Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 09, 2014

WQ. Cheng
L. Wang
H. Li
China Mobile
K. Liu
J. He
Huawei Technologies Co., Ltd.
F. Li
China Academy of Telecommunication Research, MIIT., China
J. Yang
ZTE Corporation P.R.China
JF. Wang
Fiberhome Telecommunication Technologies Co., LTD.

July 08, 2013

MPLS-TP Shared-Ring protection (MSRP) mechanism for ring topology draft-cheng-mpls-tp-shared-ring-protection-01

Abstract

This document describes requirements and solutions for MPLS-TP Shared Ring Protection (MSRP) in the ring topology for point-to-point (P2P) services. The mechanism of MSRP is illustrated and analyzed how it satisfies the requirements in RFC5654 for optimized ring protection.

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 09, 2014.

Table of Contents

As described in 2.5.6.1. ring protection of MPLS-TP requirements [RFC5654], several service providers have expressed much interest in operating MPLS-TP in ring topologies and required a high-level survivability function in these topologies. In operation network deployment, MPLS-TP networks are often constructed with ring topologies. It calls for an efficient and optimized ring protection mechanism to achieve simplified operation and fast recovery performance.

The requirements for MPLS-TP [RFC5654] state that recovery mechanisms which are optimized for ring topologies could be further developed if it can provide the following features:

a. Minimize the number of OAM entities for protection

b. Minimize the number of elements of recovery

c. Minimize the required label number

d. Minimize the amount of control and management-plane transactions

e. Minimize the impact on information exchange if the control plane supports

This document specifies MPLS-TP Shared-Ring Protection mechanisms which can meet all those requirements on ring protection listed in [RFC5654].

This document focus on the solutions for point-to-point transport path. The solution for point-to-multipoint transport is under study and will be presented in a separate document. The basic concept stated in this document also apply to point-multipoint transport path.

1.1. Requirements for MPLS-TP ring protection

The requirements for MPLS-TP ring protection are specified in RFC5654. This document elaborates the requirements in detail.

1.1.1. Recovery for Multiple failures

MPLS-TP is expected to be used in carrier grade metro networks and backbone networks to provide mobile backhaul, carry business customers' services and etc., in which the network survivability is very important. According to R106 B in RFC5654, MPLS-TP recovery mechanisms in a ring SHOULD protect against multiple failures. The following context provides some more detailed illustration about "multiple failures". In metro and backbone networks, the single risk

factor often affects multiple links or nodes. Some examples of risk factors are given as follows:

- multiple links using fibers in one cable or pipeline

- Several nodes shared one power supply system

- weather sensitive micro-wave system

Once one of the above risk factors happens, multiple links or nodes failures may occur simultaneously and those failed links or nodes may locate on a single ring as well as on interconnected rings. Ring protection against multiple failures should cover both multiple failures on a single ring and multiple failures on interconnected rings.

1.1.2. Smooth Upgrade from linear protection to ring protection

It is beneficial for service providers to upgrade protection scheme from linear protection to ring protection in their MPLS-TP network without service interruption. In-service insertion and removal of a node on the ring should also be supported. Therefore, the MPLS-TP ring protection mechanism is supposed be developed and optimized to comply with this smooth upgrading principle.

1.1.3. Configuration complexity

While deploying linear protection in MPLS-TP networks, the configuration effort of protection depends on the quantity of the

services carried. In some large metro networks with more than ten thousand services access, the LSP linear protection capabilities of the metro core nodes should be large enough to meet the network planning requirements, which also leads to the complexity of network protection configuration and operation. While ring protection can reduce the dependency of configuration on the quantity of services, it will simplify the network protection configuration and operation effort.In the application scenarios of deploying linear protection in MPLS-TP network, the configuration of protection has close relationship with the services, LSP quantities. Especially in some large metro networks with more than ten thousands of services access node, the LSP linear protection capabilities of the metro core nodes should be large enough to meet the network planning requirements, which also leads to the complexity of network protection configurations and operations. While the ring protection is based on the mechanisms on section layer, it has loose relationship with the services quantities which could simplify the network protection configurations and operations effort.

1.2. Terminology and Notation

The following syntax will be used to describe the contents of the label stack:

1. The label stack will be enclosed in square brackets ("[]").

2. Each level in the stack will be separated by the '|' character.

It should be noted that the label stack may contain additional layers. However, we only present the layers that are related to the protection mechanism.

3. If the Label is assigned by Node x, the Node Name will enclosed in bracket(" ()")

1.3. Contributing Authors

Wen Ye(China Mobile)

2. Shared-ring protection for P2P

2.1. Basic concept

This document introduces a novel logic layer of the ring for both working path and protection path for shared ring protection in MPLS-TP networks. As shown in Figure 1, the new logic layer is a ring tunnel on top of the working path or the protection path, namely working ring tunnel and protection ring tunnel respectively. Once a ring tunnel is established, the configuration, management and protection of the ring are all based on the ring tunnel. One port can carry multiple ring tunnels, while one ring tunnel can carry multiple LSPs.

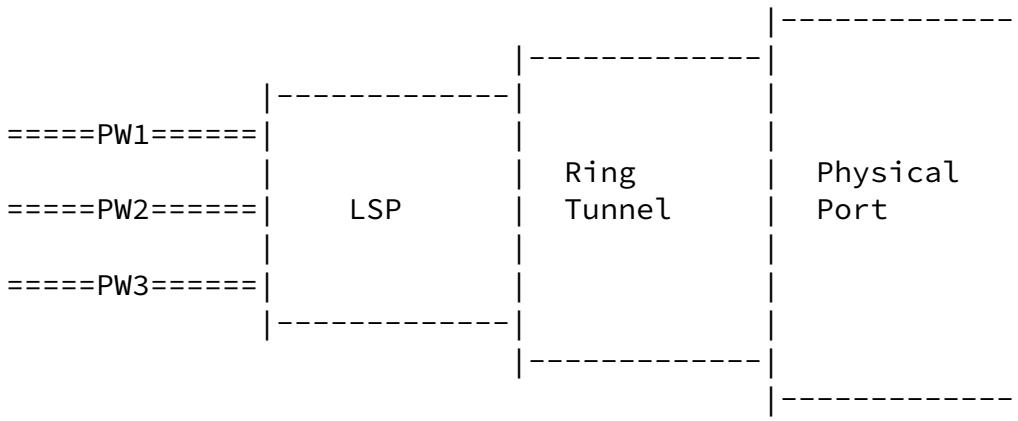


Figure 1 the logic layers of the ring

The label stack used in MPLS-TP Shared Ring Protection mechanism is shown as below.

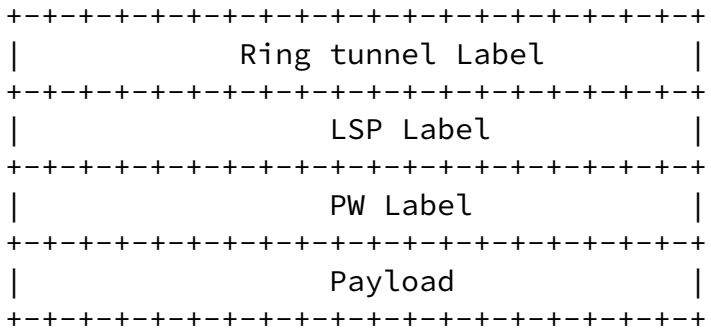


Figure 2 Label stack used in MPLS-TP Shared Ring Protection

2.1.1. The establishment of the Ring tunnels

LSPs which have same exit node share the same ring tunnel. The exit node is the node where the traffic leaves the ring. In other words, all the LSPs that traverse the ring and exit from the same node share the same working ring tunnel and protection ring tunnel. For each exit node, four ring tunnels are established:

- one clockwise working ring tunnel, which is protected by the following protection tunnel,

- one anticlockwise protection ring tunnel,

- one anticlockwise working ring tunnel, which is protected by the following protection tunnel,

- one clockwise protection ring tunnel.

An example is shown in Figure 3 where Node D is the exit node. LSP 1, LSP 2 and LSP 3 enter the ring from Node E, Node A and Node B, respectively, and all leave the ring from Node D. To protect these LSPs that traverse the ring, a clockwise working ring tunnel (RcW_D) via E->F->A->B->C->D, and its protection ring tunnel in the reverse direction (RaP_D) via D->C->B->A->F->E->D are established, respectively; Also, an anti-clockwise working ring tunnel (RaW_D) via C->B->A->F->E->D, and its clockwise protection ring tunnel (RcP_D) via D->E->F->A->B->C->D are established, respectively. Figure 3 only shows RcW_D and RaP_D. A similar provisioning should be applied for any other node on the ring. For other nodes in Figure 3 when acting as an exit node, the ring tunnels are created as follows:

To Node A: RcW_A, RaW_A, RcP_A, RaP_A;

To Node B: RcW_B, RaW_B, RcP_B, RaP_B;

To Node C: RcW_C, RaW_C, RcP_C, RaP_C;

To Node E: RcW_E, RaW_E, RcP_E, RaP_E;

To Node F: RcW_F, RaW_F, RcP_F, RaP_F;

For exit Node D, two working ring tunnels, RcW_D and RaW_D, are terminated on Node D, and two protection ring tunnels, RcP_D and RaP_D, are started from Node D. That means through these working ring tunnels with protection ring tunnels, LSPs which enter the ring from Node D can reach any other nodes on the ring, while Node D can also receive the traffic from any other nodes.

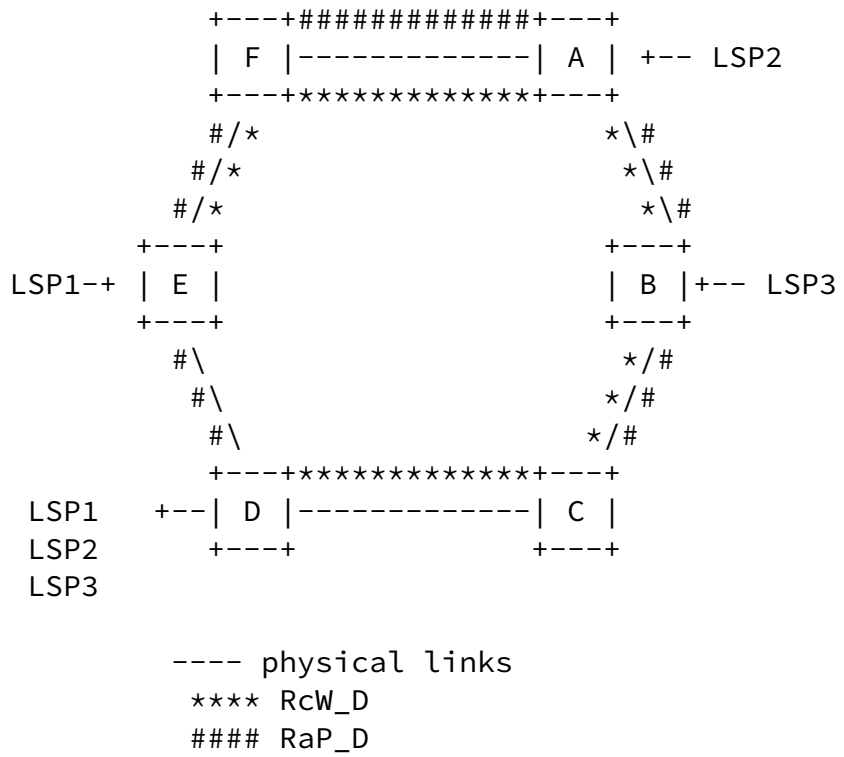


Figure 3 Ring tunnels in MSRP

2.1.2. The distribution and management of ring labels

Ring tunnel labels are distributed by means of downstream-assigned mechanism as defined in [RFC3031]. When a MPLS-TP transport path, such as LSP, enters the ring, the ingress node pushes the working ring tunnel label and sends the traffic to the next hop according to the ring ID and the exit node. The transit nodes within the working ring tunnel swap ring tunnel labels and forward the packets to the next hop; When arriving at the egress node, the egress node removes

the ring tunnel label and forwards the packets based on the inner LSP

label and PW label. Figure 4 shows the label operation in the MPLS-TP shared ring protection mechanism. Assume that LSP 1 enters the ring at Node A and exits from Node D, and the following label operations are executed.

1. The traffic LSP1 arrives at Node A with a label stack [LSP1] and is supposed to be forwarded in the clockwise direction of the ring. The clockwise working ring tunnel label RcW_D will be pushed at Node A, the label stack for the forwarded packet at Node A is changed to [RcW_D(B)|LSP1]

2. Transit nodes, in this case, Node B and Node C forward the packets by swapping the working ring tunnel labels. For example, the label [RcW_D(B)|LSP1] is swapped to [RcW_D(C)|LSP1] at Node B.

3. When the packet arrives at Node D (i.e. egress node) with label stack [RcW_D(D)|LSP1], Node D removes RcW_D(D), and subsequently deals with the inner labels of LSP1.

4. All the LSPs which exit from the same node share the same set of ring tunnel labels.

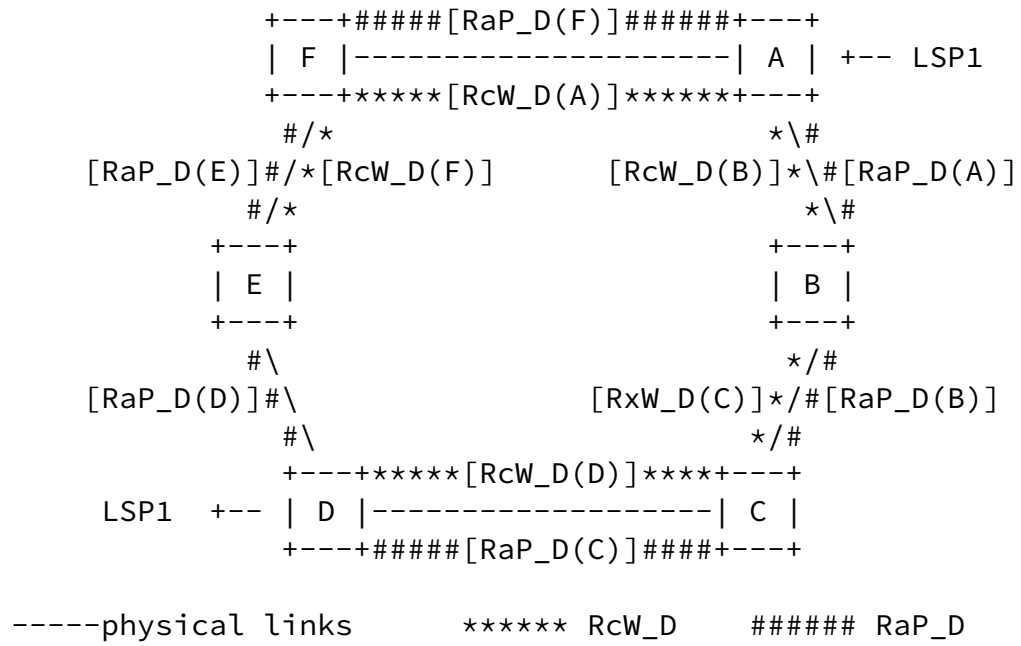


Figure 4 Label operation of MSRP

2.1.3. Failure detection

The MPLS-TP section layer OAM is used to monitor the connectivity between each two adjacent nodes on the ring using the mechanisms

defined in [RFC6371]. Protection switching is triggered by the failure detection in a link in the ring monitored by OAM functions.

Two end ports of a link form an MEG, and an MEG end point (MEP) function is installed in each ring port. CC-V OAM packets are periodically exchanged between each pair of MEPs to monitor the link health. Consecutive losses of CC-V packets (3 packets) will be interpreted as a link failure.

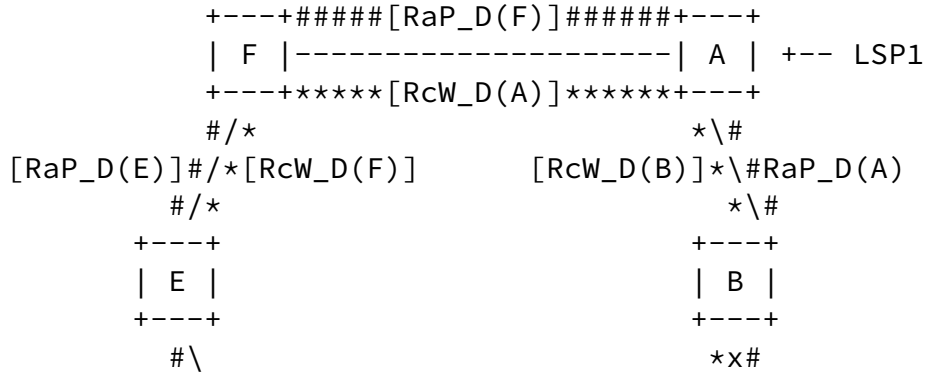
A node failure is regarded as the failure of two links attached to the node. The two nodes adjacent to the failed node detect the failure in the links that are connected to the failed node.

2.2. P2P wrapping

Normal state is shown in Figure 4. The clockwise LSP1 towards node D enters the ring at Node A. In normal state, LSP 1 follows the path A->B->C-D, label operation is [LSP1](original data traffic carried by LSP 1)->[RCW_D(B)|LSP1](NodeA)->[RCW_D(C)|LSP1](NodeB)->[RCW_D(D)|LSP1](NodeC)->[LSP1](data traffic carried by LSP 1). Then traffic packet will be forwarded based on LSP1 at nodeD.

2.2.1. Wrapping for Link Failure

When a link failure between Node B and Node C occurs, both Node B and Node C detect the failure by OAM mechanism. Node B switches the clockwise working ring tunnel (RcW_D) to the anticlockwise protection ring tunnel (RaP_D) and Node C switches anticlockwise protection ring tunnel(RaP_D) to the clockwisework ring tunnel(RcW_D). The data traffic which enters the ring at Node A and exits at Node D follows the path A->B->A->F->E->D->C->D. The label operation is [LSP1](Original data traffic)-> [RcW_D(B)|LSP1](Node A)-> [RaP_D(A)|LSP1](Node B)->[RaP_D(F)|LSP1](Node A)->[RaP_D(E)|LSP1] (Node F)->[RaP_D(D)|LSP1] (Node E)-> [RaP_D(C)|LSP1] (Node D)-> [RcW_D(D)|LSP1](Node C)->[LSP1](Data traffic exits the ring).



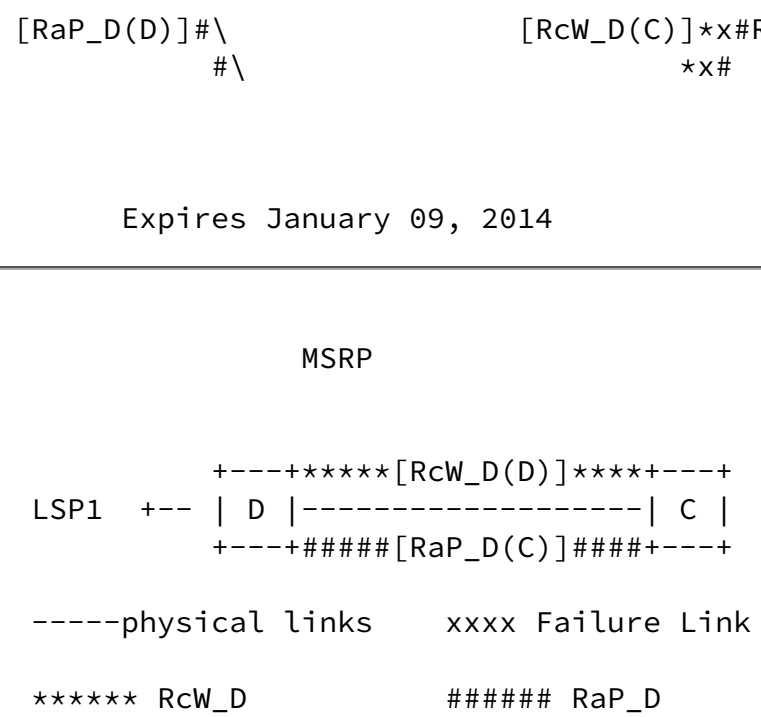


Figure 5 P2P wrapping for link failure in a single ring

2.2.2. Wrapping for node Failure

When Node B fails, Node A detects the failure between A and B and switches the clockwise work ring tunnel(RcW_D) to the anticlockwise protection ring tunnel(RaP_D), Node C detects the failure between C and B and switches the anticlockwise protection ring tunnel(RaP_D) to the clockwise working ring tunnel(RcW_D). The data traffic which enters the ring at Node A and exits at Node D follows the path A->F->E->D->C->D. The label operation is [LSP1](original data traffic carried by LSP 1)-> [RaP_D(F)|LSP1](NodeA)->[RaP_D(E)|LSP1](NodeF)-> [RaP_D(D)|LSP1](NodeE)-> [RaP_D(C)|LSP1] (NodeD)->[RcW_D(D)|LSP1] (NodeC)->[LSP1](data traffic carried by LSP 1).

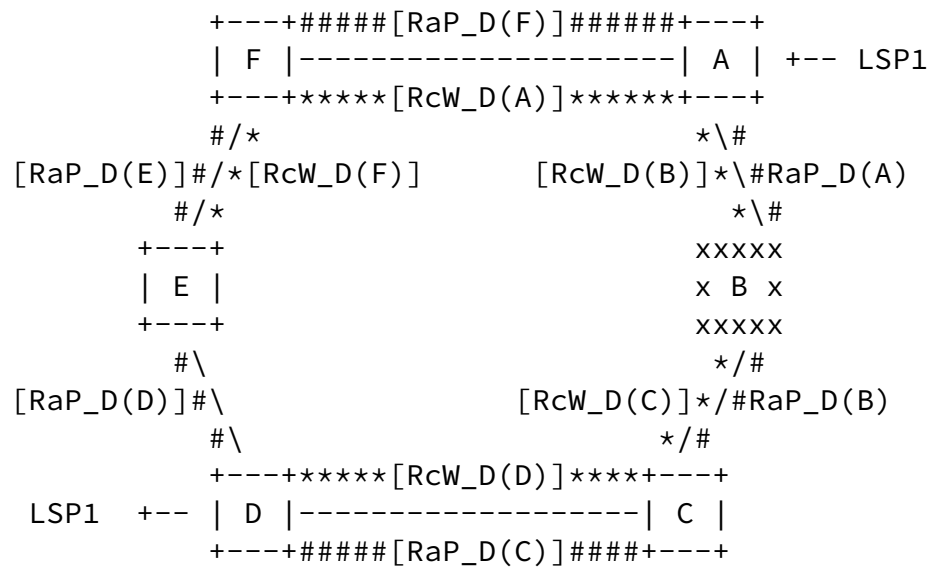


Figure 6 P2P wrapping for node failure in a single ring

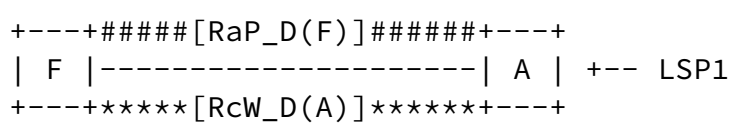
2.3. P2P short wrapping

For traditional wrapping protection scheme, Protection switching execute at both nodes neighbored failure respectively , so the traffic will be wrapped twice. This mechanism will cause more latency and bandwidth consume when traffic switched to protection path.

For Short wrapping protection, switching only execute at up-stream node neighbored failure node, and exited ring in protection ring tunnel. This scheme can optimized latency and bandwidth consume when traffic switched to protection path.

In traditional wrapping solution, protection ring tunnel is a closed path in normal state, while in short wrapping solution, protection ring tunnel will remove at exit node. Short wrapping is easy to implement in shared ring protection because the working and protection ring tunnel is established base on exit nodes.

As show in figure 7, the data traffic which enters the ring at Node A and exits at Node D follows the path A->B->C->D in normal state. When a link failure between Node B and Node C occurs, NodeB switched work ring tunnel RcW_D to opposite protection ring tunnel RaP_D same as traditionally wrapping. The different occurs in protection ring tunnel at exit node. In short wrapping protection, Rap_D will remove in Node D and deal with inner LSP label. So LSP1 will follows the path A->B->A->F->E->D when link failure between Node B and Node C when using short wrapping.



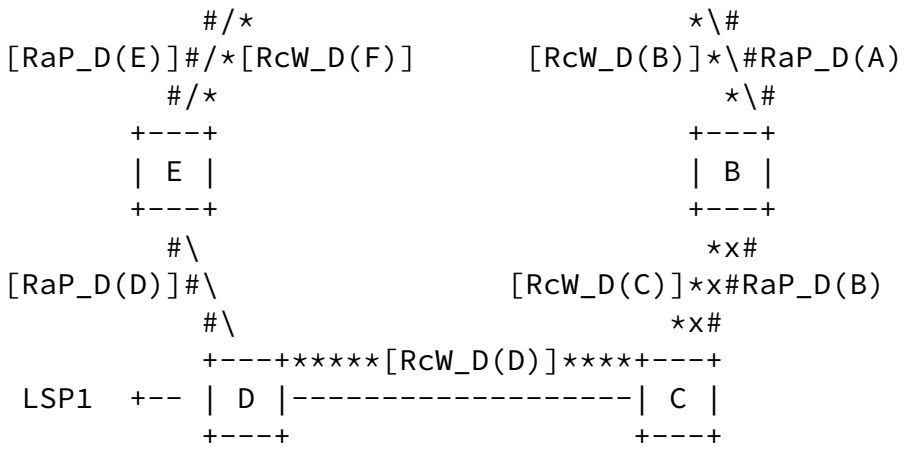
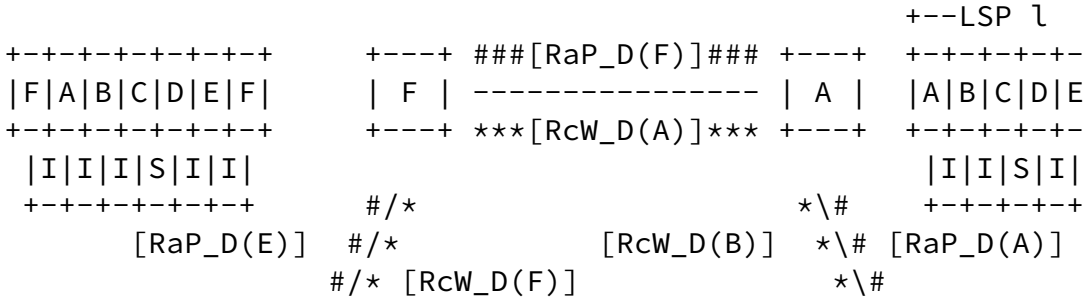


Figure 7 P2P short wrapping for link failure

2.4. P2P steering

Each working ring tunnel is associated with a protection ring tunnel in the opposite direction. Every node needs to know the ring topology by configuration or topology discovery. When the failure occurs in the ring, the nodes which detect the failure will spread the failure information in the opposite direction node by node in the ring respectively. When the node receives the message that informs the failure, it will quickly figure out the location of the fault by the topology information that is maintained by itself, so that it will determine whether the LSPs enter the ring from itself needs switch-over. If yes, it will switch the LSPs from the working ring tunnel to its protection ring tunnel.



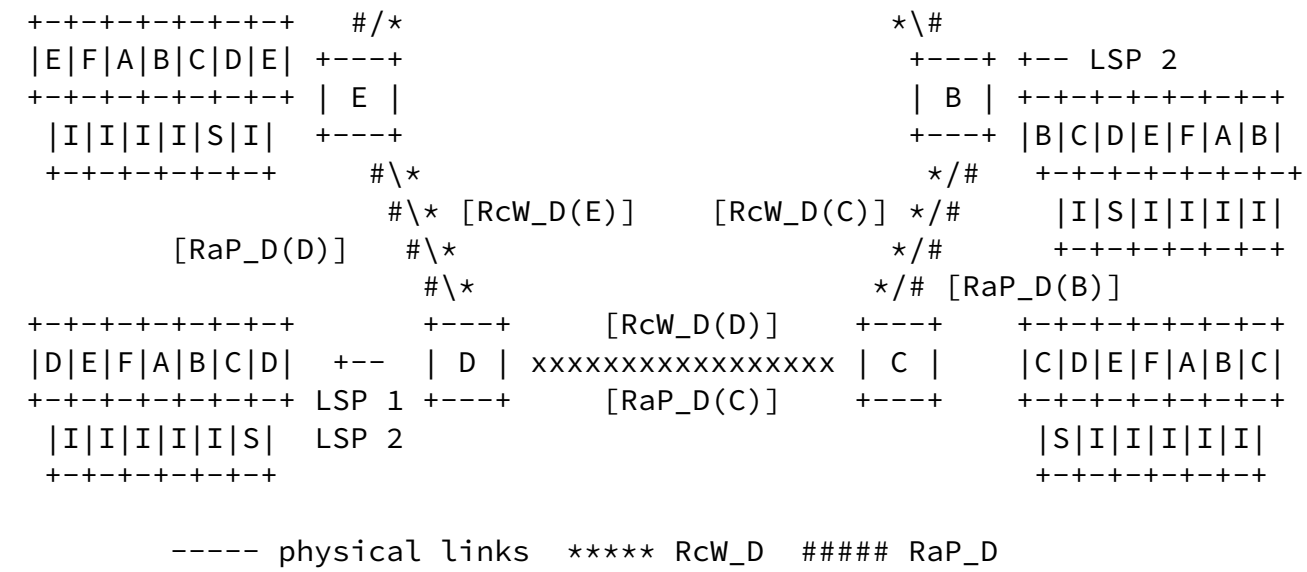


Figure 8 P2P steering operation and protection switching (1)

Steering Example is shown in Figure 8. LSP1 enters the ring from Node A while LSP2 enters the ring from Node B, and both of them have the same destination node D. As Figure 8 shows, in the normal state, LSP1 follows the path A->B->C->D, the label operation is

[LSP1](original data traffic carried by LSP 1)->[RcW_D(B)|LSP1](NodeA)->[RcW_D(C)| LSP1](NodeB)->[RcW_D(D)|LSP1](NodeC)->[LSP1] (data traffic carried by LSP 1) . LSP2 goes through the path B->C->D, the label operation is [LSP2]->[RcW_D(C)|LSP2](NodeB)->[RcW_D(D)|LSP2](NodeC)-> [LSP2] (data traffic carried by LSP 1) .

If the link between C and D breaks down, as Figure 8 shows, according to the fault detection function of each link, Node D will find out that there is a failure in the link between C and D, and it will update the link state of its ring topology, changing the link state between C and D from normal to fault, as Figure 8 shows. In the direction that goes away from the failure point, Node D will send the state report message to Node E, informing Node E of the fault between C and D, and E will update the link state of its ring topology, changing the link state between C and D from normal to fault. In this manner, the state report message is sent node by node in the clockwise direction. Similar to Node D, Node C will spread the

failure information in the anti-clockwise direction.

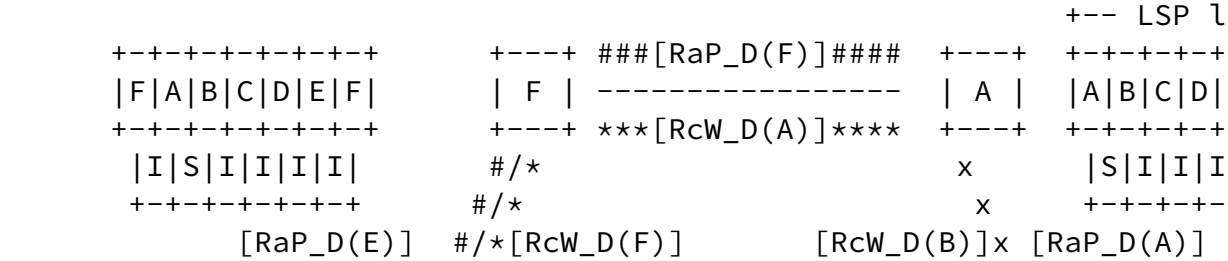
Until Node A updates the link state of its ring topology and be aware of there is a fault within its working path, it can reach the conclusion that the anticlockwise path from A to D is working all right, and thus Node A will switch the LSP1 operation to the anticlockwise ring tunnel.

LSP1 will follow the path A->F->E->D, the label operation is [LSP1](original data traffic carried by LSP 1)->[RaP_D(F)|LSP1](NodeA)->[RaP_D(E)|LSP1](NodeF)->[RaP_D(D)|LSP1](NodeE)->[LSP1](data traffic carried by LSP 1).

The same also apply to the operation of LSP2. When Node B updates the link state of its ring topology, and finds out the working path fault, it will stop sending the LSP2 operation in the clockwise direction and switch the LSP2 to the anticlockwise protection tunnel. LSP2 goes through the path B->A->F->E->D, and the label operation is [LSP2](original data traffic carried by LSP 2)-> [RaP_D(A)|LSP2](NodeB)->[RaP_D(F)|LSP2](NodeA)->[RaP_D(E)|LSP2](NodeF)->[RaP_D(D)|LSP2](NodeE)->[LSP2](data traffic carried by LSP 2).

Assume that the ring between A and B breaks down, as Figure 9 shows. Like above, Node B will find out that there is a fault in the link between A and B, and it will update the link state of its ring topology, changing the link state between A and B from normal to fault. The state report message is sent node by node in the clockwise direction, informing every node that there is a fault between node A and B, so that every node updates the link state of its ring topology. Node A will find out a fault in the working path

of LSP1, and switch LSP1 to the protection Ring tunnel, while Node B will find out the LSP2 working path is all right and there is no need for switching.



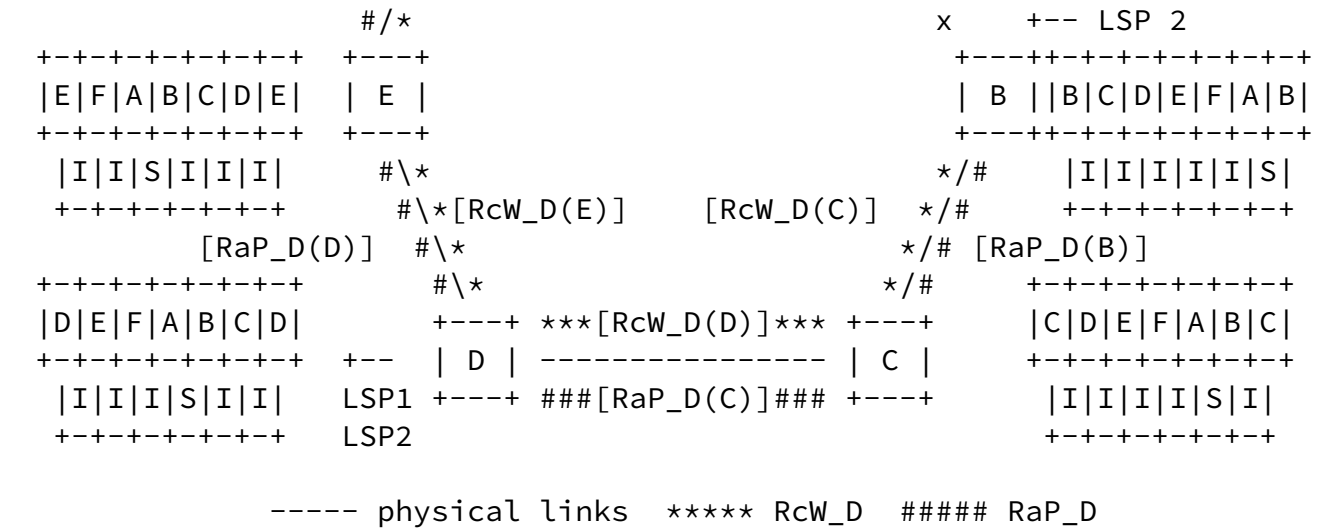


Figure 9 the P2P steering operation and protection switching (2)

2.5. P2P wrapping for Interconnected Rings

2.5.1. Interconnected ring topology

Interconnected ring topology is often used in MPLS-TP networks. There are two typical interconnected ring topologies that will be addressed in this document.

1) Single-node interconnected rings

In single-node interconnected rings, the connection between two rings is through a single node. As the interconnection node may cause a single point of failure, this topology should be avoided in real networks;

2) Dual-node interconnected rings

In dual-node interconnected rings, the connection between two rings is through two nodes. The two interconnection nodes belong to both

interconnected rings. This topology can recover from one interconnection node failure.

2.5.1.1. Single-node interconnected rings

Figure 10 shows the topology of single-node interconnected rings. Node C is interconnection node between Ring1 and Ring2.

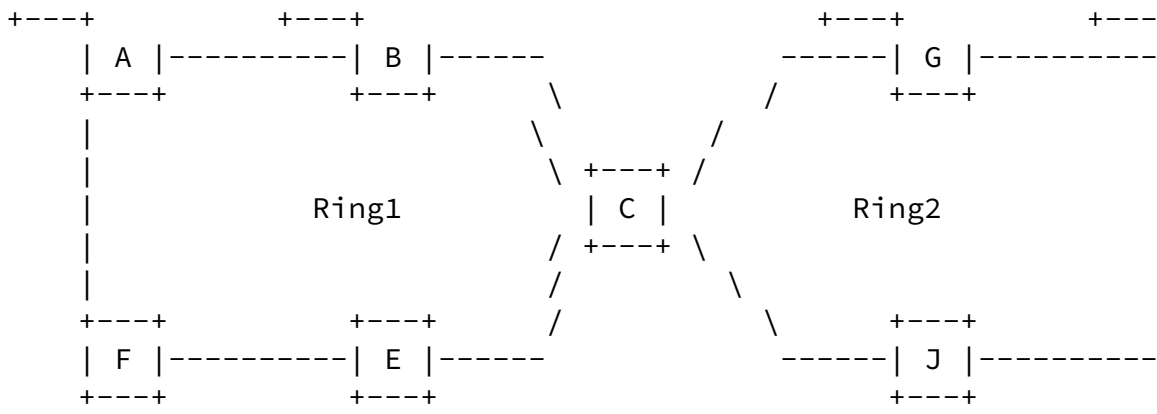


Figure 10 Single-node interconnected rings

2.5.1.2. Dual-node interconnected rings

Figure 11 shows the topology of dual-node interconnected rings. Node C and Node D are interconnection nodes between Ring1 and Ring2.

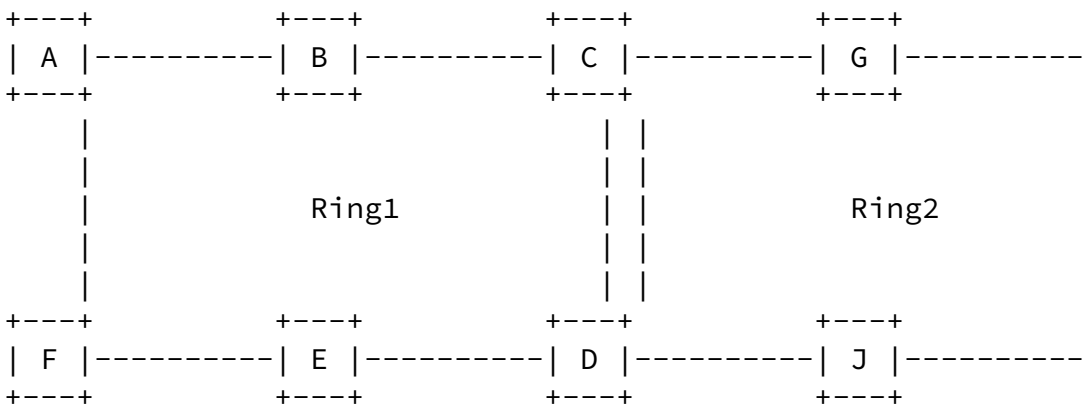


Figure 11 Dual-node interconnected rings

2.5.2. Interconnected ring protection scheme

2.5.2.1. Introduction

- Interconnected rings can be regarded as two independent rings. Each ring runs protection switching independently. Failure in one ring only triggers protection switching in itself and does not affect the other ring. Protection switch in a single ring is same as which described in section 3 Shared ring protection for P2P.

- The service LSPs that traverse the interconnected rings via the interconnection nodes must use different ring tunnels in different rings. The ring tunnel used in the source ring will be removed, and the ring tunnel of destination ring will be added in interconnection nodes.

- For protected interconnection node in dual-node interconnected ring, the service LSPs in the interconnection nodes should use the same MPLS label. So any interconnection node can terminate source ring runnel and push destination ring tunnel according to service LSP label.

- Two interconnection nodes can be managed as a virtual interconnection node group. Each ring should assign ring tunnels to the virtual interconnection node group. The interconnection nodes in the group should terminate the working ring tunnel in each ring. Protection ring tunnel is a open ring to switch with the working ring tunnel at the nodes which detect the fault and end at the egress node.

- When the service traffic passes through the interconnection node, the direction of the working ring tunnels in each ring for this service traffic should be the same. For example, if the working ring tunnel follows the clockwise direction in Ring1, the working ring tunnel for the same service traffic in Ring2 also follows the clockwise direction when the service leaves Ring1 and enters Ring2.

2.5.2.2. Ring tunnels of interconnected rings

The same ring tunnels as described in 2.1.1 are used in each ring of the interconnected rings. Besides, ring tunnels to the virtual interconnection node group will be established by each ring of the interconnected rings, i.e.:

- one clockwise working ring tunnel to the virtual interconnection node group;

- one anticlockwise protection ring tunnel to the virtual interconnection node group,

- one anticlockwise working ring tunnel to the virtual interconnection node group;

- one clockwise protection ring tunnel to the virtual interconnection node group.

These ring tunnel will terminated at all nodes in virtual interconnection node group.

All the ring tunnels established in Ring1 in Figure 11 is provided as follows:

To Node A: R1cW_A, R1aW_A, R1cP_A, R1aP_A;

To Node B: R1cW_B, R1aW_B, R1cP_B, R1aP_B;

To Node C: R1cW_C, R1aW_C, R1cP_C, R1aP_C;

To Node D: R1cW_D, R1aW_D, R1cP_D, R1aP_D;

To Node E: R1cW_E, R1aW_E, R1cP_E, R1aP_E;

To Node F: R1cW_F, R1aW_F, R1cP_F, R1aP_F;

To the virtual interconnection node group (including Node F and Node A): R1cW_F&A, R1aW_F&A, R1cP_F&A, R1aP_F&A;

All the ring tunnels established in Ring2 in Figure 11 is provided as follows:

To Node A: R2cW_A, R2aW_A, R2cP_A, R2aP_A;

To Node F: R2cW_F, R2aW_F, R2cP_F, R2aP_F;

To Node G: R2cW_G, R2aW_G, R2cP_G, R2aP_G;

To Node H: R2cW_H, R2aW_H, R2cP_H, R2aP_H;

To Node I: R2cW_I, R2aW_I, R2cP_I, R2aP_I;

To Node J: R2cW_J, R2aW_J, R2cP_J, R2aP_J;

To the virtual interconnection node group(including Node F and Node A): R2cW_FandA, R2aW_FandA, R2cP_FandA, R2aP_FandA;

2.5.2.3. Interconnected ring switch mechanism

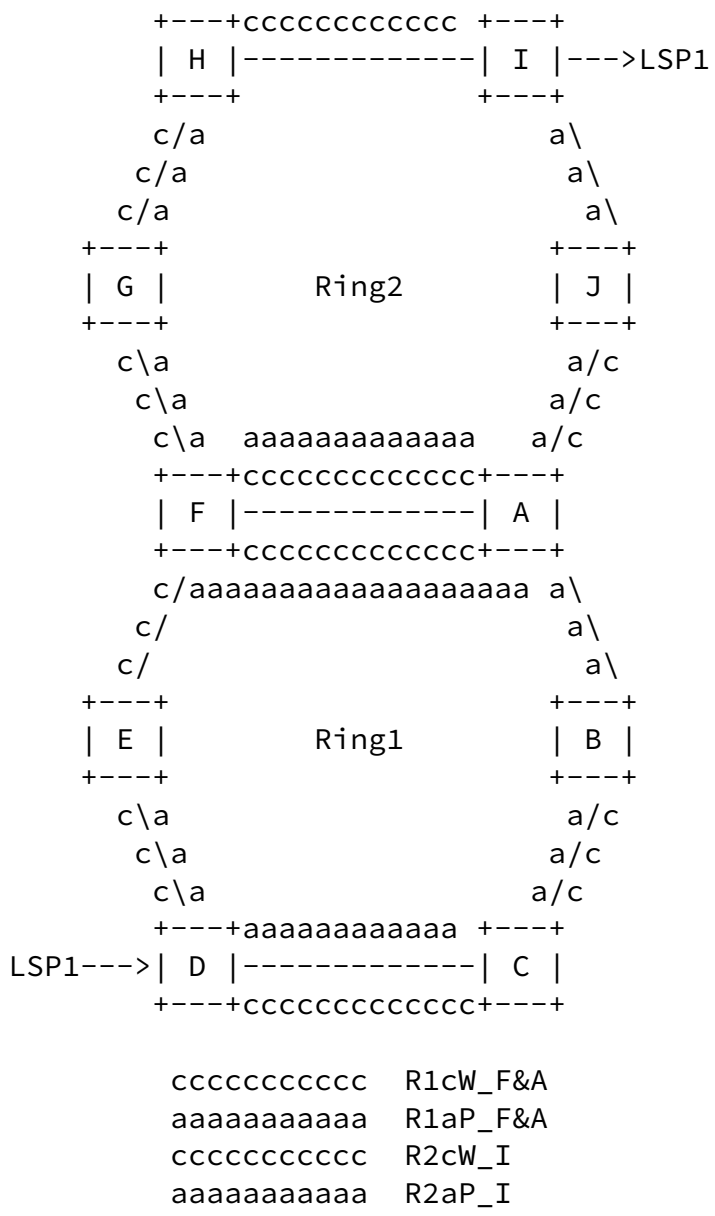


Figure 12 Ring tunnels for the interconnected rings

As shown in Figure 12, for the service traffic LSP1 which enters Ring1 at Node D and leaves Ring1 at Node F and continues to enter Ring2 at Node F and leaves Ring2 at Node I, the protection scheme is described below.

In normal state, LSP1 follows R1cW_F&A in Ring1 and R2CW_I in Ring2. The label used for the working ring tunnel R1cW_F&A in Ring1 is popped and the label used for the working ring tunnel R2cW_I will be pushed based the inner label lookup at the interconnection node F. The working path that the service traffic LSP1 follows is: LSP1->R1cW_F&A (D->E->F)->R2cW_I(F->G->H->I)->LSP1.

In case of link failure, for example, when a failure occurs on the link between Node F and Node E, Node F and E will detect the failure and execute protection switching as described in 2.2.1.1. The path that the service traffic LSP1 follows after switching change to LSP1->R1cW_F&A(D->E)->R1aP_F&A(E->D->C->B->A->F)->R1cW_F(F) ->R2cW_I(F->G->H->I)->LSP1.

In case of non interconnection node failure, for example, when the failure occurs at Node E in Ring1, Node F and E will detect failure and execute protection switching as described in 2.2.1.2. The path that the service traffic LSP1 follows after switching becomes: LSP1->R1cW_F&A(D)->R1aP_F&A(D->C->B->A->F)-> R1cW_F(F)->R2cW_I(F->G->H->I).

In case of interconnection node failure, for example, when failure occurs at the interconnection Node F. Node E and A in Ring1 will detect the failure, and execute protection switching as described in 2.2.1.2. Node G and A in Ring2 will also detects the failure, and execute protection switching. The path that the service traffic LSP1 follows after switching is: LSP1->R1cW_F&A(D->E)->R1aP_F&A(E->D->C->B->A)->R1cW_A(A) ->R2aP_I(A->J->I)->LSP1.

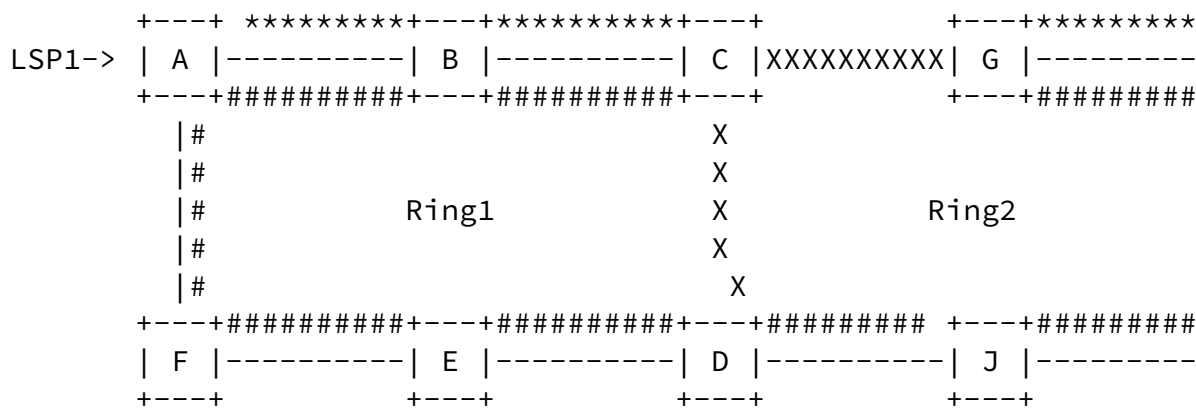
2.5.2.4. Interconnected ring topology detection mechanism

As show in Figure 13, the service traffic LSP1 traverses A->B-C in

Ring1 and C->G->H->I in Ring2. Node C and Node D is the interconnection node. When both the link between Node C and Node G and the link between Node C and Node D fail, ring tunnel from Node C to Node I in Ring 2 becomes unreachable. However, Node D is still available, by which LSP1 can still reach Node I.

In order to do so, the interconnection nodes need to know the ring topology in each ring independently so that they can judge whether a node is reachable. The judgment is based on the knowledge of ring topology and the fault location as described in section 3.4. The ring topology can be obtained by NMS or topology discovery mechanisms. The fault location can be obtained by spreading the fault information around the ring. The nodes which detect the failure will spread the fault information in the opposite direction node by node in the ring respectively. When the interconnection node receives the message that informs the failure, it will quickly figure out the location of the fault by the topology information that is maintained by itself and determine whether the LSPs enter the ring from itself can reach the destination. If the destination node is reachable, the LSP will exit the source ring and enter the destination ring. If the destination node is not reachable, the LSP will switch to the anticlockwise protection ring tunnel.

In Figure 13 Node C judges the ring tunnel to Node I is unreachable, the service traffic LSP1 of which the destination node on the ring tunnel is Node I should switch to the protection LSP (R1aP_C&D) so that the service traffic LSP1 traverses the interconnected rings at Node D. Node D will remove the ring tunnel label of Ring1 and add ring tunnel label of Ring2.



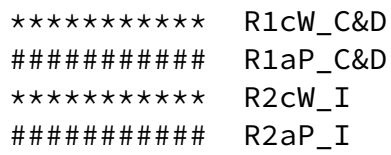


Figure 13 interconnected ring

3. Coordination protocol

TBD

4. Conclusions

TBD

5. IANA Considerations

None

6. Security Considerations

TBD

7. References

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

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

[RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[RFC6371] Busi, I. and D. Allan, "Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks", RFC 6371, September 2011.

Authors' Addresses

Weiqiang Cheng
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: chengweiqiang@chinamobile.com

Lei Wang
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: Wangleiyj@chinamobile.com

Han Li
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: Lihan@chinamobile.com

Kai Liu
Huawei Technologies Co., Ltd.
Huawei base, Bantian, Longgang District
Shenzhen 518129
China

Email: alex.liukai@huawei.com

Jia He
Huawei Technologies Co., Ltd.
Huawei base, Bantian, Longgang District
Shenzhen 518129
China

Email: hejia@huawei.com

Fang Li
China Academy of Telecommunication Research, MIIT., China
No.52 Huayuan Street
Beijing 100191
China

Email: lifang@ritt.cn

Jian Yang
ZTE Corporation P.R.China
ZTE Industrial Zone, Liuxian Road
Shenzhen 518055
China

Email: yang.jian90@zte.com.cn

Junfang Wang
Fiberhome Telecommunication Technologies Co., LTD.
No.5, Dongxin Lu
Wuhan 430073
China

Email: wjf@fiberhome.com.cn