TEAS Working Group
Internet-Draft
Intended Status: Standards Track
Expires: September 8, 2016

R. Gandhi, Ed.
Cisco Systems
H. Shah
Ciena
Jeremy Whittaker
Verizon

March 7, 2016

RSVP-TE Extensions For Associated Co-routed Bidirectional Label Switched Paths (LSPs) draft-gandhishah-teas-assoc-corouted-bidir-00

Abstract

In packet transport networks, there are requirements where reverse unidirectional LSP of a bidirectional LSP needs to follow the same path as its forward unidirectional LSP. This document describes how RSVP Extended ASSOCIATION Object can be used to bind two co-routed point-to-point unidirectional LSPs into an associated co-routed bidirectional LSP in single-sided provisioning case. The RSVP REVERSE_LSP Object is used to enable an endpoint to trigger creation of the reverse LSP along the same path as the forward LSP. Fast-reroute procedures to ensure that the traffic flows on the co-routed path after a failure event are also described.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Table of Contents

1. Introduction 3
2. Conventions Used in This Document 3
2.1. Key Word Definitions 3
2.2. Reverse Co-routed Unidirectional LSPs 3
3. Overview 4
4. Message and Object Definitions 4
4.1. Extended ASSOCIATION Object 4
5. Signaling Procedure 6
5.1. Co-routed Bidirectional LSP Association 6
5.2. Fast-Reroute For Associated Co-routed Bidirectional LSP . 6
6. Compatibility 7
7. Security Considerations 7
8. IANA Considerations 7
9. References 8
9.1. Normative References 8
9.2. Informative References 8
Authors' Addresses 9

1. Introduction

In packet transport networks, there are requirements where a reverse LSP of a bidirectional LSP needs to follow the same path as its forward LSP [RFC6373].

The RSVP Extended ASSOCIATION Object is specified in [RFC6780] which can be used generically to associate (G)MPLS LSPs. [RFC7551] defines mechanisms for binding two point-to-point unidirectional LSPs [RFC3209] into an associated bidirectional LSP. There are two models described for provisioning the LSP, single-sided and double-sided. The double-sided provisioned bidirectional LSPs are not considered in this document.

The MPLS TP [RFC6370] architecture facilitates the co-routed bidirectional LSP by using GMPLS extensions [RFC3473] to achieve congruent paths. The RSVP association signaling allows to take advantages of the co-routed bidirectional LSPs without having to deploy GMPLS extensions in the existing networks. The association signaling also allows to take advantage of the existing TE mechanisms such as fast-reroute.

[GMPLS-FRR] defines fast-reroute procedures for GMPLS signaled LSPs to ensure traffic flows on a co-routed path after a failure event on the primary LSP path. [GMPLS-FRR] defined fast-reroute mechanisms are equally applicable to the associated co-routed bidirectional LSPs.

This document describes how Extended ASSOCIATION Object can be used to bind two reverse co-routed unidirectional LSPs into an associated co-routed bidirectional LSP in single-sided provisioning case. The REVERSE_LSP Object is used to enable an endpoint to trigger creation of the reverse LSP along the same path as the forward LSP. Fast-reroute procedures to ensure that the traffic flows on the co-routed path after a failure event are also described.

2. Conventions Used in This Document

2.1. Key Word Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Reverse Co-routed Unidirectional LSPs

Two reverse unidirectional LSPs are setup in the opposite directions

between a pair of source and destination nodes to form an associated bidirectional LSP. A reverse unidirectional LSP originates on the same node where the forward unidirectional LSP terminates, and it terminates on the same node where the forward unidirectional LSP originates. A reverse co-routed unidirectional LSP traverses along the same path of the forward direction unidirectional LSP in the opposite direction.

3. Overview

For single-sided provisioning, the RSVP Traffic Engineering (TE) tunnel is configured only on one endpoint. An LSP for this tunnel is initiated by the originating endpoint with Extended ASSOCIATION Object containing Association Type set to "single-sided associated bidirectional LSP" and REVERSE_LSP Object inserted in the Path message. The remote endpoint then creates the corresponding reverse TE tunnel and signals the reverse LSP in response using information from the REVERSE_LSP Object and other objects present in the received Path message [RFC7551]. The reverse LSP thus created may or may not be congruent.

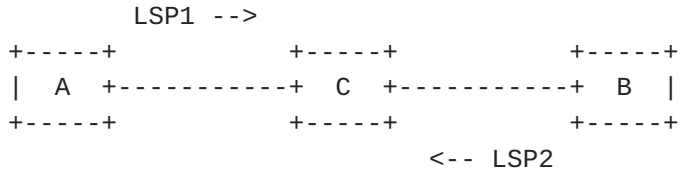

Figure 1: An Example of Associated Co-routed Bidirectional LSP

As shown in Figure 1, creation of reverse LSP2 on remote endpoint B is triggered by LSP1. LSP2 follows the path in the reverse direction using the EXPLICIT_ROUTE Object (ERO) from the received REVERSE_LSP Object in the Path message of LSP1.

For co-routed bidirectional LSP, the originating endpoint A ensures the reverse LSP follow the same path as the forward LSP by populating EXPLICIT_ROUTE Object in the REVERSE_LSP Object using the hops traversed by the forward LSP in the reverse order.

4. Message and Object Definitions

4.1. Extended ASSOCIATION Object

The Extended ASSOCIATION Object is populated using the rules defined

in [RFC7551] for the Association Type "single-sided associated bidirectional LSP".

The Extended Association ID is set by the originating node to the value specified as following.

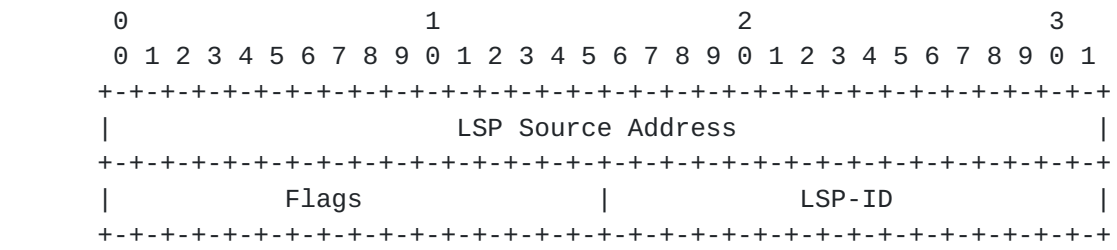

Figure 2: IPv4 Extended Association ID Format

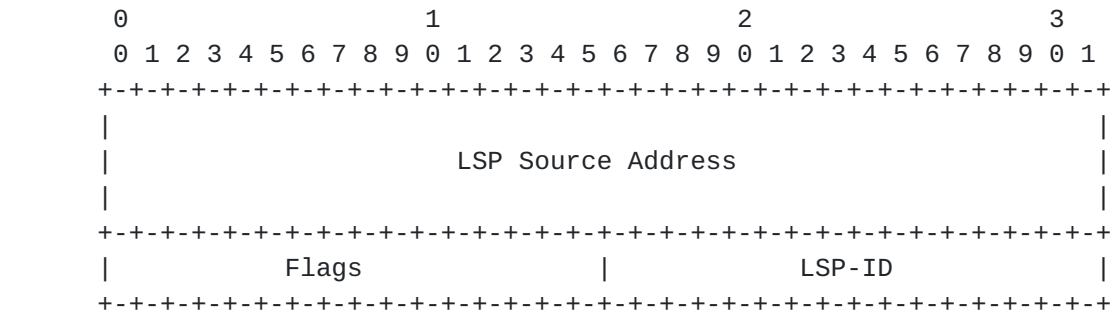

Figure 3: IPv6 Extended Association ID Format

LSP Source Address

IPv4/IPv6 source address of the originating LSP.

LSP-ID

16-bits LSP-ID of the originating LSP.

Flags

Bit 0: COROUTED-LSP-FLAG: When set, this flag indicates the associated bidirectional LSP is co-routed.

Bit 1-15: Not used. Must be set to 0.

5. Signaling Procedure

5.1. Co-routed Bidirectional LSP Association

In general, the processing rules for the Extended ASSOCIATION Object as specified in [RFC6780] and [RFC7551] are followed for co-routed bidirectional LSP association.

The originating head-end MUST add Extended ASSOCIATION Object with Association Type set to "single-sided associated bidirectional LSP" and the extended association ID as specified in Section 4.1 of this document. The COROUTED-LSP-FLAG MUST be set to indicate the nodes on the LSP path that bidirectional LSP is co-routed. In addition, the originating head-end node MUST add EXPLICIT_ROUTE Object (ERO) in the REVERSE_LSP Object by using the hops traversed by the forward LSP in the reverse order to ensure that reverse LSP follows the same path as forward direction LSP in the opposite direction.

As defined in [RFC7551], the remote endpoint simply copies the content of the received Extended ASSOCIATION Object including the extended association ID in the reverse LSP Extended ASSOCIATION Object. In addition, the remote endpoint builds the ERO of the reverse LSP using the ERO from the received REVERSE_LSP Object of the forward LSP.

As contents of the Extended ASSOCIATION Object are unique for each associated co-routed bidirectional LSP, a node can unambiguously identify the associated LSP pair by matching their Extended ASSOCIATION Objects. At a transit LSR, reverse LSP can identify the matching forward LSP by checking the originating LSP source address and LSP-ID in the extended association ID. In addition, a node can identify an originating (forward) LSP by matching the LSP source address with the source address in the extended association ID.

5.2. Fast-Reroute For Associated Co-routed Bidirectional LSP

The procedures defined in [GMPLS-FRR] are used for associated co-routed bidirectional LSP to ensure that traffic flows on a co-routed path after a link or node failure. The COROUTED-LSP-FLAG is used by the Point of Local Repair (PLR) nodes to provide fast-reroute protection using associated co-routed bypass tunnels.

As described in [GMPLS-FRR], BYPASS_ASSIGNMENT subobject in RRO is used to co-ordinate bypass tunnel assignment between a forward and

reverse direction PLRs. This subobject MUST be added by the forward direction PLR in the Path message of the originating LSP. The reverse direction PLR (forward direction LSP merge-point (MP)) simply reflects the bypass tunnel assignment for the reverse direction LSP on the co-routed path.

After a link or node failure, PLRs in both directions trigger fast-reroute independently using the procedures defined in [RFC4090].

As specified in [GMPLS-FRR], re-corouting procedure can be used to reroute the traffic in the reverse direction on the co-routed bypass tunnel path. Reverse direction PLR will assume the role of Point of Remote Repair (PRR) and trigger the fast-reroute in the reverse direction on the matching co-routed bypass tunnel to ensure that both traffic and RSVP signaling flow on the co-routed path after the failure.

6. Compatibility

The Extended ASSOCIATION Object has been defined in [RFC6780], with class number in the form 11bbbbbb, which ensures compatibility with non-supporting nodes. Per [RFC2205], such nodes will ignore the object but forward it without modification.

This document defines the content of the Extended Association ID for the Extended ASSOCIATION Object for co-routed bidirectional LSPs. Operators wishing to use this function SHOULD ensure that it is supported on the node that is expected to act on the association.

7. Security Considerations

This document uses signaling mechanisms defined in [RFC7551] and [GMPLS-FRR] and does not introduce any additional security considerations other than already covered in [RFC7551], [GMPLS-FRR] and the MPLS/GMPLS security framework [RFC5920].

Using the extended association ID in the intercepted signalling message, a node may be able to get additional information of the LSP such as co-routed type and the originating node. This is judged to be a very minor security risk as this information is already available by other means.

8. IANA Considerations

This document does not make any request for IANA action.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC4090] Pan, P., Ed., Swallow, G., Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, May 2005.

[RFC6780] Berger, L., Le Faucheur, F., and A. Narayanan, "RSVP Association Object Extensions", RFC 6780, October 2012.

[RFC7551] Zhang, F., Ed., Jing, R., and Gandhi, R., Ed., "RSVP-TE Extensions for Associated Bidirectional LSPs", RFC 7551, May 2015.

[GMPLS-FRR] Taillon, M., Saad, T., Ed., Gandhi, R., Ed., Ali, Z., Bhatia, M., Jin, L., "Extensions to Resource Reservation Protocol For Fast Reroute of Traffic Engineering GMPLS LSPs", draft-ietf-teas-gmpls-lsp-fastreroute.

9.2. Informative References

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3473] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC5920] Fang, L., "Security Framework for MPLS and GMPLS Networks", RFC 5920, July 2010.

[RFC6370] Bocci, M., Swallow, G., and E. Gray, "MPLS Transport Profile (MPLS-TP) Identifiers", RFC 6370, September 2011.

[RFC6373] Andersson, L., Berger, L., Fang, L., Bitar, N., and E. Gray, "MPLS Transport Profile (MPLS-TP) Control Plane Framework", RFC 6373, September 2011.

Authors' Addresses

Rakesh Gandhi (editor)
Cisco Systems, Inc.

EMail: rgandhi.ietf@gmail.com

Himanshu Shah
Ciena

EMail: hshah@ciena.com

Jeremy Whittaker
Verizon

EMail: jeremy.whittaker@verizon.com