Point to Multipoint Traffic Engineered MPLS LSPs RSVP-TE Extensions P2MP/MP2MP LDP Label Switched Paths

April 2012

Document ID:ITD-10341v9
Status: Draft

Revisions

Date	Revisions/Changes
8/30/06	**First Draft**
8/31/07	**Updated Reference**
3/1/09	**Updated**
3/2/10	**References brought up to date**
1/9/2011	**Added test cases for mLDP for P2MP/MP2MP LSPs**
03/24/2012	**Updated testcase and reference**
08/28/2012	**Updated testcase and reference**

TABLE OF CONTENTS

1 Introduction

This document provides a test plan to further test MPLS Traffic Engineering for P2MP LSPs.

This test plan addresses the requirements for signaling techniques used for P2MP LSPs according to RFC 4461. P2MP TE LSPs provide efficient MPSL traffic engineering by avoiding unnecessary packet replication at the ingress routers. A P2MP LSP uses sub-LSPs to reach multiple destinations (egress LSRs). This document mainly focuses on RSVP-TE requirements for establishment and maintenance of P2MP LSPs.

LDP has been extended to support the multicast through RFC 6388 in IETF to address the creation of P2MP and MP2MP LSPs, generally referred as multipoint LSPs. mLDP is receiver driven and the LSP path selection is based on the root address (shown in the figure 2). It uses downstream on demand label allocation, which implies that the labels are allocated when the receiver needs one. All implementations support mLDP extension require to support the LDP capabilities negotiation as defined in the RFC 5561 and at least support one of the P2MP or MP2MP TLVs. mLDP defines the FEC elements for multipoint LSPs – P2MP, MP2MP downstream and MP2MP upstream FEC elements which are capable of carrying opaque values. This document presents some basic interoperability tests verifying the functionality of the mLDP in a multivendor environment. Figure 2 shows a general purpose setup, the actual test setup may vary based on the number of participants.

This document is work-in-progress and will be refined and updated based on the input from test participants (vendors) and carrier members of Isocore Internetworking lab.

2 Sample Test Topology

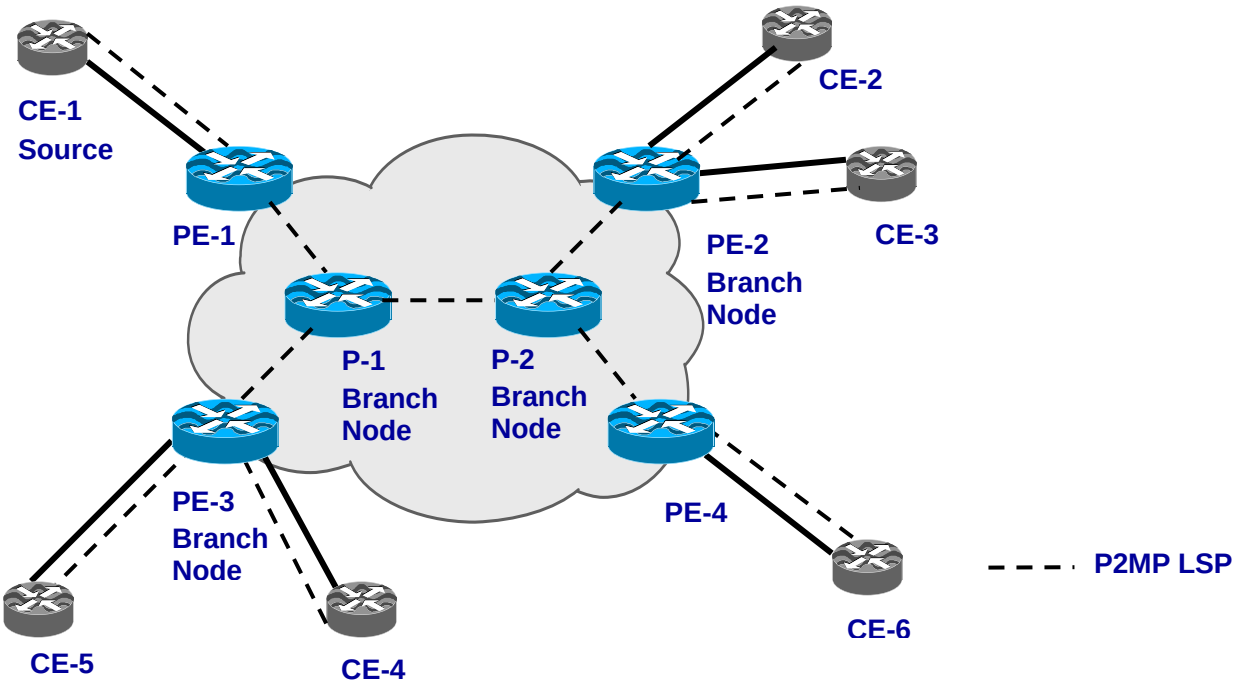

Figure 1: RSVP-TE P2MP Tunnels

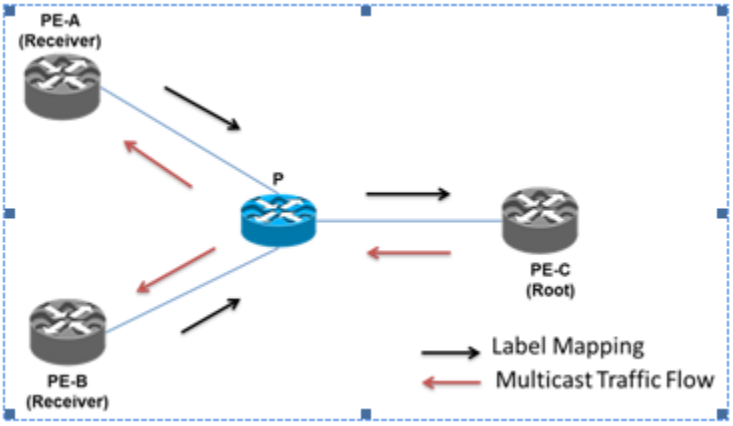

Figure 2: mLDP Setup with root, receivers and P router holding the P2MP state

3 Test Areas – P2MP RSVP-TE

3.1 Test Case: Addition of Sub-LSPs

Purpose: Verify that sub-LSPs can be added to the main P2MP LSP without affecting the traffic and other sub-LSPs.

Procedure:

1. In the above figure configure CE1 with a main LSP.
2. For this main LSP, configure 3 Sub-LSPs to CE2 through CE4.
3. Verify that the paths are established.
4. Add the fourth sub-LSP to CE5 through PE2.
5. Verify that this path is established without disrupting the other sub-LSPs.

3.2 Test Case: Removal of Sub-LSPs

Purpose: Verify that sub-LSPs can be removed from the main P2MP LSP without affecting the traffic and other sub-LSPs.

Procedure:

1. In the above figure configure CE1 with a main LSP.
2. For this main LSP, configure 4 Sub-LSPs to CE2 through CE4.
3. Verify that the paths are established.
4. Remove two sub-LSPs; for example, remove the path to CE2 and CE5.
5. Verify that these paths are removed without disrupting the other sub-LSPs.

3.3 Test Case: Verify Link Protection for Sub-LSPs

Purpose: Verify that if a sub-LSP goes down, the bypass LSP is used while recovering the failure.

Procedure:

1. Configure link protection on the each sub-LSP
2. Configure Link protection on the RSVP interfaces for the routers on the path of the Sub-LSP
3. Verify that the bypass link is established
4. Bring down a sub-LSP by removing a link.
5. Verify that the Bypass LSP is used and the destination is still reachable.

3.4 Test Case: Verify DiffServ on P2MP LSPs

Purpose: Verify that all the packets belonging to a particular FEC and originated from a particular node follow the same P2MP tree.

Procedure:

1. Configure a several P2MP TE LSPs with several sub-LSPs on the ingress LSR.
2. Configure Diffserv TE classes for different incoming traffic types.
3. Verify that the traffic which belong to the same class traverse the same P2MP LSP.

3.5 Test Case: Verify QoS Parameters

Purpose: Verify that QoS parameters such as priority and bandwidth set by the ingress LSR are not changed by the downstream LSRs.

Procedure:

1. Configure QoS parameters such as bandwidth and priority for the P2MP outgoing interface on the ingress LSR.
2. Verify that these requirements are signaled to all the LSR including branching LSRs.
3. Verify that packets belonging to a particular P2MP tree retain the end to end QoS requirements after each hop.

3.6 Test Case: Verify the co-existence of P2P LSPs and P2MP LSPs

Purpose: Verify that P2MP and P2P TE LSPs can be signaled on the same interface.

Procedure:

1. Configure several P2MP LSPs each with several sub-LSPs on the ingress LSR.
2. Configure P2P LSP on the same LSR, same interface.
3. Verify that the paths belonging to both P2MP and P2P LSPs are established.
4. Verify that the branching LSR can act as a transit LSR for the P2P LSP path.

3.7 Test Case: Verify the RSVP sessions for P2MP LSPs

Purpose: Verify that that RSVP session maintains P2MP sessions for ingress, transit, and egress states.

Procedure:

1. Configure several P2MP LSPs each with several sub-LSPs on the ingress LSR.
2. Configure RSVP for each P2MP LSP on all the LSRs.
3. Verify that the RSVP P2MP sessions are established on the ingress LSR as well as transit and egress LSRs.

4 Test Case: mLDP

4.1 Test Case: Verify the basic P2MP LSP setup with LDP with P2MP FEC elements – consider the following tree types

4.1.1.1 Tree Type considerations (primarily for address family IPv4, IPv6 if interest and support exists) –

4.1.1.2 P2MP

4.1.1.3 MP2MP Downstream

4.1.1.4 MP2MP Upstream

4.2 Test Case: Verify the basic P2MP LSP with P2MP FEC elements using different opaque values

4.2.1.1 Opaque Types considered

4.2.1.2 IPv4

4.2.1.3 MP2MP Downstream

4.2.1.4 MP2MP Upstream

4.3 Test Case: Verify the basic MP2MP LSP setup with LDP using MP2MP FEC elements

4.4 Test Case: Verify the support for LDP MP Status TLV

4.5 Test Case: Verify the in-band signaling for assigning multicast flows to a multipoint LSP

Figure 2 reference network that will be used for the various configuration scenarios

4.5.1 PIM-SSM Transit Application

PIM-SSM transit supports the forwarding of (S, G) states at the IP edge across the MPLS core. It can be summarized as follows:

- Supports (S, G) transit for both IPv4 and IPv6 multicast
- Carried across MPLS core using a P2MP LSP
- Opaque value comprises the (S, G) value of the transit stream
- Signaling is done in-band
- Source prefixes (at PEs) are distributed using BGP
- Root derived from BGP next-hop of source
- No PIM necessary in MPLS core
- PIM at edge
- P2MP LSP in core

4.5.2 Multicast VPN Application

The Multicast VPN solution (mVPN) is based on Multicast Distribution Trees (MDT), which are tunnels built over a core network. Customer multicast traffic is then transported/tunneled via these MDTs. The mVPN architecture has been designed to be independent of the tunneling mechanism used to create the MDTs.

MLDP creates the MDTs as follows:

- The Default MDT uses MP2MP LSPs
    - Supports low bandwidth and control traffic between VRFs
- The Data MDT uses P2MP LSPs
    - Supports single high bandwidth source stream from a VRF

All other operation of mVPN remains the same regardless of the tunneling mechanism:

- PIM neighbors in a VRF are seen across an LSP-VIF
- VPN multicast state is signaled by PIM

4.5.3 Direct MDT (VPNv4) Application

The Direct MDT or VPNv4 Transit is very similar in its operation to the PIM-SSM Transit application. The difference is that a direct MDT is VPN specific and uses the RD along with the (S, G) in the Opaque value to make an MP LSP unique. Direct MDT uses in-band signaling; that is, the Opaque Value is derived from the multicast flow and is used to signal the mapping between the LSP and the VPN multicast flow.

With mVPN, you normally need a Default MDT for control traffic (PIM) and low bandwidth sources. The Default MDT would then be used to send Join TLV to signal a move to a Data MDT. Direct MDT does not require the Default MDT mechanism and its associated PIM signaling to create what looks and behaves like a Data MDT; instead it uses a P2MP LSP with in-band signaling. There is no PIM adjacency running over the Direct MDT LSP.

The Direct MDT application would benefit Multicast VPNs, where the there are limited high bandwidth sources constantly sending traffic to a number of receivers spread around the MPLS network.
Another benefit of Direct MDTs is that they support the building of extranet P2MP LSPs, which will be discussed further in the chapter. The VPN (S, G) states can be selectively filtered to use a Direct MDT or Default/Data MDTs.

In summary, Direct MDTs:

- Are similar to IPv4 transit LSP but for VPN traffic
  - Use in-band signaling of (S, G) along with RD in Opaque Value
- Do not use Default/Data MDT control planes
- Use VPN Multicast state signaled in-band like IPv4 transit
  - One P2MP LSP per (S, G) state within VPN (SSM Only)
- Have extranet multicast streams that are supported
- Can be used in conjunction with Default/Data MDTs
  - (S, G) operation can be selective within VPN
  - Either over Direct MDT or Default MDT
- Are useful for VPNs with a limited number of states

4.6 Test Case: Verify the out-of-band signaling for assigning flows to a multipoint LSP

4.6.1.1 Consider the following options for overlay protocol –

a. **PIM**

b. **BGP**

5 Layer 3 VPN Services – Different Flavors of P-tunnels instantiating PMSIs

5.1.1.1 mVPN with GRE

5.1.1.2 mVPN with P2MP LSPs

5.1.1.3 mVPN with mLDP and BGP AD

5.1.1.4 mVPN with mLDP with no auto discovery

5.1.1.5 NG-MVPN for both P2MP and mLDP with I-PMSI

References

[1]"Signaling Requirements for Point to Multipoint Traffic Engineered MPLS LSPs", RFC 4461, April 2006.

[2]"Extensions to RSVP-TE for Point to Multipoint TE LSPs", RFC487, May 2007

[3] "Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths", RFC6388, April 2011

[4] "Multicast in MPLS/BGP IP VPNs", RFC6512, February 2012

[5]" BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs", RFC6515, February 2012

[6]" mLDP based in-band signaling for Point-to-Multipoint and Multipoint-to- Multipoint Label Switched Paths", draft-wijnands-mpls-mldp-in-band-signaling-02