

MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 29, 2011

G. Liu
J. Yang
l. Jiang
z. Fu
ZTE Corporation
September 25, 2010

Multiprotocol Label Switching Transport Profile Ring Protection draft-liu-mpls-tp-ring-protection-01

Abstract

according to [RFC 5654](#) MPLS-TP Requirement, there are two requirements : requirement 56.B Recovery techniques used for P2P and P2MP should be identical to simplify implementation and operation. another requirement as [section 2.5.6.1](#) describes: within the context of recovery in MPLS-TP networks, the optimization criteria considered in ring topologies are as follows: 1 minimize the number of OAM entities that are needed to trigger the recovery operation; 2 Minimize the number of elements of recovery in the ring; 3 Minimize the number of labels required for the protection paths across the ring; 4 minimize the amount of control and management plane transactions during maintenance operation. this document will describe and provide two types of ring protection solutions. both solutions can satisfy these requirements of recovery in mpls-tp ring network.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

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 March 29, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	3
3.	proposed ring protection solution	4
3.1.	sub-path tunnel protection solution	4
3.2.	Extend Steering protection	8
3.2.1.	P2P Service Protection	8
3.2.2.	P2MP Service Protection	10
3.3.	Comparison	13
4.	Security Considerations	15
5.	IANA Considerations	15
6.	Acknowledgments	15
7.	References	15
7.1.	Normative References	15
7.2.	Informative References	15
7.3.	URL References	16
	Authors' Addresses	16

1. Introduction

this draft mainly describes two new ring protection solutions, solution 1 is based on sub-path Tunnel protection solution to implement to protect all kind of service by protecting sub-path when there are a few faults or defects in the ring .and there are fewer Sub-Path Tunnels to be set up in the ring network. while solution 2 is based on Steering protection solution of G.8132 to be able to implement to protect P2P or P2MP service very quickly. at last it provides the comparsion of the two ring protection solutions from the view of a protection performance and effect.

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

LSR:Label Switching Router

P2MP:Point to Multi-Point

P2P:Point to Point

APS:Automatic Protection Switch

PSC:Protection Switching Coordination

SD:Signal Degrade

SF:Signal Fail

BFD:Bidirectional Forward Detection

MPLS:Multi-Protocol Label Switching

MPLS-TP:Multi-Protocol Label Switching Transport Profile

TTSI:Trail Termination Source Identifier_source LER ID+LSP ID

MEP:MEG End Point

LER: Label Edge Router

PST: Path Segment Tunnel

SPME: Sub-Path maintenance entity

3. proposed ring protection solution

this section mainly proposed two types of ring protection solution. the two ring protection solutions need to detect and notify the failure of the ring by OAM or APS functions, so that the source node of working sub-path tunnel and LSP path will switch these protected services into protecting sub-path tunnel and LSP path. but the two ring protection solutions also have a few differences. solution 1 provide protection of all failure LSP services of a working sub-path tunnel by setting up protecting sub-path tunnel, while the later ring protection solution provides one dedicate protection path for each working LSP path to protect and recovery all failure services in the ring.

3.1. sub-path tunnel protection solution

This ring protection solution in MPLS-TP network mainly make use of protecting sub-path tunnel to protect all LSP services of a failure working sub-path tunnel. firstly two prime transfer nodes will be selected for the ring. and the two prime transfer nodes would backup for each other to ensure to transport service under the condition that one prime transfer node has failure. and other nodes in the ring need to pre-configured and set up two bidirectional sub-path tunnel separately in the direction of clockwise and anticlockwise along the ring to the two prime transfer nodes; and there is CC or CV packet to verify the connectivity of every sub-path tunnel. and each sub-path Tunnel will reserve 50 percent bandwidth or capacity to use for protecting another working sub-path tunnel.

when an end node of a working sub-path tunnel detects a failure in its own sub-path tunnel by OAM function, it will generate a State notify message (APS or PSC) to send to another end node of the sub-path tunnel through pre-configured relative protecting sub-path. and the frame format of the state notify message is as the following:

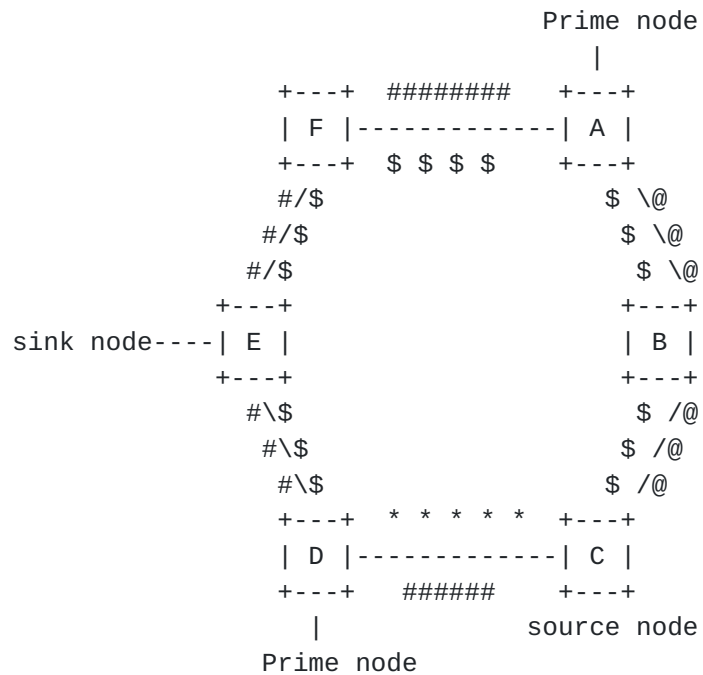

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 0001| 0000 |      00000000      | channel type (APS or PSC)|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
|                      state control message                      |
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Figure 1

when another end node of the sub-path tunnel received State Notify message from peer node, it would process the message and switch to its relative protecting sub-path to transport all LSP Services of the failure working sub-path tunnel. for example, there is the following ring include A ,B, C,D,E,F node. and A and D node is configured as two prime transfer nodes separately for the ring.while working and protecting sub-path tunnel will be set up and pre-configured between two primer transfer nodes A ,D and other nodes include B,C,D,E,F.it will need to configure and set up 16 sub-path tunnel in the ring. for C node, there need to set up four bidirectional sub-path tunnels,which are separately working sub-path tunnel(A-B-C) identified by signal (@) and protecting sub-path tunnel (A-F-E-D-C) identified by signal (#) between Prime node A and source node C . at the same time, they are including bidirectional working sub-path tunnel(C-D) identified by signal(*) and protecting sub-path tunnel(C-B-A-F-E-D) identified by signal(\$) between prime node D and source node C, as the following figure.



NOTE:

- @: working sub-path tunnel between A and C
- #: protecting sub-path tunnel between A and C
- *: working sub-path tunnel between C and D
- \$: protecting sub-path tunnel between C and D

Figure 2

For a LSP service from source node C to sink node E ,under normal contidion,it would push into working sub-path tunnel (w)PCA|LC(A)|BOS firstly,then it will pop sub-path tunnel label and swap LSP label in the prime transfer node A .and then push into another sub-path tunnel (w)PAE|LA(E)|BOS and transport to sink node E. here PXY denotes a sub-path tunnel from LSR-X to LSR-Y , '|' can be used to separate each level in label stack .LX(Y) denotes a LSP service from LSR-X to LSR-Y. BOS denotes the bottom of label stack. when it detects a failure in the working sub-path tunnel(C-B-A) by OAM function as the following figure.

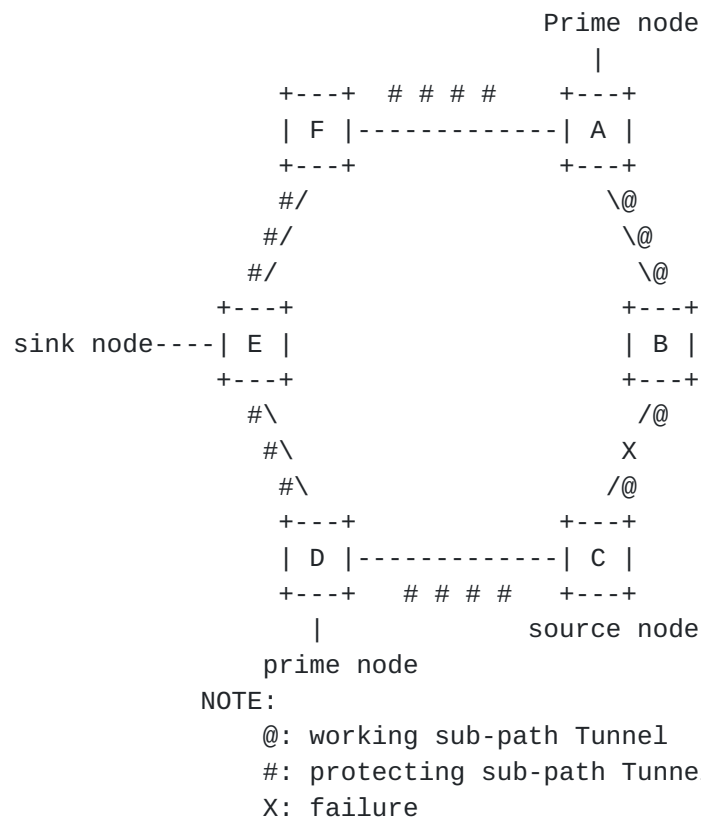


Figure 3

for example, there is a failure in the link(C-B),all LSP services which would be carried and sent between C and prime node A by working sub-path tunnel(C-B-A) should switch to protecting sub-path tunnel(C-D-E-F-A) and push into protecting sub-path tunnel(P)PCA|LC(A)|BOS and be transported by the protecting sub-path tunnel if the protecting sub-path tunnel has no failure at the same time. when it arrived at the prime node A through the protecting sub-path tunnel, the outer-top SPME label would be popped and swap LSP label in the prime transfer node A, then the LSP service would push into another working sub-path tunnel (w)PAE|LA(E)|BOS and be carried to sink node E .in addtion, when the prime transfer node A is bad or the relative protecting sub-path tunnel has failure too, another prime transfer node D will become active prime transfer node for the LSP service. All LSP services of working sub-path tunnel(C-B-A) would push into working sub-path tunnel(C-D) (w)PCD|LC(D)|BOS to be sent to backup prime node D, and then POP outer-top sub-path tunnel label and swap LSP label.then the LSP service would push into another sub-path tunnel (w) PDE|LD(E)|BOS and be carried and sent to sink node E.

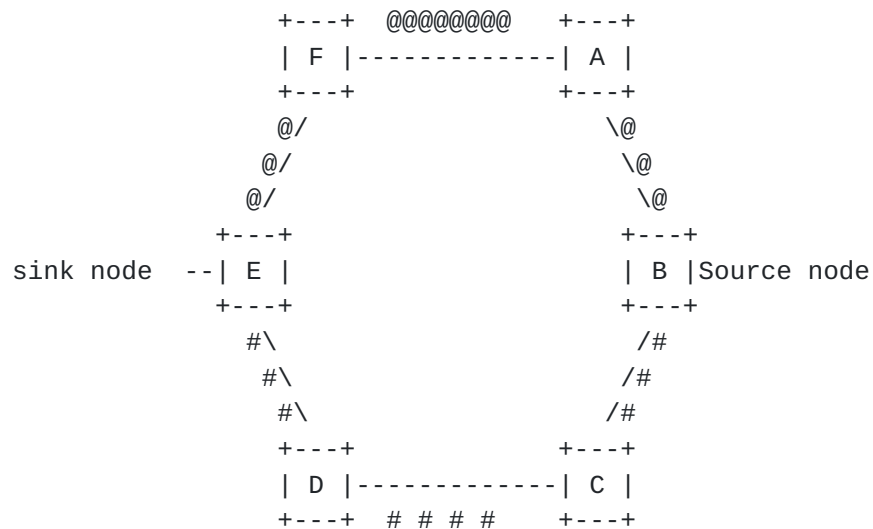
From the number of configuring sub-path tunnel, if there are n nodes in the ring, there only need to set up and configure $(n-2)*2$ working sub-path tunnels and $(n-2)*2$ protecting sub-path tunnel. if configuring one working sub-path tunnel and one protecting sub-path tunnel between each node and other nodes of the ring, then there need to set up and configure $O(n^2)$ sub-path tunnels. so this solution may solve the N square problem.

3.2. Extend Steering protection

This ring protection solution can extend G.8132 Steering protection solution to simply, quickly and effectively protect LSP service include p2p or p2mp in the MPLS-TP network ring. in order to protect and restore all failure services when a failure has happened in the ring. firstly each LSP path should configure one working LSP path and one protecting LSP path in the ring. and the direction of the two LSP path is reverse in the ring. when a failure has been detected by OAM function of section layer, a state notify message packet will be generated and sent to other nodes in the ring by control channel or other channel very quickly for the first three packets. when other nodes receive the state notify message packet, they would analysis and judge which LSP service would be affected by the failure by state notify message or PRO of each LSP in the node.

3.2.1. P2P Service Protection

if the LSP service affected by the failure is P2P service, the source node of the LSP service would switch into its own protecting LSP path to transport to the sink node. while the sink node of the LSP service would select protecting LSP path to receive the service. for example, now there is a LSP service from B to E as the following figure. its working LSP path is B-A-F-E identified by signal @, while its protecting LSP path is B-C-D-E. Under normal state, the LSP service would be sent by the working LSP path in the source node. while be received by selecting working LSP path in the sink node.



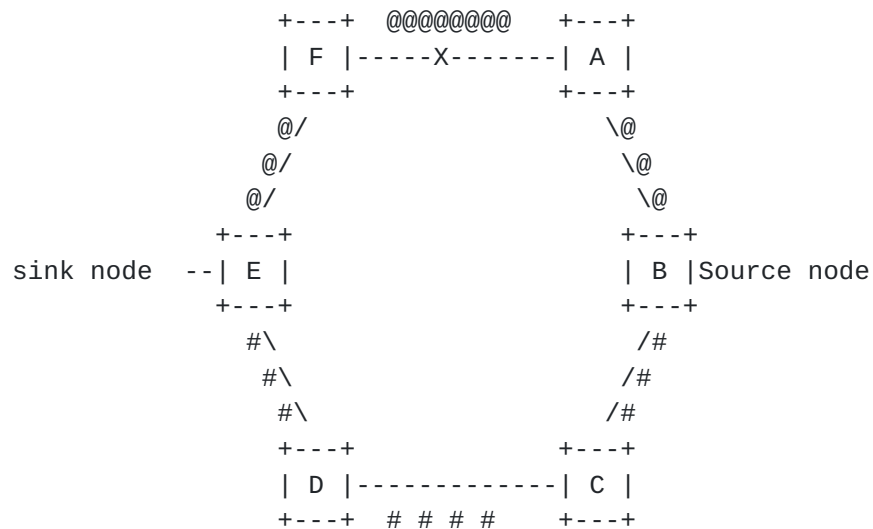
NOTE:

@: working LSP path;

#: protecting LSP path;

Figure 4

if there is a failure in the working LSP path. for example a failure happened in the link A-F as the following figure. node A or F would detect a failure by section CC&CV packet firstly. then node A or F would generate state notify message to other nodes in the ring. when other nodes of the ring received the state notify message, they would receive and process the state notify message. for the source node B and sink node E of the LSP service, they would analysis and judge whether the LSP service would be affected by the failure based by state notify message and PRO of each LSP in the node. as the link(A-F) failure would affect working LSP path of the LSP Service. the source node B of the LSP service would switch to bridge to protecting LSP path. At the same time, the sink node E of the LSP Service would select protecting LSP path to accept service.



NOTE:

@: working LSP path;
 #: protecting LSP path;
 X: failure

Figure 5

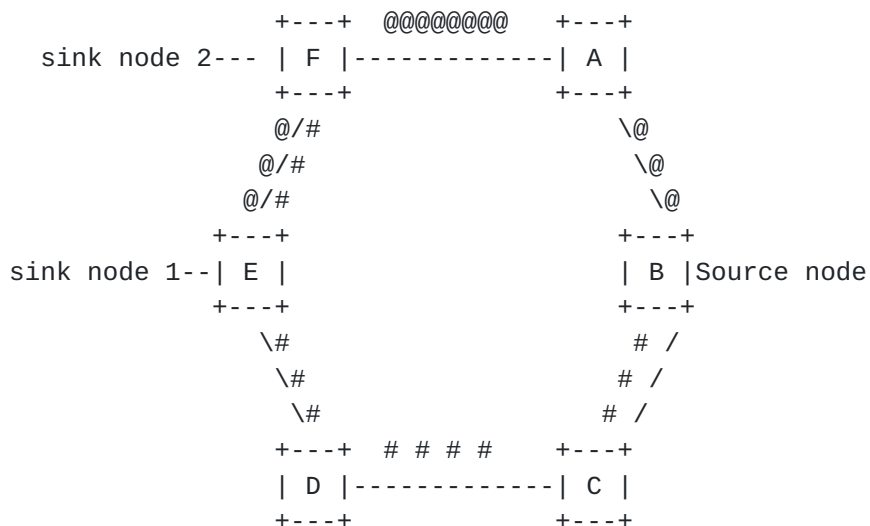
when the failure is clear, node A or F would generate failure clear notify message to other nodes of the ring . when the source node B and the sink node E of the LSP service received the failure clear notify message , they would restore to send and receive service packet from working LSP path.

[3.2.2.](#) P2MP Service Protection

For P2MP service of the ring , it must be unidirectional path and more than one egress nodes. it is difficult for source node or sink node to judge and analysis which P2MP LSP service would be affected by the failure only based by state notify message. so when a failure has been detected by section CC&CV function, the nodes which detect the failure would generate state notify message to send to other nodes of the ring. when other nodes received the state notify message,the source nodes of P2MP service firstly make their p2mp services bridge to the working path and the protecting path and send the service to its destination node along the directions of working path and protecting path. if a node in the ring is destination node for p2mp service. It will merge select a direction of path to accept

service packet. Then each sink node will detect whether the direction of receive service packet is changable. if it happens, the sink nodes will periodically generate the message of receiving state changing and send to its source node for the p2mp service. when the source node for the p2mp service receives all the messages from other sink nodes and processes them, judge whether all sink nodes of the p2mp service s in the same direreceive the service packetction include working path or protecting path. the source node of the service will select a path(working path or protecting path) to send service packet. or else it will continue to send service packet in the two path(working path and protecting path). when the failure is clear, the nodes which detect free-failure will generate a free-failure notify message and send to all other nodes in the ring. all other nodes receive the free-failure notify message and stop sending the message of receiving state changing periodically ,all service packets will come back to be transported in the working path. at the same time , each sink node for the service will select the direction of working path to receive service packet as idle state condition.

the implement in detail as the following figure. for example, there is a p2mp service from source node B to sink node F,E. and working path is B-C-D-[E]-[F] identified by signal(#) ,while protecting path is B-A-[F]-[E] identified by singal(@).under normal situation,the service pakcet will be transported by working path B-C-D-[E]-[F].

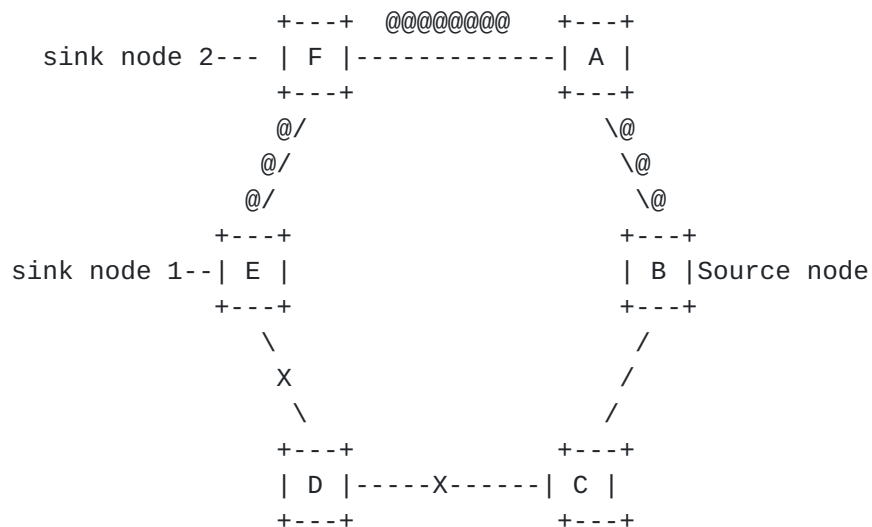


NOTE:

@: working path ;
#: protecting path;

Figure 6

when link C-D and link D-E failure happens, node C or node E that detects a failure will generate a state notify message packet to send to other nodes in the ring through control channel or other channel. when other node C,B,A,F receive the state notify message packet, they will make all source services bridge to working path and protecting path firstly. eg. the service from B to E,F , node B firstly send the service packet separately along its working path B-C-D-[E]-[F] and its protecting path B-A-[F]-[E]. As there are the failures in C-D link and D-E link, the sink node E ,F will not receive service packet by its working path B-C-D-E-F. so the two sink nodes E ,F must merge select its protection path B-A-[F]-[E] to receive the service packet.at the same time. As the sink node E, F is sink nodes of the p2mp service ,so the node E,F will generate the message of receiving state changing and send to source node B of the p2mp service periodically. so source node B will receive the message and process the message. because both sink nodes receive service packet from their protecting path. then the source node B will only select protecting path to send its service packet as the following figure:

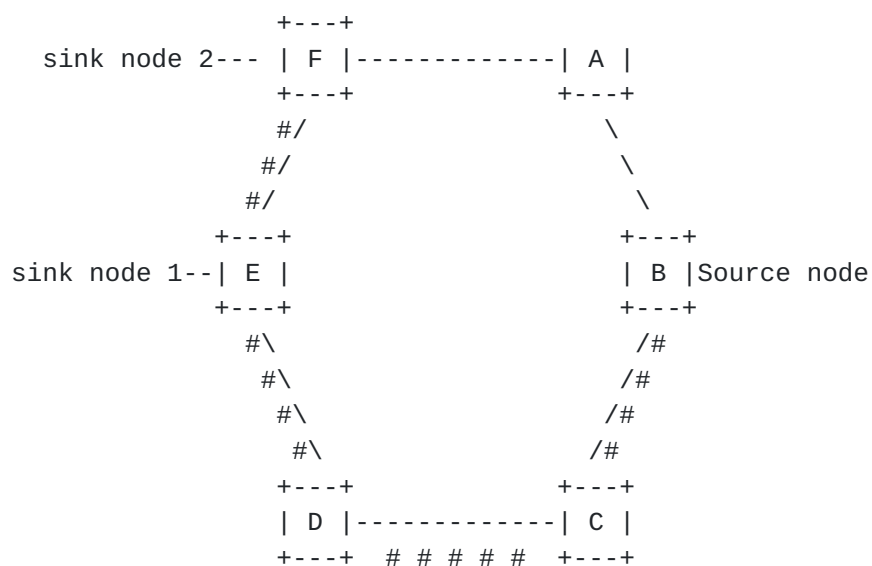


NOTE:

@: transport service by protecting path
X: failure

Figure 7

when the failure is clear , the node C,E detect the failure state have been clear up, the node C ,E will generate a free-failure notify message and send to all other nodes in the ring. when other nodes receive the free-failure notify message , each node will send and receive its own service only by its own working path .eg,the p2mp service from B to E,F will come back to working path B-C-D-[E]-[F] to send and receive its own service packet as the following. at the same time, all sink nodes of p2mp services would stop generating and sending the message of receiving state changing at once.



NOTE:

#: transport service

X: failure

Figure 8

3.3. Comparison

The two ring protection solutions can fulfil MPLS-TP requirement of ring recovery. but there are different protection and recovery mechanism and different character, the detail is the following table:

Items	solution 1	solution 2
Amounts of the backup LSP	Less	As many as the protected LSP
Bandwidth utilization ratio	lower	high
Bandwidth share	Support	Support
the number of elements of , recovery	less	more
the number of OAM	less	more
complexity	simple	complex
Lable stack	Increase one more layer	Changeless
P2P and P2MP service	Support	Support
multi-failure recovery	support	support
time of recovery	slow	fast

Table 1: comparison of ring protection

Figure 9

4. Security Considerations

The security considerations for the authentication TLV need further study.

5. IANA Considerations

TBD.

6. Acknowledgments

thank Huub van Helvoort ,Italo Busi, Yaacov Weingarten, malcolm.betts and other experts providing some good comments and advices for this draft.

7. References

7.1. Normative References

[IETF [RFC4090](#)]

IETF, "IETF [RFC4090](#)(Fast Reroute Extensions to RSVP-TE for LSP Tunnels)", May 2005.

[IETF [RFC5654](#)]

IETF, "IETF [RFC5654](#)(Requirements of an MPLS Transport Profile)", september 2009.

[IETF [RFC5921](#)]

IETF, "IETF [RFC5921](#)(A Framework for MPLS in Transport Networks)", July 2010.

[RFC 5586]

IETF, "IETF [RFC5586](#)(MPLS Generic Associated Channel)", June 2009.

7.2. Informative References

[ITU-T-G.8132 Draft]

ITU-T, "Draft ITU-T Recommendation G.8132(T-MPLS shared protection ring)", February 2008.

[MPLS TP Fault Management]

G. Swallow,A. Fulignoli,M. Vigoureux,S. Boutros,D. Ward ,
"MPLS Fault Management OAM", July 2010.

[MPLS-TP Ring protection]

Y. Weingarten, S. Bryant, N. Sprecher, D. Ceccarelli, D. Caviglia, F. Fondelli, M. Corsi, "MPLS-TP Ring Protection", August 2010.

[MPLS-TP Ring protection switching]

Igor Umansky, Huub van Helvoort, "MPLS-TP Ring Protection Switching (MRPS)", August 2010.

[MPLS-TP Survivability Framework]

N. Sprecher, A. Farrel, "Multiprotocol Label Switching Transport Profile Survivability Framework", June 2009.

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

Yang Jian
ZTE Corporation
5F,RD Building 3,ZTE Industrial Park,XiLi LiuXian Road
Nanshan District,Shenzhen 518055
P.R.China

Phone: +86 755 26773731
Email: yang_jian@zte.com.cn

Jiang lili
ZTE Corporation
No.68, Zijinghua Road, Yuhuatai District
Nanjing 210012
P.R.China

Phone: +86 025 52871745
Email: jiang.lili@zte.com.cn

Fu zhentao
ZTE Corporation
No.68, Zijinghua Road, Yuhuatai District
Nanjing 210012
P.R.China

Phone: +86 025 52877162
Email: fu.zhentao@zte.com.cn

