents the covert acquisition of the label stack for the purposes of an attack. This is particularly important in the case of a network deploying MNA, because the MNA information may be sensitive. Thus the confidentiallity and authentication achieved through the use of link-level security is particularly advantageous.

A cornerstone of MPLS security is that packets entering an MPLS network from an untrusted third party are immediately encapsulated in an MPLS label stack specified by the MPLS network operator and thus are unable to present any labels to the network forwarding system.

It is thus difficult for an attacker to pass a raw MPLS-encoded packet into a network, and operators have considerable experience in excluding such packets at the network boundaries, for example, by excluding all MPLS packets and all packets that are revealed to be carrying an MPLS packet as the payload of IP tunnels.

Within a single well-managed domain, an adjacent domain may be considered to be trusted provided that it is sufficiently shielded from third party traffic ingress and third party traffic observation. In such a situation, no new security vulnerabilites are introduced by MNA.

In some inter-domain applications (including carrier's carrier) where a first network's MPLS traffic is encapsulated directly over a second MPLS network by simply pushing additional MPLS LSEs, the contents of the first network's payload and label stack may be visible to the forwarders in the second network. Historically this has been benign, and indeed useful for the purposes of ECMP. However where the first network's traffic has MNA information this may be exposed to MNA capable forwarders causing unpredictable behaviour or modification of the customer MPLS label stack or MPLS payload. This is an increased vulnerability introduced by MNA that SHOULD be addressed in any MNA solution.

There are a number of mitigations that are available to an operator:

a) Reject all incoming packets containing MNA information that do not come from a trusted network. Note that it may be acceptable to accept and process MNA information from a trusted network.

b) Fully encapsulate the inbound packet in a new additional MPLS label stack such that the forwarder finds a BoS bit imposed by the carrier network and only finds MNA information added by the carrier network.

A mitigation that we reject as unsafe is having the ingress LSR push sufficient additional labels such that any MNA information received in packets entering the network from a third party network is made inaccessible due to it being below the RLD. This is unsafe in the presence of an overly conservative RLD value which can result in the thirty party MNA information becoming visible to and acted on by an MNA forwarder in the carrier network.

8. IANA Considerations

This document requests that IANA allocate a code point from the "IGP MSD-Types" registry in the "Interior Gateway Protocol (IGP)

Parameters" namespace for "Readable Label Depth", referencing this document.

9. Acknowledgements

This document is the result of work started in MPLS Open Desgign Team, with participation by the MPLS, PALS and DETNET working groups.

The authors would like to thank Adrian Farrel for his contributions and to John Drake and Jie Dong for their comments.

10. References

10.1. Normative References

[I-D.ietf-mpls-mna-requirements] Bocci, M., Bryant, S., and J. Drake, "Requirements for MPLS Network Actions", Work in Progress, Internet-Draft, draft-ietf-mpls-mna-requirements-07, 18 September 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-mna-requirements-07>.

[I-D.ietf-mpls-opportunistic-encrypt] Farrel, A. and S. Farrell, "Opportunistic Security in MPLS Networks", Work in Progress, Internet-Draft, draft-ietf-mpls-opportunistic-encrypt-03, 28 March 2017, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-opportunistic-encrypt-03>.

[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>.

[RFC7274] Kompella, K., Andersson, L., and A. Farrel, "Allocating and Retiring Special-Purpose MPLS Labels", RFC 7274, DOI 10.17487/RFC7274, June 2014, <https://www.rfc-editor.org/info/rfc7274>.

[RFC8662] Kini, S., Kompella, K., Sivabalan, S., Litkowski, S., Shakir, R., and J. Tantsura, "Entropy Label for Source Packet Routing in Networking (SPRING) Tunnels", RFC 8662, DOI 10.17487/RFC8662, December 2019, <https://www.rfc-editor.org/info/rfc8662>.

[RFC9017] Andersson, L., Kompella, K., and A. Farrel, "Special-Purpose Label Terminology", RFC 9017, DOI 10.17487/RFC9017, April 2021, <https://www.rfc-editor.org/info/rfc9017>.

[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>.

[RFC9089] Xu, X., Kini, S., Psenak, P., Filsfils, C., Litkowski, S., and M. Bocci, "Signaling Entropy Label Capability and Entropy Readable Label Depth Using OSPF", RFC 9089, DOI 10.17487/RFC9089, August 2021, <https://www.rfc-editor.org/info/rfc9089>.

[MACsec] IEEE Computer Society, "IEEE 802.1AE Media Access Control (MAC) Security", August 2006.

[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>.

[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>.

[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>.

[RFC5714] Shand, M. and S. Bryant, "IP Fast Reroute Framework", RFC 5714, DOI 10.17487/RFC5714, January 2010, <https://www.rfc-editor.org/info/rfc5714>.

[RFC4385] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, DOI 10.17487/RFC4385, February 2006, <https://www.rfc-editor.org/info/rfc4385>.

[I-D.ietf-mpls-1stnibble]
Kompella, K., Bryant, S., Bocci, M., Mirsky, G., Andersson, L., and J. Dong, "IANA Registry for the First Nibble Following a Label Stack", Work in Progress, Internet-Draft, draft-ietf-mpls-1stnibble-02, 5 July

2023, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-1stnibble-02>.

[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>.

10.2. Informative References

[RFC4928] Swallow, G., Bryant, S., and L. Andersson, "Avoiding Equal Cost Multipath Treatment in MPLS Networks", BCP 128, RFC 4928, DOI 10.17487/RFC4928, June 2007, <https://www.rfc-editor.org/info/rfc4928>.

[RFC8296] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Tantsura, J., Aldrin, S., and I. Meilik, "Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks", RFC 8296, DOI 10.17487/RFC8296, January 2018, <https://www.rfc-editor.org/info/rfc8296>.

[MPLSODT] "MPLS Working Group Wiki", n.d., <https://wiki.ietf.org/en/group/mpls/odt/main>.

Authors' Addresses

Loa Andersson
Huawei Technologies

Email: loa@pi.nu

Stewart Bryant
University of Surrey 5GIC

Email: sb@stewartbryant.com

Matthew Bocci
Nokia

Email: matthew.bocci@nokia.com

Tony Li
Juniper Networks

Email: tony.li@tony.li