Network Working Group   Z. Li
Internet-Draft   X. Zeng
Intended status: Standards Track   Huawei Technologies
Expires: January 5, 2015   July 4, 2014

Proxy MPLS Traffic Engineering Label Switched Path(LSP) draft-li-mpls-proxy-te-lsp-01

Abstract

This document describes a method to setup MPLS TE proxy egress LSP which can help setup end-to-end LSP through stitching MPLS TE proxy egress LSP with BGP LSP in the Seamless MPLS network. The method is achieved by new Proxy Destination Object carried in RSVP-TE messages.

Requirements Language

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].

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 http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 5, 2015.

Copyright Notice

Table of Contents

1. Introduction

Seamless MPLS[I-D.ietf-mpls-seamless-mpls] provides an end to end service independent transport architecture. It removes the need for service specific configurations in network transport nodes. Seamless MPLS uses existing protocols like LDP, IS-IS, etc. to build intra-area segments and uses MP-BGP as the inter-area routing and label distribution protocol.

In the typical Seamless MPLS architecture, LDP DoD are adopted to setup the segment LSP which is stitched with BGP LSP. When Seamless MPLS is applied to integrate the mobile backhaul network with the core/aggregation network, since MPLS TE is always adopted to deploy in the mobile backhaul network for requirements on high reliability, QoS, etc., it has to set up the MPLS TE proxy egress LSP in the mobile backhaul network to stitch with BGP LSP for the end-to-end transport.

This document introduces a new Proxy Destination Object for RSVP-TE. Through the RSVP-TE extension the proxy egress LSP can setup for RSVP-TE. It makes possible to setup the end-to-end LSP when deploy MPLS TE in the Seamless MPLS scenario to integrate the mobile backhaul network with the core/aggregation network.

2. Terminology

Proxy Egress LSP: It is defined in Sec. 4.1.4 of [RFC3031]. It is the LSP which is setup by the proxy egress LSR instead of the actual destination LSR.

3. Problem Statement

The typical Seamless MPLS architecture is shown in the figure 1. The typical procedure of setting up the end-to-end transport LSP described in [I-D.ietf-mpls-seamless-mpls] is as follows:

1. Setup the access segment LSP from Access Node (AN) to Aggregation Node (AGN) using LDP with longest-match as defined in [RFC5283]. It requires only static routes and it is not necessary to know the actual destination (FEC of the LDP LSP);

2. The Aggregation Node (AGN) stitches the proxy egress LDP LSP with the BGP ingress LSP according to the key of FEC;

3. The remote Aggregation Node (AGN) setup the Ingress LDP LSP to remote Access Node (AN) which has the actual destination.

4. The remote Aggregation Node (AGN) stitches the egress BGP LSP with an ingress LDP LSP according to the key of FEC.

LSPs set up with MPLS TE (RSVP-TE) provide a higher reliability and better QoS as compared to LSPs set up with LDP. So MPLS TE is always adopted to deploy in the mobile backhaul network. But when the mobile backhaul network integrates with the core network based on Seamless MPLS ([I-D.li-mpls-seamless-mpls-mbb]), it is difficult to setup end-to-end MPLS TE LSP spanning multiple domains. The possible way to setup the end-to-end LSP is that the proxy egress RSVP-TE LSP should be able to setup in the mobile backhaul network to stitch with BGP LSP at the Aggregation Node.

4. Solutions

When setup a proxy egress RSVP-TE LSP in the Seamless MPLS scenario as shown in the Figure 1, there are two destination addresses to be carried by the RSVP-TE message:

- Actual destination address: the actual destination address is the destination address of the end-to-end LSP for stitching the proxy egress LSP and the BGP LSP;

o Proxy destination address: the proxy destination address is the address of Aggregation Node which stitches the proxy egress RSVP-TE LSP and BGP LSP.

When set up the proxy egress RSVP-TE LSP on the Access Node, it must specify the actual destination address and the proxy destination address. The Access Node needs to calculate the path based on the proxy destination address for the proxy egress RSVP-TE LSP. Then The Path message will be sent from the ingress node to the proxy destination node which is identified by the proxy destination address in the message. At the same time, the Path message carries the actual destination address of the LSP. When the proxy destination node receives the Path message, it sends back the Resv message to allocate label and reserve resource. And the proxy destination node can use the actual destination address to stitch BGP LSP which has the same address as the actual destination address of the proxy egress RSVP-TE LSP.

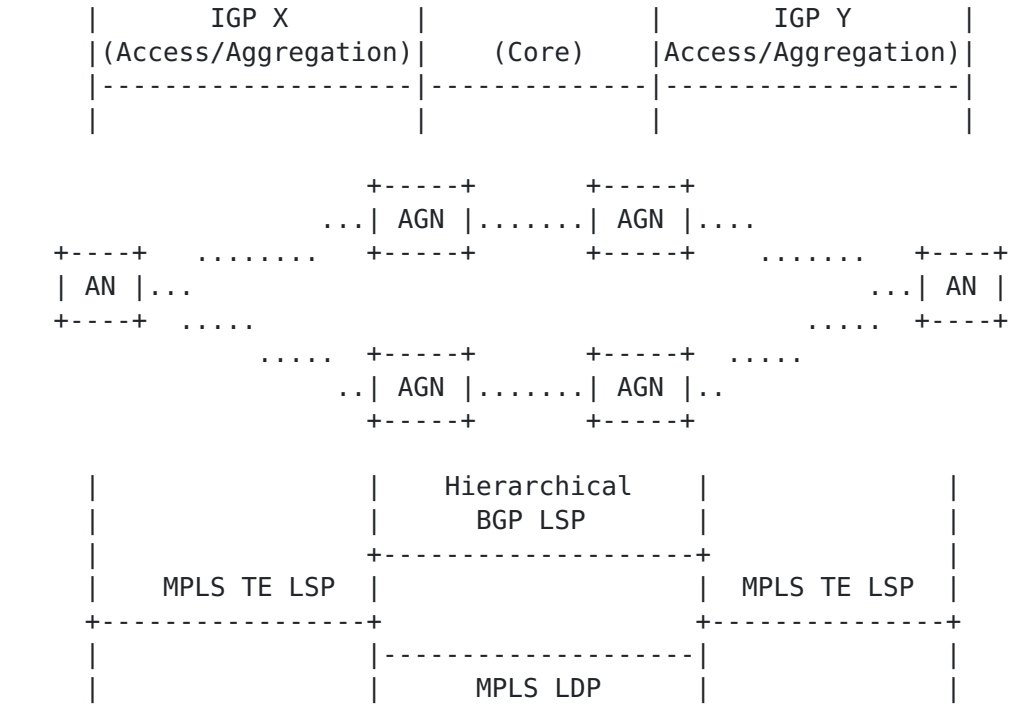


Figure 1 Seamless MPLS Scenario with MPLS TE

In order to support setup of the proxy egress RSVP-TE LSP, the new Proxy Destination Object is introduced to carry the proxy destination address besides the actual destination address which is carried in the Session Object. Both the Session Object and the Proxy

Destination Object are carried in the RSVP-TE Path message and Resv message to set up the proxy egress LSP.

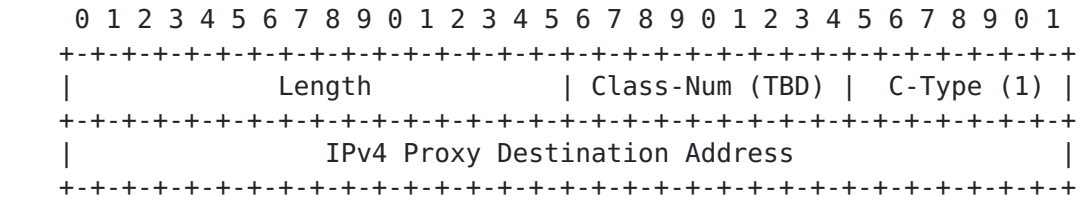
5. Proxy Destination Object

5.1. Format

The Proxy Destination Object is an optional object which MAY be carried in Path or Resv Messages. The Proxy Destination Class-Number is TBD (of form 0bbbbbbb). RSVP-TE routers that do not support the object SHOULD reject the entire message and return an "Unknown Object Class" error.

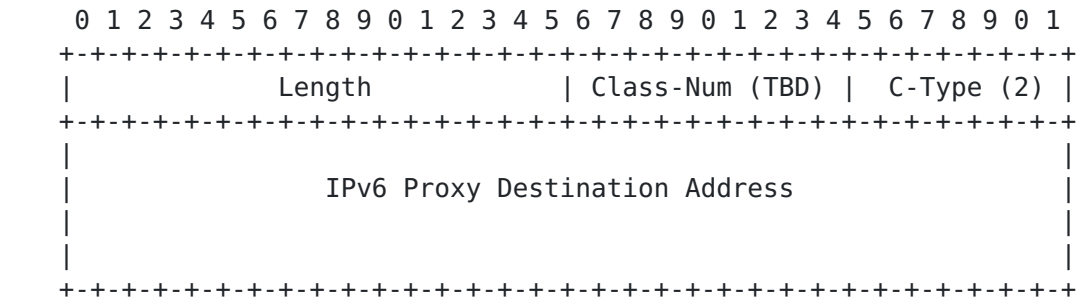
The format of the Proxy Destination Object is as follows:

1. IPv4 Proxy Destination Object



IPv4 Proxy Destination Address: 32 bits. IPv4 address of the proxy destination node of the proxy egress RSVP-TE LSP.

2. IPv6 Proxy Destination Object



IPv6 Proxy Destination Address: 16 bytes. IPv6 address of the proxy destination node of the proxy egress RSVP-TE LSP.

If a message contains multiple Proxy Destination Objects, only the first object is meaningful. Subsequent Proxy Destination Objects SHOULD be ignored and SHOULD NOT be propagated.

5.2. Procedures

When the ingress LSR sets up the proxy egress LSP, the Proxy Destination Object MUST be inserted in the Path message to indicate the address of the proxy destination node and the actual destination address MUST be specified in the Session Object of the Path message. When receive the Resv messages, the ingress LSR SHOULD check if the Proxy Destination object is included. If the Path message includes the Proxy Destination object and the corresponding Resv message does not include this object, the ingress LSR MUST treat the Resv message as wrong messages and MUST NOT set up LSP.

On the transit LSR, when receiving the messages with Proxy Destination object, it MUST include the Proxy Destination object in the outgoing Path or Resv message without change of the object. When it is necessary for the transit LSR to calculate the path, the proxy destination address identified by the Proxy Destination Object MUST be used instead of the actual destination address identified by the Session Object. If the transit LSR receives the Path message including the Proxy Destination object but receives the corresponding Resv message which does not include this object, it MUST treat the Resv message as wrong messages and MUST NOT set up LSP.

On the egress LSR, when receiving Path messages with Proxy Destination object, it MUST include this object in the corresponding Resv message.

6. IANA Considerations

IANA should allocate Class-Num and C-Type for IPv4 Proxy Destination Object and IPv6 Proxy Destination Object which are defined in this document.

7. Security Considerations

This document does not introduce any additional security issues above those identified in [RFC3209].

8. Acknowledgements

The authors would like to thank Loa Andersson for his valuable comments and suggestions on this draft.

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.

[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.

9.2. Informative References

[I-D.ietf-mpls-seamless-mpls] Leymann, N., Decraene, B., Filsfils, C., Konstantynowicz, M., and D. Steinberg, "Seamless MPLS Architecture", draft-ietf-mpls-seamless-mpls-07 (work in progress), June 2014.

[I-D.li-mpls-seamless-mpls-mbb] Li, Z., Li, L., Morillo, M., and T. Yang, "Seamless MPLS for Mobile Backhaul", draft-li-mpls-seamless-mpls-mbb-01 (work in progress), February 2014.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC5283] Decraene, B., Le Roux, JL., and I. Minei, "LDP Extension for Inter-Area Label Switched Paths (LSPs)", RFC 5283, July 2008.

Authors' Addresses

Zhenbin Li
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: lizhenbin@huawei.com

Xinzong Zeng
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: zengxinzong@huawei.com