MPLS Working Group S. Bryant
Internet-Draft M. Chen
Intended status: Informational Z. Li
Expires: August 2, 2018 Huawei
G. Swallow
S. Sivabalan
Cisco Systems
G. Mirsky
Ericsson
January 29, 2018

Synonymous Flow Label Framework
draft-ietf-mpls-sfl-framework-01

Abstract

draft-ietf-mpls-flow-ident describes the requirement for introducing flow identities within the MPLS architecture. This document describes a method of accomplishing this by using a technique called Synonymous Flow Labels in which labels which mimic the behaviour of other labels provide the identification service. These identifiers can be used to trigger per-flow operations on the on the packet at the receiving label switching router.

Table of Contents

1. Introduction 2
2. Requirements Language 2
3. Synonymous Flow Labels 3
4. User Service Traffic in the Data Plane 4
4.1. Applications Label Present 4
4.1.1. Setting TTL and the Traffic Class Bits 5
4.2. Single Label Stack 5
4.2.1. Setting TTL and the Traffic Class Bits 6
4.3. Aggregation of SFL Actions 6
5. Equal Cost Multipath Considerations 7
6. Privacy Considerations 8
7. Security Considerations 8
8. IANA Considerations 8
9. References 8
9.1. Normative References 8
9.2. Informative References 9
Authors' Addresses 9

1. Introduction

[I-D.ietf-mpls-flow-ident] describes the requirement for introducing flow identities within the MPLS architecture.

This document describes a method of accomplishing this by using a technique called Synonymous Flow Labels (SFL) (see (Section 2)) in which labels which mimic the behaviour of other labels provide the identification service. These identifiers can be used to trigger per-flow operations on the packet at the receiving label switching router.

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.

3. Synonymous Flow Labels

An SFL is defined to be a label that causes exactly the same behaviour at the egress Label Switching Router (LSR) as the label it replaces, but in addition also causes an agreed action to take place on the packet. There are many possible additional actions such as the measurement of the number of received packets in a flow, triggering IPFIX inspection, triggering other types of Deep Packet Inspection, or identification of the packet source. In, for example, a Performance Monitoring (PM) application, the agreed action could be the recording of the receipt of the packet by incrementing a packet counter. This is a natural action in many MPLS implementations, and where supported this permits the implementation of high quality packet loss measurement without any change to the packet forwarding system.

Consider an MPLS application such as a pseudowire (PW), and consider that it is desired to use the approach specified in this document to make a packet loss measurement. By some method outside the scope of this text, two labels, synonymous with the PW labels are obtained from the egress terminating provider edge (T-PE). By alternating between these SFLs and using them in place of the PW label, the PW packets may be batched for counting without any impact on the PW forwarding behaviour (note that strictly only one SFL is needed in this application, but that is an optimization that is a matter for the implementor).

Now consider an MPLS application that is multi-point to point such as a VPN. Here it is necessary to identify a packet batch from a specific source. This is achieved by making the SFLs source specific, so that batches from one source are marked differently from batches from another source. The sources all operate independently and asynchronously from each other, independently co-ordinating with the destination. Each ingress is thus able to establish its own SFL to identify the sub-flow and thus enable PM per flow.

Finally we need to consider the case where there is no MPLS application label such as occurs when sending IP over an LSP. In this case introducing an SFL that was synonymous with the LSP label would introduce network wide forwarding state. This would not be acceptable for scaling reasons. We therefore have no choice but to introduce an additional label. Where penultimate hop popping (PHP) is in use, the semantics of this additional label can be similar to the LSP label. Where PHP is not in use, the semantics are similar to

an MPLS explicit NULL. In both of these cases the label has the additional semantics of the SFL.

Note that to achieve the goals set out in Section 1 SFLs need to be allocated from the platform label table.

4. User Service Traffic in the Data Plane

As noted in Section 3 it is necessary to consider two cases:

1. Applications label present

2. Single label stack

4.1. Applications Label Present

Figure 1 shows the case in which both an LSP label and an application label are present in the MPLS label stack. Traffic with no SFL function present runs over the "normal" stack, and SFL enabled flows run over the SFL stack with the SFL used to indicate the packet batch.

```
 +-----------------+          +-----------------+
 |                 |          |                 |
 |       LSP       |          |       LSP       | <May be PHPed
 |      Label      |          |      Label      |
 +-----------------+          +-----------------+
 |                 |          |                 |
 |   Application   |          | Synonymous Flow |
 |      Label      |          |      Label      |
 +-----------------+          +-----------------+ <= Bottom of stack
 |                 |          |                 |
 |    Payload      |          |    Payload      |
 |                 |          |                 |
 +-----------------+          +-----------------+


"Normal" Label Stack         Label Stack with SFL
```

Figure 1: Use of Synonymous Labels In A Two Label MPLS Label Stack

At the egress LSR the LSP label is popped (if present). Then the SFL is processed in exactly the same way as the corresponding application label would have been processed.

4.1.1. Setting TTL and the Traffic Class Bits

The TTL and the Traffic Class bits [RFC5462] in the SFL LSE would normally be set to the same value as would have been set in the label that the SFL is synonymous with. However it is recognised that there may be an applications need to set the SFL to some other value. An example would be where it was desired to cause the SFL to trigger an action in the TTL expiry exception path as part of the label action.

4.2. Single Label Stack

Figure 2 shows the case in which only an LSP label is present in the MPLS label stack. Traffic with no SFL function present runs over the "normal" stack and SFL enabled flows run over the SFL stack with the SFL used to indicate the packet batch. However in this case it is necessary for the ingress LSR to first push the SFL and then to push the LSP label.

```
                             +-----------------+
                             |                 |
                             |       LSP       | <= May be PHPed
                             |      Label      |
    +-----------------+      +-----------------+
    |                 |      |                 | <= Synonymous with
    |       LSP       |      | Synonymous Flow |    Explicit NULL
    |      Label      |      |      Label      |
    +-----------------+      +-----------------+ <= Bottom of stack
    |                 |      |                 |
    |    Payload      |      |    Payload      |
    |                 |      |                 |
    +-----------------+      +-----------------+


   "Normal" Label Stack         Label Stack with SFL
```

Figure 2: Use of Synonymous Labels In A Single Label MPLS Label Stack

At the receiving LSR it is necessary to consider two cases:

1. Where the LSP label is still present

2. Where the LSP label is penultimate hop popped

If the LSP label is present, it processed exactly as it would normally processed and then it is popped. This reveals the SFL which in the case of [RFC6374] measurements is simply counted and then discarded. In this respect the processing of the SFL is synonymous

with an Explicit NULL. As the SFL is the bottom of stack, the IP packet that follows is processed as normal.

If the LSP label is not present due to PHP action in the upstream LSR, two almost equivalent processing actions can take place. Either the SFL can be treated as an LSP label that was not PHPed and the additional associated SFL action is taken when the label is processed. Alternatively, it can be treated as an explicit NULL with associated SFL actions. From the perspective of the measurement system described in this document the behaviour of two approaches are indistinguishable and thus either may be implemented.

4.2.1. Setting TTL and the Traffic Class Bits

The TTL and the Traffic Class considerations described in Section 4.1.1 apply.

4.3. Aggregation of SFL Actions

There are cases where it is desirable to aggregate an SFL action against a number of labels. For example where it is desirable to have one counter record the number of packets received over a group of application labels, or where the number of labels used by a single application is large, and consequently the increase in the number of allocated labels needed to support the SFL actions consequently becomes too large to be viable. In these circumstances it would be necessary to introduce an additional label in the stack to act as an aggregate instruction. This is not strictly a synonymous action in that the SFL is not replacing a existing label, but is somewhat similar to the single label case shown in Section 4.2, and the same signalling, management and configuration tools would be applicable.

```
                                 +-----------------+
                                 |                 |
                                 |       LSP       | < May be PHPed
                                 |      Label      |
       +-----------------+       +-----------------+
       |                 |       |                 |
       |       LSP       |       |    Aggregate    |
       |      Label      |       |       SFL       |
       +-----------------+       +-----------------+
       |                 |       |                 |
       |   Application   |       |   Application   |
       |      Label      |       |      Label      |
       +-----------------+       +-----------------+ <= Bottom of stack
       |                 |       |                 |
       |    Payload      |       |    Payload      |
       |                 |       |                 |
       +-----------------+       +-----------------+


      "Normal" Label Stack         Label Stack with SFL
```

Figure 3: Aggregate SFL Actions

The Aggregate SFL is shown in the label stack depicted in Figure 3 as preceding the application label, however the choice of position before, or after, the application label will be application specific. In the case described in Section 4.1, by definition the SFL has the full application context. In this case the positioning will depend on whether the SFL action needs the full context of the application to perform its action and whether the complexity of the application will be increased by finding an SFL following the application label.

5. Equal Cost Multipath Considerations

The introduction to an SFL to an existing flow may cause that flow to take a different path through the network under conditions of Equal Cost Multipath (ECMP). This is turn may invalidate the certain uses of the SFL such as performance measurement applications. Where this is a problem there are two solutions worthy of consideration:

1. The operator can elect to always run with the SFL in place in the MPLS label stack.

2. The operator can elect to use [RFC6790] Entropy Labels in a network that fully supports this type of ECMP. If this approach is adopted, the intervening MPLS network MUST NOT load balance on any packet field other than the entropy label. Note that this is stricter than the text in Section 4.2 of [RFC6790]. In networks

in which the ECMP decision is independent of both the value of any other label in the label stack, and the MPLS payload, the path of the flow with the SFL will be congruent with the path without the SFL.

6. Privacy Considerations

Recent IETF concerns on pervasive monitoring are described in [RFC7258]. The inclusion of originating and/or flow information in a packet provides more identity information and hence potentially degrades the privacy of the communication. Whilst the inclusion of the additional granularity does allow greater insight into the flow characteristics it does not specifically identify which node originated the packet other than by inspection of the network at the point of ingress, or inspection of the control protocol packets. This privacy threat may be mitigated by encrypting the control protocol packets, regularly changing the synonymous labels and by concurrently using a number of such labels. Minimizing the scope of the identity indication can be useful in minimizing the observability of the flow characteristics.

7. Security Considerations

The issue noted in Section 6 is a security consideration. There are no other new security issues associated with the MPLS dataplane. Any control protocol used to request SFLs will need to ensure the legitimacy of the request.

8. IANA Considerations

This draft makes no IANA requests.

9. References

9.1. 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>.

[RFC5462] Andersson, L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, DOI 10.17487/RFC5462, February 2009, <https://www.rfc-editor.org/info/rfc5462>.

[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>.

9.2. Informative References

[I-D.ietf-mpls-flow-ident]
Bryant, S., Pignataro, C., Chen, M., Li, Z., and G. Mirsky, "MPLS Flow Identification Considerations", draft-ietf-mpls-flow-ident-06 (work in progress), December 2017.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, DOI 10.17487/RFC6374, September 2011, <https://www.rfc-editor.org/info/rfc6374>.

[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>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

Authors' Addresses

Stewart Bryant
Huawei

Email: stewart.bryant@gmail.com

Mach Chen
Huawei

Email: mach.chen@huawei.com

Zhenbin Li
Huawei

Email: lizhenbin@huawei.com

George Swallow
Cisco Systems

Email: swallow@cisco.com

Siva Sivabalan
Cisco Systems

Email: msiva@cisco.com

Gregory Mirsky
Ericsson

Email: gregory.mirsky@eicsson.com