INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

TD 35 (PLEN/15)

STUDY GROUP 15

Original: English

Question(s):	9/15	Geneva, 19-30 June 2017

TD

Source:	Editors of G.8132/Y.1383
Title:	Draft Recommendation ITU-T G.8132/Y.1383 (for Consent, 30 June 2017)
Purpose:	Discussion

Contact:	Jeong-dong Ryoo ETRI Rep. of Korea	Tel: +82-42-862-2480 Email: ryoo@etri.re.kr
Contact:	Lei Wang China Mobile Communications Corporation R. P. China	Tel: +86-15801696688-37077 Email: wangleiyj@chinamobile.com

This document provides Draft Recommendation G.8132/Y.1383, MPLS-TP Shared Ring Protection.

This document is the output of the Q9 interim meeting held in Tokyo in April 2017.

Recommendation ITU-T G.8132/Y.1383

MPLS-TP Shared Ring Protection

Summary

This recommendation provides architecture and mechanisms for shared ring protection for MPLS transport profile (MPLS-TP) networks. It describes the MPLS-TP Shared Ring Protection (MSRP) mechanisms and the Ring Protection Switch (RPS) protocol.

The mechanisms defined herein protect point-to-point MPLS-TP label switched aths (LSPs) against failures at the MPLS-TP section layer.

Keywords

MPLS-TP shared ring protection

Introduction

<Optional – This clause should appear only if it contains information different from that in Scope and Summary>

1 Scope

This recommendation provides architecture and mechanisms for shared ring protection for MPLS transport profile (MPLS-TP) networks.

It describes the MPLS-TP Shared Ring Protection (MSRP) mechanisms and the Ring Protection Switch (RPS) protocol defined in [IETF RFC XXXX].

The mechanisms defined herein protect point-to-point MPLS-TP label switched paths (LSPs) against failures at the MPLS-TP section layer.

This Recommendation provides a representation of the MPLS-TP technology using the methodologies that have been used for other transport technologies (e.g., synchronous digital hierarchy (SDH), optical transport network (OTN) and Ethernet).[1]

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G. 800] Recommendation ITU-T G.800 (2012), *Unified functional architecture of transport networks*.

[ITU-T G. 805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[1] This ITU-T Recommendation is intended to be aligned with the IETF MPLS RFCs normatively referenced by this Recommendation.

[ITU-T G.808.2] Recommendation ITU-T G.808.2 (2013), *Generic protection switching – Ring protection*.

[ITU-T G.8110.1] Recommendation ITU-T G.8110.1 (2011), *Architecture of the Multi-Protocol Label Switching transport profile layer network*.

[ITU-T G.8121] Recommendation ITU-T G.8121 (2016), *Characteristics of MPLS-TP equipment functional blocks*.

[IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[IETF RFC 5586] IETF RFC 5586 (2009), *MPLS Generic Associated Channel*.

[IETF RFC 5654] IETF RFC 5654 (2009), *Requirements of an MPLS Transport Profile*.

[IETF RFC 6371] IETF RFC 6371 (2011), *Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks*.

[IETF RFC XXXX] IETF RFC XXXX (draft-ietf-mpls-tp-shared-ring-protection-05), *MPLS-TP Shared-Ring protection (MSRP) mechanism for ring topology*.

[Editor's note: Update the ITU-T references as well as the reference to draft-ietf-mpls-tp-shared-ring-protection once the draft is published as an RFC. Other references to be added as appropriate.]

3 Definitions

<Check in the ITU-T terms and definitions database at www.itu.int/go/terminology-database whether the term has already been defined in another Recommendation. It would be more consistent to refer to such a definition rather than to redefine the term>

3.1 Terms defined elsewhere

<Normally, terms defined elsewhere will simply refer to the defining document. In certain cases, it may be desirable to quote the definition to allow for a stand-alone document>

This Recommendation uses the following terms defined elsewhere:

3.1.1 ring map [IETF RFC XXXX]:

NOTE – Ring map defined in [IETF RFC XXXX] is slightly different in meaning from the one that [ITU-T G.808.2] uses. The ring map in [ITU-T G.808.2] includes only the ring topology map information while the ring map in [IETF RFC XXXX] also includes the ring connectivity status information.

3.1.2 <Term 2> [Reference]: <optional quoted definition>.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 <Term 3>: <definition>.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CV Connectivity Verification

EXER Exercise

FS	Forced Switch
LP	Lockout of Protection
LSP	Label Switched Path
LW	Lockout of Working
MEG	Maintenance Entity Group
MEP	Maintenance Entity Point
MPLS	Multi-Protocol Label Switching
MPLS-TP	Multi-Protocol Label Switching – Transport Profile
MS	Manual Switch
MSRP	MPLS-TP Shared Ring Protection
NR	No Request
OAM	Operation, Administration and Maintenance
PDU	Protocol Data Unit
PS	Protection Switching
RPS	Ring Protection Switch
RR	Reverse Request
SF	Signal Fail
WTR	Wait to Restore

<Include all abbreviations and acronyms used in this Recommendation>

5 Conventions

<Mandatory clause. Describe any particular notation, style, presentation, etc. used within the Recommendation, if any. If none, write "None.">

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 is enclosed in parentheses ("(X)")

6 Overview

This Recommendation specifies MPLS-TP Shared Ring Protection switching mechanisms to be applied to MPLS-TP layer networks as described in [ITU-T G.8110.1].

Section 4.1 of [IETF RFC XXXX] provides an overview of MPLS-TP Shared Ring Protection.

7 Network objectives

The following objectives shall be met:

1. MPLS-TP ring protection shall be capable to protect against the following events:

   a) MPLS-TP Section layer failures
   b) Node failures

2. It shall be capable to protect point-to-point LSPs.
3. The transfer time (Tt), as defined in [ITU-T G.808.1]), for any of the above failures (single failure) shall be less than 50 ms in an MPLS-TP ring without congestion conditions impacting the transmission performances of the protection coordination protocol messages (see below), with all the nodes in idle state, with zero hold-off time (see below), with less than 1200 km of ring fibre circumference and up to 16 ring nodes.
4. Traffic types::
   a) Normal traffic: normal traffic as defined in [G.808.2] shall be protected.
   b) Non-pre-emptible unprotected traffic: this type of traffic is on the physical ring network but not protected by MPLS-TP ring protection.
   c) Pre-emptible extra traffic: this type of traffic is on the physical ring network but not protected by MPLS-TP ring protection.
5. Configurable hold-off times should be supported to avoid protection switching cascade in different network layers if a lower layer protection mechanisms are being utilized in conjunction with MPLS-TP layer ring protection mechanisms. Usage of hold-off timers allows the lower layers to restore working traffic before the MPLS-TP layer initiates shared ring protection actions.
6. Configurable wait to-restore times should be supported to avoid bouncing of the protection switching in case of unstable network failure condition.
7. Extent of protection
   a) In case of a single failure, it shall be capable to restore all protected traffic that would be passing through the failed location.
   b) It should be capable to restore all protected traffic, if possible, under multiple failures condition.
8. RPS protocol and algorithm
   a) The switching protocol shall be able to accommodate as minimum up to 127 nodes on a ring.
   b) The RPS protocol and associated section OAM functions shall accommodate the capability to upgrade the ring (node insertion / removal), limiting the possible impact on existing traffic to protection switching hits only.
   c) All spans on a ring shall have equal priority in case of multiple failures.
   d) The RPS protocol shall allow coexistence of multiple ring switch requests as a result of combination of failures and manual/forced request resulting in the ring segmenting into separate segments.
   e) The RPS protocol shall be reliable and robust enough to avoid any cases of missing of protection switch request as well as wrong interpretation of request.
9. Protection switching actions shall not create any traffic misconnection.
10. Only revertive operation type shall be supported.
11. Only bidirectional protection switching type shall be supported.

12. The following externally initiated commands shall be supported: Lockout of Working, Lockout of Protection, Forced Switch, Manual Switch, Exercise and Clear command.
13. The following automatically initiated commands shall be supported: Signal Fail – Working, Signal Fail – Protection, Wait-To-Restore, Reverse Request and No Request. The criteria for Signal Fail should be in harmony with definitions used in ITU-T Rec. G.8121/Y.1381.

[Editor's Note: Each network objective in this clause needs to make a reference to RFC 5654 and indicate the requirement number(s) shown in RFC 5654, if the corresponding requirement can be found. Not all the ring-related requirements in RFC 5654 need to be identified, but the requirement numbers included in this clause will be limited to the ones that this Rec. (or IETF RFC XXXX) can support: Text on the traffic types (normal, NUT, extra) needs to be enhanced. -- Contributions are invited.

8 Functional model

When an MPLS-TP transport path, such as an LSP, enters the ring, the ingress node on the ring pushes the working ring tunnel label according to the egress node and sends the traffic to the next hop. The transit nodes on the working ring tunnel swap the ring tunnel labels and forward the packets to the next hop. When the packet arrives at the egress node, the egress node pops the ring tunnel label and forwards the packets based on the inner LSP label and PW label.

MSRP ring tunnel is modelled as a server sub-layer for the MT LSP sub-layer. MSRP sub-layer functional model is described in Figure 8-1, which based on Figure 11-3 in [ITU-T G.808.2].

MSRP relies on "MPLS-TP section layer OAM" for fault detection, as indicated in section 4.2 of [IETF RFC XXXX], and to carry RPS protocol messages. Therefore, the server sub-layer for the MSRP is the MT (Section) sub-layer which provides Section OAM monitoring of the link.

[Editor's Note: For Figure 8-1, a generic figure based on Figure 11-3 in G.808.2 is needed]

Figure 8-1 – MPLS-TP Shared Ring Protection functional model

8.1 Label operations

This clause describes the forwarding operations for an example in section 4.1.3 of [IETF RFC XXXX] using the ITU-T functional model (complementing it with the description of how LSP1 traffic is forwarded outside of the ring). Figure 8-2 shows the example of label operations in the MPLS-TP shared ring protection mechanisms. In the figure, RcW_D and RaP_D denote clockwise working ring tunnel for node D and anticlockwise protection ring tunnel for node D, respectively.

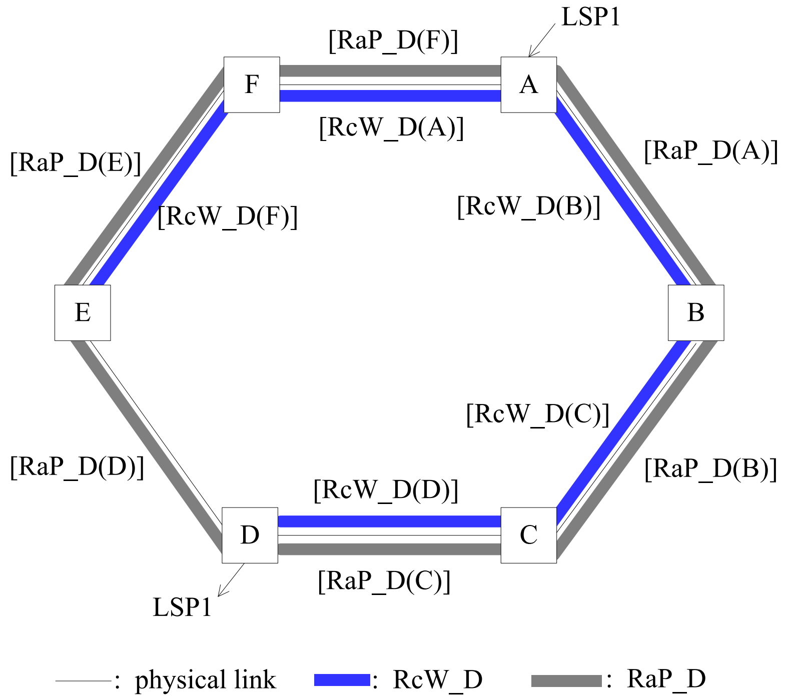

Figure 8-2 – Label operations of MPLS-TP Shared Ring Protection

8.1.1 Ingress node

Figure 8-3 describes the forwarding actions in the MT LSP sub-layer and the forwarding actions in the MSRP sub-layer for node A in Figure 8-2. Note that node B and node F are node A's adjacent nodes and East(N) represents the normal traffic going to the east port of node A.

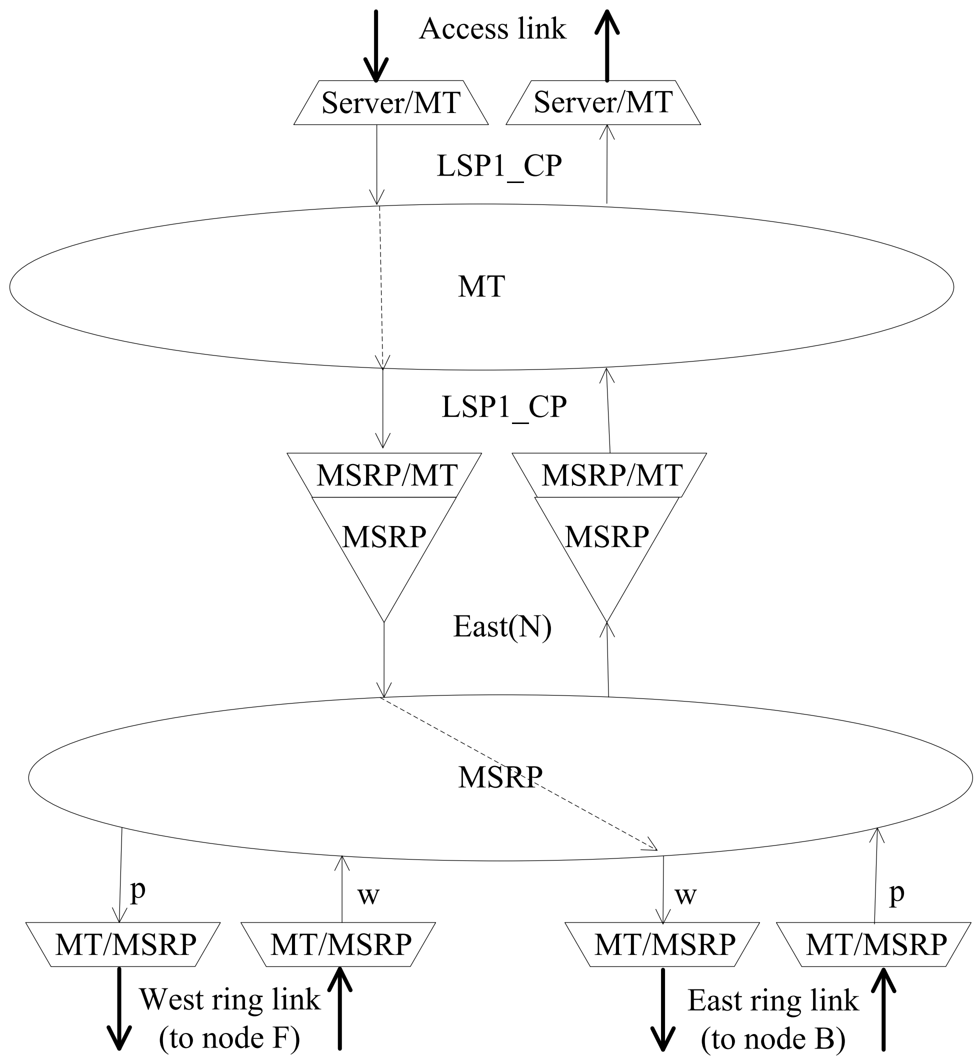

Figure 8-3 – Functional model of ingress node (node A)

Label operations performed up to the MPLS-TP LSP sub-layer on the traffic entering the ring at the ring ingress nodes depends on the role the ingress node plays at the MPLS-TP LSP sub-layer.

As shown in Figure 8-3, these label operations are modelled using the atomic functions already defined in [ITU-T G.8110.1] and [ITU-T G.8121], together with a new MSRP/MT_A atomic function to be defined in [ITU-T G.8121] for modelling the adaptation between the MPLS-TP LSP and the MSRP ring tunnel.

In Figure 8-3, node A is an LSR for the LSP1 entering the ring: in this case MPLS packets of LSP1 arrive at node A from an access link with the [LSP1(A)] label stack and the received LSP1(A) label value is swapped to the LSP1(D) label value assigned by the ring egress node D:

- The Server/MT_A_Sk function is configured to send the traffic unit received from the access link with the LSP1(A) label value to the MT_CP associated with LSP1.
- The MT_C atomic function is configured to forward the traffic from the MT_CP associated to LSP1 on the Server/MT_A_Sk to the MT_CP associated with LSP1 on MSRP_MT_A_So.

- Likewise the Server/MT_A_So function, defined in [ITU-T G.8121], the MSRP/MT_A_So function is configured to assign the LSP1(D) label value to the traffic units received from the MT_CP associated with LSP1.

The ingress node should also push [RcW_D(B)] ring tunnel label; this operation is modelled using the MSRP/MT_A, MSRP_TT, MSRP_C and MT/MSRP_A atomic functions shown in Figure 8-3.

- The MSRP/MT_A_So is configured with node D as the ring egress node ID for the traffic units received from the MT_CP associated with LSP1: this information is sent, together with the traffic unit, to the MSRP_TCP which is associated with the east (clockwise) direction.
- In normal conditions, the MSRP_C atomic function is configured to forward the traffic units, together with the ring egress node ID, from the MSRP_TCP associated with the east (clockwise) direction to the MSRP_CP associated with the working traffic on the east ring link;
- The MT/MSRP_A_So, on the east ring link, is configured to assign the label value RcW_D(B) to the traffic units received from MSRP_CP associated with the working traffic and whose ring egress node is node D.

8.1.2 Transit node

The ring tunnel label swapping operations in the transit nodes is modelled by using the MSRP_C and MT/MSRP_A atomic functions shown in Figure 8-4.

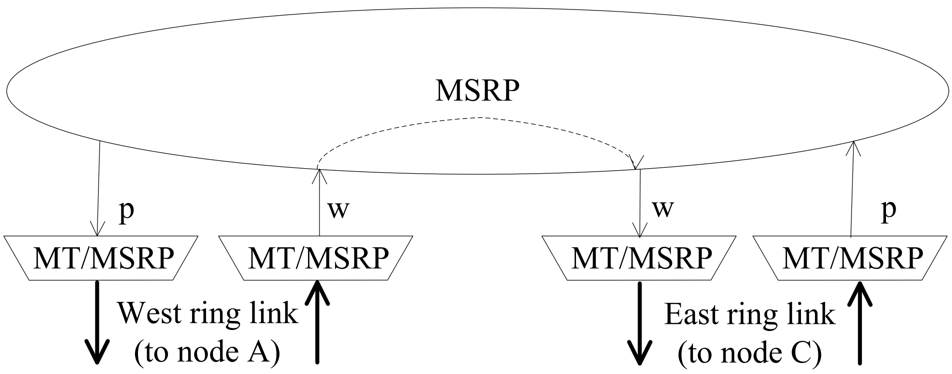

Figure 8-4 – Functional model of transit node (node B)

In node B, the ring tunnel label [RcW_D(B)] is swapped into [RcW_D(C)]:

- The MSRP/MT_A_Sk, on the west ring link, is configured to send the packets received with the top label [RcW_D(B)] through the MSRP_CP associated with the working traffic and that node D is the ring egress node for these packets.
- In normal conditions, the MRSP_C atomic function is configured to forward the traffic units, whose ring egress node is not node B, received from the MSRP_CP associated with the working traffic on the west ring link to the MSRP_CP associated with the working traffic on the east ring link: the ring egress node ID is also passed through.
- The MT/MSRP_A_So, on the east ring link, is configured to assign the label value RcW_D(C) to the traffic units received from MSRP_CP associated with the working traffic and whose ring egress node is node D.

8.1.3 Egress node

The egress node D should also perform a ring tunnel label pop operation, which can be modelled using the MSRP/MT_A, MSRP_TT, MSRP_C and MT/MSRP_A atomic functions shown in Figure 8-5.

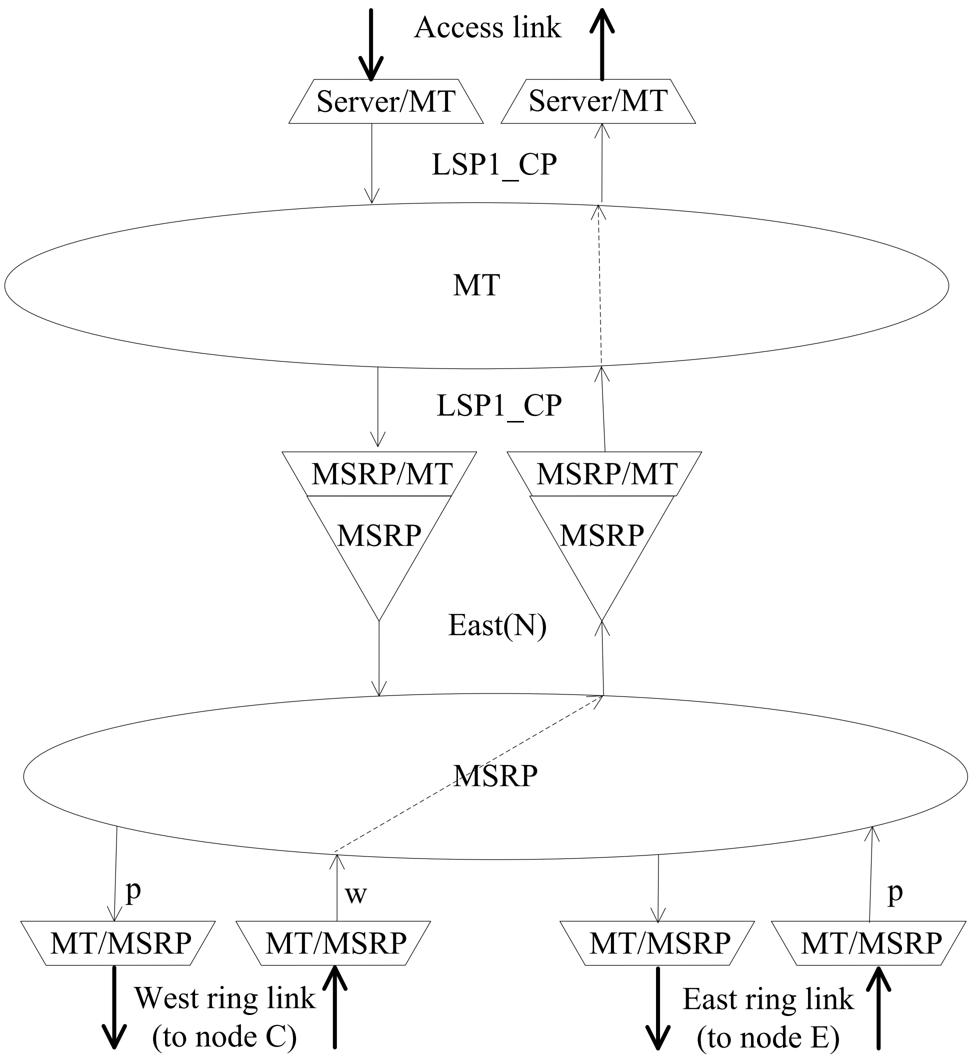

Figure 8-5 – Functional model of egress node (node D)

In node D the ring tunnel label [RcW_D(D)] is popped:

- The MT/MSRP_A_Sk, on the west ring link, is configured to send the packets received with the top label [RcW_D(D)] through the MSRP_CP associated with the working traffic and that node D is the ring egress node for these packets.
- In normal conditions, the MRSP_C atomic function is configured to forward the traffic units, whose ring egress node is node D, received from the MSRP_CP associated with the working traffic on the west ring link to the MSRP_TCP associated with the west (clockwise) direction.

Label operations performed up to the MPLS-TP LSP sub-layer on the traffic leaving the ring at the ring egress nodes depends on the role the egress node plays at the MPLS-TP LSP sub-layer.

As shown in Figure 8-5, these label operations can be modelled using the atomic functions already defined in G.8110.1 [4] and G.8121 [5], together with a new MSRP/MT_A atomic function to be defined in G.8121 [5] for modelling the adaptation between the MPLS-TP LSP and the MSRP ring tunnel.

In Figure 8-5, the ring egress node (node D) is an LSR for the LSP1 leaving the ring: in this case MPLS packets of LSP1 arrive at node D with the [LSP1(D)] label at the top of the label stack and the received LSP1(D) label value is swapped to the value assigned by node D's next hop X with LSP1(X) label value:

- The MSRP/MT_A_Sk function is configured to send the traffic unit received from the ring with the LSP1(D) label value to the MT_CP associated with LSP1.
- The MT_C atomic function is configured to forward the traffic from the MT_CP associated to LSP1 on the MSRP/MT_A_Sk to the MT_CP associated with LSP1 on Server_MT_A_So.
- The Server/MT_A_So function is configured to assign the LSP1(X) label value to the traffic units received from the MT_CP associated with LSP1.

9 Protection Architecture types

Three types of ring protection mechanisms are specified: wrapping, short wrapping and steering.

The mechanisms of three types of ring protection can be found in section 4.3 of [IETF RFC XXXX].

10 Switching types

MSRP supports only the bi-directional protection switching type. This means that in case of unidirectional failures, both directions of the protected MPLS-TP LSPs, including the affected direction and the unaffected direction, are switched to protection

11 Operation types

MSRP supports only the revertive protection operation type, which implies that the traffic will always return to (or remain on) the working entities if the switch requests are terminated.

If local Signal Fail (SF) that has been active previously now has become inactive, a local Wait-to-Restore state is entered. This state normally times out and becomes a No Request state and reverts back to the normal operation condition. The Wait-to-Restore timer is stopped if any local request of higher priority pre-empts this state.

12 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 [IETF RFC 6371].

How defect conditions on each MPLS-TP Section are detected is the subject of [ITU-T G.8121]. For the purpose of the MSRP switching process, a span within the ring has a condition of OK or failed (Signal fail (SF)).

Signal fail (SF) is declared when the MPLS-TP trail termination sink (MT_TT_Sk) function of an MPLS-TP Section MEP detects a trail signal fail as defined in [ITU-T G.8121].

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

13 Ring protection switch (RPS) protocol

The MSRP protection operations are controlled by the Ring Protection Switch Protocol (RPS) as described in section 5.1 of [IETF RFC XXXX].

13.1 Transmission and acceptance of RPS requests

RPS request messages are transmitted as described in section 5.1.1 of [IETF RFC XXXX].

13.2 RPS PDU format

The format of RPS PDU is as described in section 5.1.2 of [IETF RFC XXXX].

13.3 Ring node RPS state

The definition and detailed specification of the RPS states a ring node can enter are as described in section 5.1.3 of [IETF RFC XXXX].

13.4 RPS state transition

The rules of RPS state transition are as described in section 5.1.4 of [IETF RFC XXXX].

14 Misconnection avoidance

MSRP requires that the "label distribution policy" assigns a unique label value per path, in such a way that it avoids different label switched paths (LSPs) and Ring Tunnels to access the protection resource (even in transient phases) with the same label. A unique label per path is sufficient to prevent misconnections without the need to other mechanisms like squelching described in section 22.1 of [ITU-T G.808.2].

15 RPS switch initiation criteria

15.1 Administrative commands

Administrative commands, which can be initiated by the network operator, as described in section 5.2.1.1 of [IETF RFC XXXX].

15.2 Automatically initiated commands

Automatically initiated commands, which can be initiated based on MPLS-TP section layer OAM indication and the received switch requests, are described in section 5.2.1.2 of [IETF RFC XXXX].

Annex A

State transition tables of protection switching

(This annex forms an integral part of this Recommendation.)

RPS state machines are defined in section 5.2 of [IETF RFC XXXX]: section 5.2.3 defines the state transitions triggered by local requests; section 5.2.4 defines the state transitions triggered by remote RPS requests addressed to the node and section 5.2.5 defines the state transitions triggered by remote RPS requests addressed to a different node.

In order to avoid potential mistakes in duplicating the state transition tables from [IETF RFC XXXX], the tables are omitted in this Recommendation.

Annex B

Bandwidth sharing

(This annex forms an integral part of this Recommendation.)

The bandwidth on each ring is shared so that part of ring capacity is guaranteed for the working traffic and part is used for the protection traffic in case of failure on the ring. The part of the ring bandwidth rotating in one direction is used to carry the working traffic from the ring rotating in other direction in case of failure.

Both CIR and EIR traffic types can be either protected or unprotected.

Extra Traffic (in terms of SDH extra traffic) is not required: a similar capability can be achieved by unprotected best effort traffic

Appendix I

Wrapping and Steering examples

(This appendix does not form an integral part of this Recommendation.)

I.1 Wrapping

Operational examples of wrapping mechanism is shown in section 4.3.1 of [IETF RFC XXXX].

I.2 Short Wrapping

Operational examples of short wrapping mechanism is shown in section 4.3.2 of [IETF RFC XXXX].

I.3 Steering

Operational examples of steering mechanism is shown in section 4.3.3 of [IETF RFC XXXX].

Bibliography

[b-ITU-T X.yyy] Recommendation ITU-T X.yyy (date), *Title*.