MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 2, 2012

G. Liu
ZTE Corporation
Y. Ji
Beijing University of Posts and Telecommunications
j. Yu
X. Xu
ZTE Corporation
Z. Du
Beijing University of Posts and Telecommunications

March 1, 2012

Multiprotocol Label Switching Transport Profile p2mp Shared Protection
draft-liu-mpls-tp-p2mp-shared-protection-03

Abstract

This document will describle two protection solutions to support protection of failures in p2mp path in MPLS-TP. According to the protection Requirements in RFC 5654, there are requirements for MPLS-TP to support sharing of protection resources such that protection paths that are known not to be required concurrently can share the same protection resources. In addition, there is a requirement for MPLS-TP to support unidirectional 1:n protection for p2mp paths. These requirements are further addressed in draft-ietf-mpls-tp-survive-fwk . so this draft will present proposed solutions .

This document is a product of a joint Internet Engineering Task Force(IETF) / International Telecommunications Union Telecommunications Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionalities of a packet transport network as defined by the ITU-T.

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 September 2, 2012.

Table of Contents

1. Introduction

This document describes protection solutions for MPLS-TP p2mp paths. The first solution is based on extending 1:1 protection solution to implement 1:n protection by using one shared protection p2mp path when there may have failures on the protected working p2mp paths. A second solution uses one p2mp protection path to protect each protected p2mp working path, and these p2mp protection path maybe share common segment resource. when detecting defects on a p2mp working path to implement (1:1)^n protection. Both protection solutions satisfy and fulfill requirement 69 and 67B in [RFC 5654]. These solutions can't exclude 1+1 and 1:1 protection solutions for p2mp path in draft-ietf-mpls-tp-survive-fwk and draft-ietf-mpls-tp-linear-protection. it will be used to implement the requirement of recovery for p2mp path. If only 1+1 protection is used for p2mp path, there need to set up a disjoint protection path for each working path, This will increase the cost of maintaining and monitoring each of these paths (i.e. both the working and protection paths). In addition, since the p2mp service must be transported on both the working and protection paths at the same time, more bandwidth resource will be wasted for the p2mp service . Due to these limitations and defects, it is neccesary to consider using shared protection resources for many p2mp working paths.

2. Conventions used in this document

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.

OAM: Operations, Administration, Maintenance

LSP: Label Switched Path.

TLV: Type Length Value

P2MP:Point to Multi-Point

P2P:Point to Point

PSC:Protection Switching Coordination

SD:Signal Degrade

SF:Signal Fail

RDI:Remote Defect Indication

MPLS:Multi-Protocol Label Switching

MPLS-TP:Multi-Protocol Label Switching Transport Profile

ME: Maintenance Entity

MEP:MEG End Point

ACH: Associated Channel Header

CC-V: Contunuity Check-Verification;

3. p2mp shared protection solution

This section describes two types of p2mp shared protection solutions. The first proposed solution utilizes one p2mp protection path to protect many p2mp working paths . When a protected p2mp working path detects a failure, the leaf node of the p2mp working path will notify its own root node of defective message by RDI packet by return path. If there is no other higher priority protected p2mp working path or control command that requires the use of the protection path, then the defective p2mp service packet will switch to p2mp protection path to be transported. All leaf nodes of the defective p2mp path will select protection path to receive p2mp service packets.

The second proposed solution utilizes one p2mp protection path to protect its corresponding protected p2mp working path.and these protection paths maybe shared common segment resource. When a failure is detected on a protected p2mp working path, the leaf node which has already detected the failure will notify root node of the failure message. then the root node of protection path will be basis on the priority of protected service or failure to select the highest priority service to be protected. then it will notity all leaf nodes of which working path will be protected by extensive PSC packet as the following figure 1.As a result, the selected failure service will switch to the protection path to be transported .

The two p2mp shared protection solutions separately implement 1:n and (1:1)^n protection for p2mp path, The following sub-section describes the protection switching methods in detail.

3.1. 1:n protection

The 1:n protection solution should be similar to 1:1 protection solution described in [survivability-framework] to use one protection path to protect many p2mp working paths. However, in this mechanism since the protected traffics are transported by different working

path. Its implication regarding the p2mp protection path will be configured between the protection domain root node and all leaf nodes of protected p2mp working paths. when a leaf node of a protected p2mp working path detect a failure, The leaf node should generate RDI packet to notify its own root node of the defective message . When the root node of the p2mp working path receives the RDI packet and knows some failures in one or more one branch path of the p2mp working path, it may send protection switch requirement control packet to the root node of its own protection path or access node of the protected p2mp service. When the root node of the protection path receives the protection switch requirement control packet from any root node of the protected defective p2mp working path The root node of the protection path MUST choose one defective path to be protected based on the priority of these protected defective p2mp working paths. Then the root node of protection path SHALL generate extensive PSC packet including the selected p2mp defective path identifier in a TLV field of the message packet .The following figure 1 is the format of extensive PSC packet .Then it will send the extensive PSC message to all leaf nodes of the p2mp protection path .

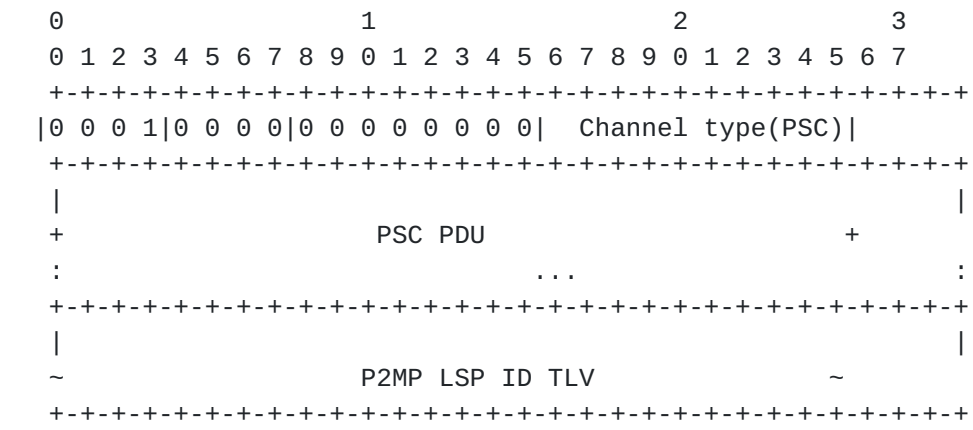


Figure 1

NOTE:

P2MP LSP ID TLV: a standard TLV frame structure. including Type , Length,and Value, and the value field may be identifier of p2mp LSP which have defect and need to be protected. this p2mp LSP ID TLV format is as the following figure 2

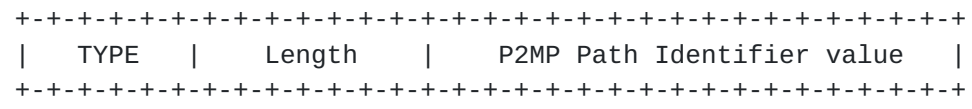
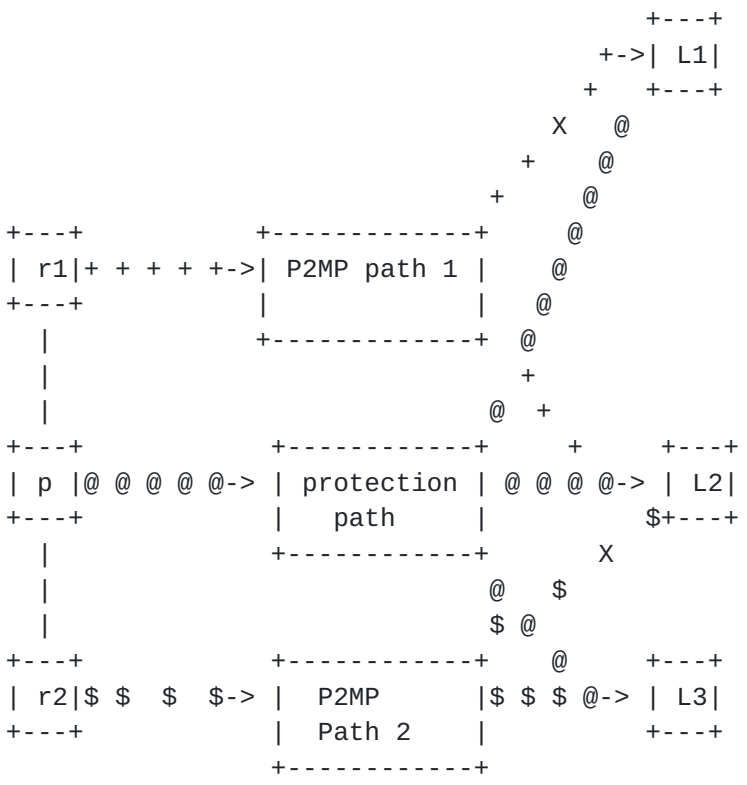


Figure 2

At the same time, the root node of the protection path generates notify message control packet including selective protected working path identifier and send it to the root node of each defective p2mp working path by control channel ,so the root node of each defective p2mp working path can know whether it may be selected to be protected based on the notify message control packet. If it has already been selected to be protected, it will stop sending service packet on the p2mp working path Then the protected service will switch to the p2mp protection path to be transported.

On the other hand, all leaf nodes of the protection path receive the extensive PSC message by the protection path. Then they will know whether to accept and process the service packet from the protection path based on p2mp LSP ID TLV field in the extensive PSC packet. If the leaf node is a sink node of the protected service, it will accept and process the service packet from the protection path. Or else, it will drop the service packet.

the implement in detail as the following figure is 1:2(n=2) protection instance.



NOTE:
@@@@@@: p2mp protection path
+++++: p2mp working path 1
$$$$$: p2mp working path 2
X: failure

Figure 3

For the above p2mp network topology , there are two different p2mp services which need to be transported separately by p2mp working path 1(r1-p2mp path 1-L1,L2) identified by (+) and p2mp working path 2(r2- p2mp path 2-L2,L3) identified by ($) . under normal condition. the p2mp service from root node r1 will be sent and transported to leaf nodes L1,L2 by p2mp working path 1, and another p2mp service from the root node r2 will be sent and transported to leaf nodes L2,L3. in addition, only one p2mp protection path (P-protection path-L1,L2,L3)identified by (@) is used to protect the p2mp working path 1 and the p2mp working path 2. supposing the priority of p2mp working path 1 is higher than p2mp working path 2. if there is a

failure on separately branch path(r1-p2mp path 1-L1) of p2mp working path 1 and branch path(r2-p2mp path 2-L2) of p2mp working path 2, Leaf node L1 and leaf node L3 will separately send RDI packet to root node r1 and root node r2 by return path. when root node r1 and r2 received the RDI packet and processed it. then the control packet of protection switch requirement will be sent to the root node P of protection path by control channel . Then the root node P will choose one working path to be protected. As the priority of p2mp working path 1 is higher than p2mp working path 2. so the root node P of protection path will select p2mp working path 1 to be protected, and send extensive PSC packet including p2mp LSP ID TLV to all Leaf nodes(L1,L2,L3) of the protection path. At the same time, It will generate response control packet for the protection switch requirement of the root node r1 and r2. the service of the working path 1 will be selected to be protected. So the root node r1 of working path 1 will stop sending its p2mp service in the working path 1, Then the service of the working path 1 will switch to the protection path to be transported. on the other hand, for leaf nodes(L1,L2,L3), when they received the extensive PSC packet from the root node P, They will decide whether to accept and process the service packet from the protection path based on selective protected working path identifer. As leaf nodes(L1,L2) are the leaf nodes of p2mp working path 1, they will both accept and process the service packet from the p2mp protection path. but for leaf node L3, as it is not the leaf node of p2mp working path 1. it will drop the service packet from the p2mp protection path. While the service of p2mp working path 2 can't be selected to be protected, so the root node r2 will continue to send their own service packet by p2mp working path 2.

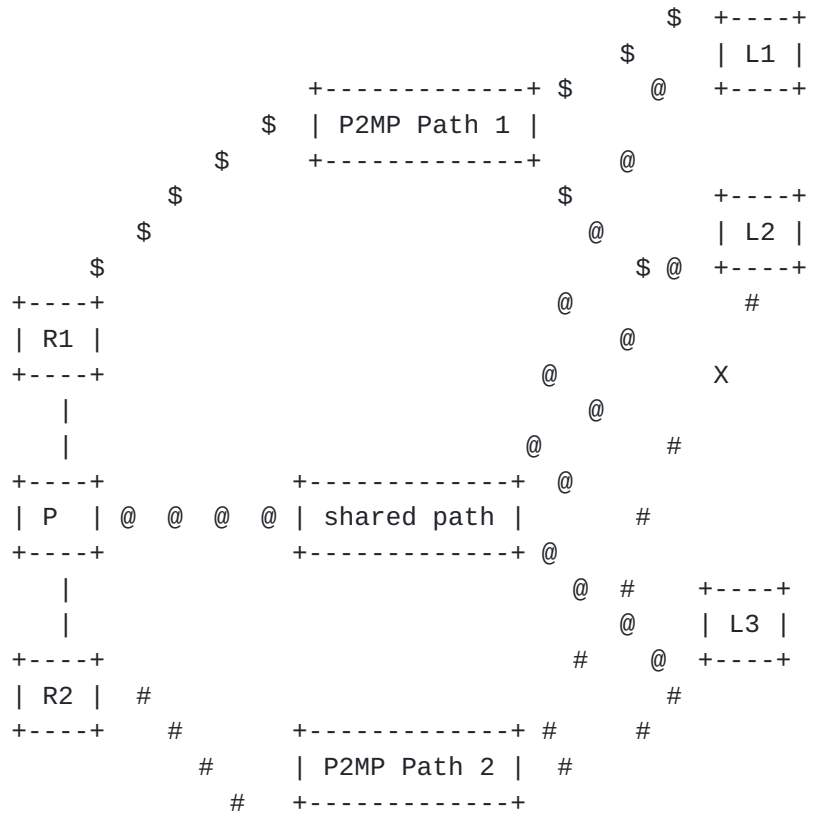
3.2. (1:1)^n protection

This protection solution can use p2mp protection path to protect its corresponding p2mp working path.and these protection paths will share a few common segment resource.when a failure is detected on some protected p2mp working path, it must notify the failure message to the root node of its corresponding protection path. when the root node of the protection path received the failure message, it must compare the priority among these protection paths and select the highest priority service to be tranported on its corresponding protection path.and it notify each leaf node of the protection path which protection path will be selected to use the common protection resource by extending PSC message.

for example, there is a (1:1)^2(n=2) protection instance as the following figure 4:

there are two p2mp working paths : p2mp working path 1(r1-p2mp Path

1-L1,L2) identified by ($) and p2mp working path 2(r2-p2mp Path 2-L2,L3) identified by (#).in order to protect the service, its corresponding protection path(P-shared path-L1,L2) and (P-shared path-L2,L3) identified by(@) will be pre-configured for working path 1 and working path 2. and the two protection path will share common segment.



NOTE:
@: P2MP protection path LSP;
$: P2MP Working Path LSP 1
#: P2MP Working Path LSP 2
X: failure

Figure 4

when the p2mp working path LSP 1 and the p2mp working path LSP 2 have a failure at the same time, The leaf node L2 will generate failure notify message to send to the root node R1 and R2 . Then R1 and R2 will notify the root node(P) of the failure. so the root node P will select the higher priority working path to be protected and notify all leaf nodes of the protection path which working path will be protected by extensive PSC packet including selective protected p2mp LSP identifier. when these leaf nodes receive the extensive PSC packet, they decide which path to receive the service packet. here if the root node P select working path 1 to be protected. so the leaf nodes L1,L2 will receive the service packet from protection path(P-shared path-L1,L2).but the leaf nodes(L2,L3) of the working path 2 will still receive the service packet from their working path 2. .

3.3. Conclusion

The two types of p2mp protection solution will individually implement 1:n and (1:1)^n protection for p2mp service. They can fulfill the requirement of unidirectional p2mp protection and sharing protection resource. .

4. Security Considerations

The security considerations for the authentication TLV need further study.

5. IANA Considerations

TBD.

6. Acknowledgments

The authors would like to thank yaccov for giving a lot of good comments and revising many syntax for the document. And thank Malcolm Betts and other experts for Providing some good comments and their input to and review of the current document .

7. References

7.1. Normative References

[RFC 5654]
IETF, "IETF RFC5654(MPLS-TP requirement)", September 2009.

[RFC 5921]
IETF, "IETF RFC5654(MPLS-TP framework)", July 2010.

[RFC 6372]
IETF, "MPLS Transport Profile (MPLS-TP) Survivability Framework", September 2011.

[RFC 6378]
IETF, "MPLS Transport Profile (MPLS-TP) Linear Protection", November 2011.

7.2. Informative References

[L2VPN ICCP]
Luca Martini, Samer Salam, Ali Sajassi, Satoru Matsushima, Matthew Bocci, Thomas D. Nadeau, "Inter-Chassis Communication Protocol for L2VPN PE Redundancy", Oct 2010.

[MPLS-TP linear protection]
Z.Haiyan, I.umansky, L. han,J.Ryoo, D'Alessandro , "Linear Protection Switching in MPLS-TP", July 2010.

7.3. URL References

[MPLS-TP-22]
IETF - ITU-T Joint Working Team, "", 2008, <http://www.example.com/dominator.html>.

Authors' Addresses

Liu guoman
ZTE Corporation
No.68, Zijinghua Road, Yuhuatai District
Nanjing 210012
P.R.China

Phone: +86 025 52871606
Email: liu.guoman@zte.com.cn

Yuefeng Ji
Beijing University of Posts and Telecommunications
P.O. Box 128, No.10, Xi Tu Cheng Road
Beijing 100876
P.R.China

Email: jyf@bupt.edu.cn

Yu jinghai
ZTE Corporation
No.68, Zijinghua Road, Yuhuatai District
Nanjing 210012
P.R.China

Phone: +86 025 52871606
Email: yu.jinghai@zte.com.cn

Xu xueqiong
ZTE Corporation
No.68, Zijinghua Road, Yuhuatai District
Nanjing 210012
P.R.China

Phone: +86 025 52871606
Email: xu.xueqiong@zte.com.cn

Zongpeng Du
Beijing University of Posts and Telecommunications

Email: duzongpeng@gmail.com