INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG15-TD247R1/WP3

STUDY GROUP 15

Original: English

Question(s): 9/15 Geneva, 8-19 October 2018

TD

Source: Editor of G.mtdh

Title: Latest Draft to Recommendation G.mtdh

Purpose: Discussion

Contact:
Lei WANG
China Mobile Communications Group Co.,Ltd.
P.R. China

Tel: +86-10-15801696688-37077
Fax: +86-10-63601087
E-mail: wangleiyj@chinamobile.com

Keywords: MPLS-TP; Dual-homing; Protection

Abstract: This document provides the latest draft of Recommendation ITU-T G.mtdh “MPLS-TP Dual-homing Protection”.

Document history:

Version	Date	Description
0.01	Wd09-06R1 (02/2018) Geneva	Initial version created by input texts mainly from C468, C650 and C656
0.02	Cd01(07/2018)	The texts that were agreed on the formal Q9 correspondence activity related to the work on G.mtdh in May 2018. This version added the functional model and addressed some editor’s notes
0.03	WD0905R1 (10/2018) Geneva	Output of the October 2018 SG15 plenary meeting from C844, C850 and C1083

Draft Recommendation ITU-T G.mtdh

MPLS-TP Dual-Homing Protection

Summary

This Recommendation provides architecture and mechanisms for Pseudowire (PW) dual-homing protection in MPLS transport profile (MPLS-TP) networks. It also describes the Dual-Homing Coordination (DHC) protocol defined in [IETF RFC 8184] and [IETF RFC 8185].

The mechanisms defined herein protect point-to-point MPLS-TP PWs against failures within or at the edges of the MPLS-TP network.

Keywords

MPLS-TP; Dual-homing; Protection

Draft Recommendation ITU-T G.mtdh

MPLS-TP Dual-Homing Protection

1 Scope

This Recommendation provides architecture and mechanisms for Pseudowire (PW) dual-homing protection in MPLS transport profile (MPLS-TP) networks. It also describes the Dual-Homing Coordination (DHC) protocol defined in [IETF RFC 8184] and [IETF RFC 8185].

Both one-side and two-side dual-homing protection mechanisms are provided.

The mechanisms defined herein protect point-to-point MPLS-TP PWs against failures within or at the edges of the MPLS-TP network.

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.8121]	Recommendation ITU-T G.8121 (2016), *Characteristics of MPLS-TP equipment functional blocks*.
[ITU-T G.8113.1]	Recommendation ITU-T G.8113.1 (2016), *Operations, administration and maintenance mechanism for MPLS-TP in packet transport networks*.
[ITU-T G.8131]	Recommendation ITU-T G.8131 (2014), *Linear protection switching for MPLS transport profile*.

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

[IETF RFC 3985] IETF RFC 3985 (2005), *Pseudo Wire Emulation Edge-to-Edge (PWE3) 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 5921] IETF RFC 5921 (2010), *A Framework for MPLS in Transport Networks*

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

[IETF RFC 8184] IETF RFC 8184 (2017), *Dual-Homing Protection for MPLS and the MPLS Transport Profile (MPLS-TP) Pseudowires*

[IETF RFC 8185] IETF RFC 8185 (2017), *Dual-Homing Coordination for MPLS Transport Profile (MPLS-TP) Pseudowires Protection*

3 Definitions

<Editor's instruction: Check in the ITU-T Terms and definitions database on the public website whether the term is already defined in another Recommendation. It may be more consistent to refer to such a definition rather than redefine it>

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **Attachment Circuit** [IETF RFC 3985]

3.1.2 **Customer Edge** [IETF RFC 5921]

3.1.3 **Provider Edge** [IETF RFC 3985]

3.1.4 **Working transport entity** [ITU-T G.808]

3.1.5 **Protection transport entity** [ITU-T G.808]

3.1.6 **Recovery domain** [ITU-T G.7701]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **Attachment Circuit (AC) recovery domain**: A recovery domain that is adjacent to the MPLS-TP dual-homing protection domain and provides reliable transfer of information of the client traffic using two redundant attachment circuits (ACs) between the MPLS-TP dual-homing protection domain and one Customer Edge (CE) node.

3.2.2 **Dual-homing nodes:** Two Provider Edge (PE) nodes which are dual-homed to the same Customer Edge (CE) node to provide PE node resiliency at the boundary of the MPLS-TP transport network.

3.2.3 **Dual-Node Interconnection (DNI) transport entity:** The transport entity (i.e., PW) established between dual-homing nodes. The DNI transport entity is pre-established and used when there is a need of fast switchover.

3.2.4 **MPLS-TP dual-homing protection domain**: A recovery domain which is using the mechanisms defined in this Recommendation to provide reliable transfer of information of the client traffic through an MPLS-TP network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC	Attachment Circuit
APC	Automatic Protection Coordination
CE	Customer Edge
DHC	Dual-Homing Coordination
DNI	Dual-Node Interconnection
LSP	Label Switched Path
MEP	Maintenance Entity Point
MPLS	Multi-Protocol Label Switching
MPLS-TP	Multi-Protocol Label Switching Transport Profile
OAM	Operation, Administration and Maintenance
PE	Provider Edge
PW	Pseudowire
SF	Signal Fail
WTR	Wait to Restore

<Include all abbreviations and acronyms used in this Recommendation>

5 Conventions

In this document, the term Dual-Homing Coordination (DHC) protocol is used to describe the means to coordinate the two MPLS-TP dual-homing nodes via the exchange of messages as defined in [IETF RFC 8185].

6 Overview

[IETF RFC 8184] describes the scenarios and applications for using Dual-Node Interconnection (DNI) PW to provide the dual-homing protection. Both one-side and two-side dual-homing protection scenarios are provided as described in section 2.2.1 and in section 2.2.2 of [IETF RFC 8184] respectively.

Figure 6-1 illustrates a reference network to describe the one-side dual-homing protection scenario where one CE (i.e., CE1) is attached to single node A and another CE (i.e.,CE2) is attached to two dual-homing nodes (Z1 and Z2). A working transport entity (i.e., working PW) connects node A to node Z1, a protection transport entity (i.e., protection PW) connects node A to node Z2, and a DNI transport entity (DNI PW) is used to provide connectivity between nodes Z1 and Z2 during protection switching conditions. MPLS-TP LSPs are established as underlay server-layer trails for each PW but they are not shown in Figure 6-1.

In Figure 6-1, if Attachment Circuit (AC) to Z1 (i.e., AC1) fails, then the AC to Z2 (i.e., AC2) is activated and DNI PW forwards the traffic between Z1 and Z2, so that the working PW works as usual.

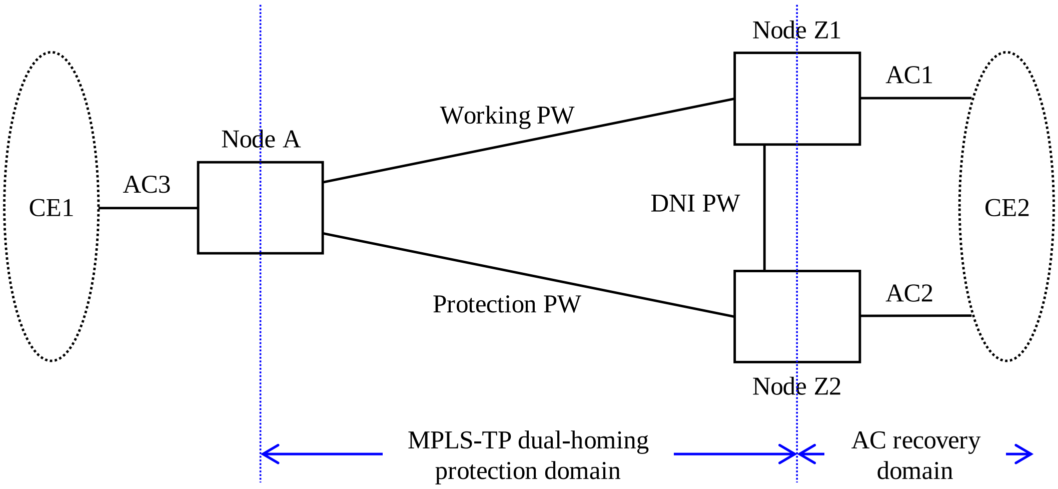

Figure 6-1 – One-side MPLS-TP dual-homing reference network

[IETF RFC 8185] specifies the mechanisms to provide the dual-homing protection against the failures within the MPLS-TP dual-homing protection domain and the Dual-Homing Coordination (DHC) protocol to coordinate protection switching action between dual-homing nodes (Z1 and Z2). The coordination messages are transported on the DNI transport entity (DNI PW) over the Generic Associated Channel (G-ACh).

This Recommendation assumes that the automatic protection coordination (APC) protocol, defined in [ITU-T G.8131], is used to coordinate protection switching actions between the two ends of the MPLS-TP dual-homing protection domains (i.e., nodes A and Z2).

Figure 6-2 illustrates a reference network to describe the two-side dual-homing protection scenario where the CE1 is also attached to two dual-homing nodes (A1 and A2). In this case, one DHC protocol is used to coordinate protection switching between nodes A1 and A2, and the other DHC protocol is used to coordinate protection switching between nodes Z1 and Z2, and the APC protocol is assumed to be used to coordinate protection switching between nodes A2 and Z2.

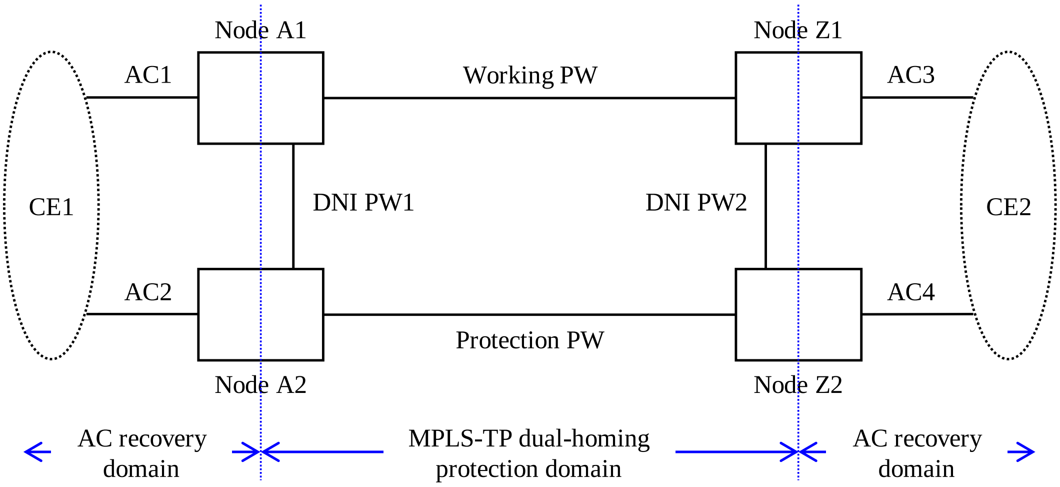

Figure 6-2 – Two-side MPLS-TP dual-homing reference network

The mechanisms used to provide protection against failures within the Attachment Circuit (AC) recovery domains are outside the scope of this Recommendation. It is assumed that these mechanisms will activate one and only one AC at a given time within each AC recovery domain and are capable to report the active/stand-by status of a local AC to the PE node.

The MPLS-TP PW dual-homing protection mechanisms operates independently from the client layer protocols (i.e., the client services in transport) encapsulated in the PW and therefore are applicable to any PW client such as Ethernet, TDM and ATM.

Through these working and protection PWs and their LSPs, services over dual-homing nodes can be protected from a single failure on either the working PW, the protection PW, a dual-homing node

(node Z1 or node Z2) or an AC connecting a CE with dual-homing nodes. Recovery of multiple-failure scenarios is outside the scope of this Recommendation.

7 Dual-homing Protection Architecture

Dual-homing protection architecture is based on 1:1 PW trail protection.

It supports only bidirectional protection switching type, i.e., both directions of the connection for a service, including the affected direction and the unaffected direction, are switched to protection.

Both revertive and non-revertive operation types are supported.

Both one-side and two-side dual-homing architectures are supported.

7.1 One-side dual-homing

In one-side dual-homing, only one side of the client sites is dual-homed. The scenario is described in Section 2.2.1 of [IETF RFC 8184].

7.2 Two-side dual-homing

In two-side dual-homing, both sides of the client sites are dual-homed. The scenario is described in Section 2.2.2 of [IETF RFC 8184].

8 Protection Signalling

To coordinate the switching of working and protection PW (i.e., the working and protection transport entities) and activate the DNI PW (i.e., DNI transport entity), between the dual-homing nodes, the DHC protocol as specified in Section 4 of [IETF RFC 8185] shall be used. Any status and switchover coordination messages between the dual-homing nodes shall be sent over Generic Associated Channel (G-ACh) [IETF RFC 5586] of the DNI PW.

The switching of working and protection PW, between the two ends of the MPLS-TP dual-homing protection domains, is coordinated using the mechanisms defined in [ITU-T G.8131]. The APC messages shall be sent over the protection PW as defined in [ITU-T G.8131].

9 Functional model

The end points of each working transport entity shall have PW OAM functions to monitor the status of the working transport entity (working PW). Because the protection transport entity and the DNI transport entity are pre-established, the status of the protection transport entity (protection PW) and of the DNI transport entity (DNI PW) shall also be monitored at the end points using PW OAM functions.

APC messages are transported over the protection transport entity, and the DHC messages are exchanged over the DNI transport entity.

The functional architecture of DNI protection is shown in Figure 9-1.

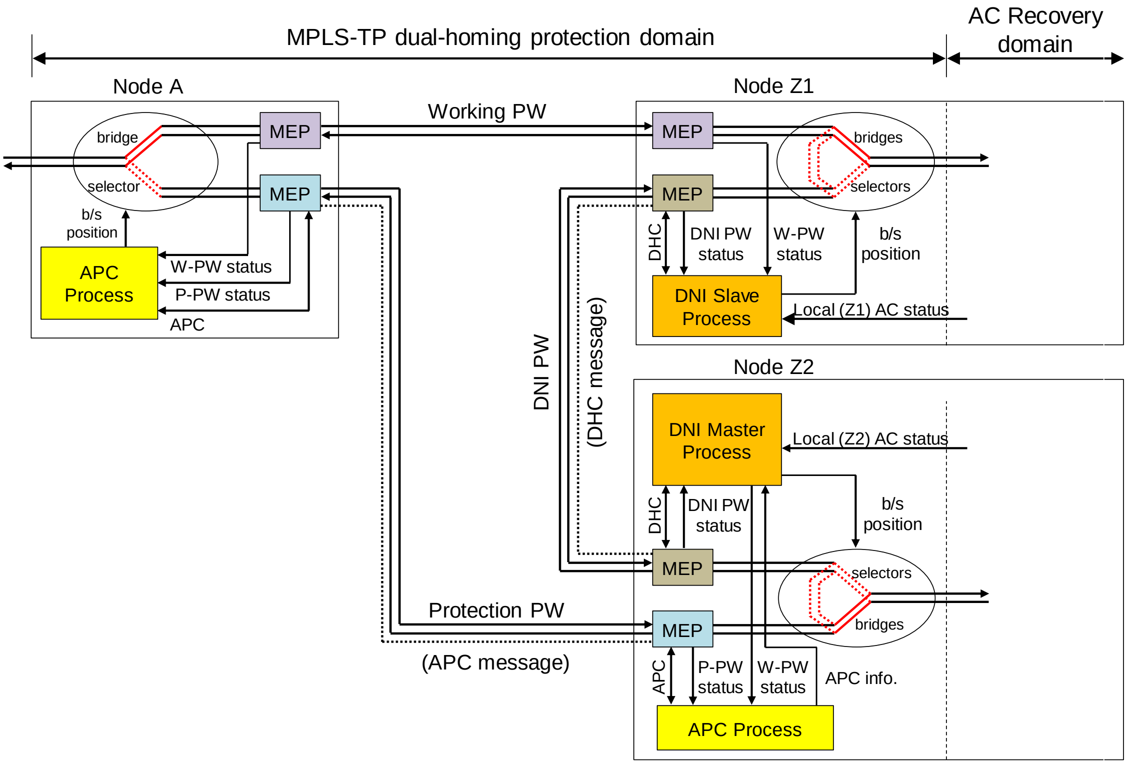

Figure 9-1 MPLS-TP Dual-homing protection architecture

Node A implements PW trail protection, as defined in [ITU-T G.8121], so that protection switching to the protection PW in both directions can be realized as specified in [ITU-T G.8131]; while nodes Z1 and Z2 implement PW DNI protection, as defined in this Recommendation and in [IETF RFC 8184] and [IETF RFC 8185].

The bridges/selectors, in nodes Z1 and Z2, implement the forwarding behavior defined in Table 1 of [IETF RFC 8185].

The APC process in node Z2 determines the new switching states of the working PW and the protection PW based on the local status of the protection PW (determined by the protection PW MEP), the status of the working PW (from the DHC messages received by the DNI Master Process), the local operator's commands and the APC messages exchanged with the remote node A. The switching state of a PW indicates whether the PW is active (i.e., used for transmitting and receiving traffic) or not. Only one of the working and protection PWs should be active at any given time.

The DNI Master process in node Z2 controls the bridges/selectors forwarding behavior within node Z2, implementing the state machine defined in [IETF RFC 8185] based on the local status of the DNI PW (determined by the DNI PW MEP), the local AC status, and the switching state of the protection PW (determined by the APC process). It also exchanges DHC messages with the peer DNI Slave process to send the switching state of the working PW (determined by the APC process) and to receive the peer status of the working PW.

The DNI Slave process in node Z1 controls the bridges/selectors forwarding behavior within node Z1, implementing the state machine defined in [IETF RFC 8185] based on local status of the DNI PW (determined by DNI PW MEP), the local AC status, and the switching state of the working PW (based on received DHC messages). It also transmits to the peer DNI Master process, DHC messages carrying the local status of the working PW (determined by the working PW MEP).

The MPLS-TP dual-homing protection switching is modelled as an MPLS-TP dual-homing protection sub-layer (MTd), as shown in Figures 9-2 and 9-3:

- The MTd_C atomic function is a connection function implementing the dual-homing protection switching using the bridges/selectors, the DNI processes and the APC process as shown in Figure 9-1. The MTd_C atomic functions in nodes Z1 and Z2 differ depending on whether the APC process exists or not and whether the DNI process is a master or a slave.
- The MT/MTd_A atomic function inserts/extracts the APC and DHC messages to/from the protection PW and DNI PW respectively.

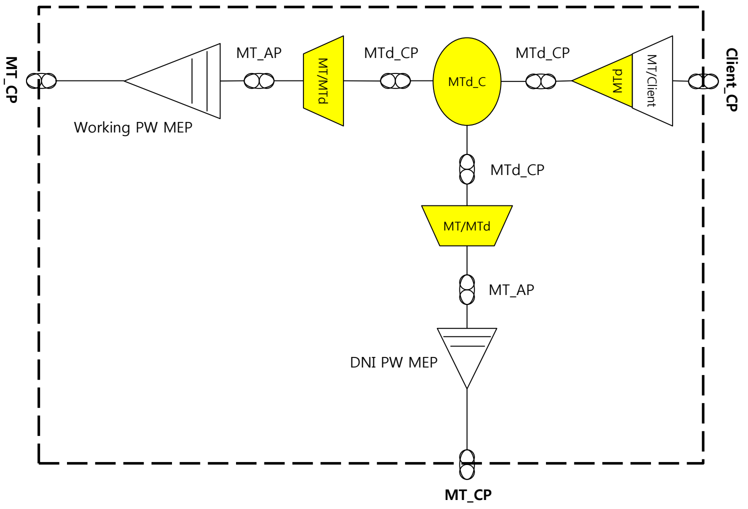

Figure 9-2 MPLS-TP dual-homing protection sub-layer (Z1)

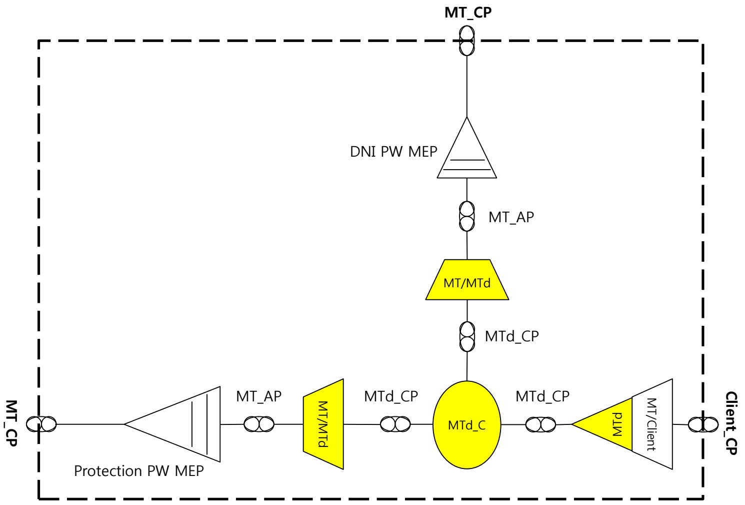

Figure 9-3 MPLS-TP dual-homing protection sub-layer (Z2)

10 Hold-off timer

MPLS-TP dual-homing protection relies upon the hold-off timer logic defined in [ITU-T G.8131] to coordinate timing of protection switches at multiple layers for working and protection PWs.

As a consequence, the hold-off timer of the APC process within the protection PE shall be configured via MTd_C_MI_PS_HoTime.

11 Wait-to-restore timer

MPLS-TP dual-homing protection relies upon the WTR state defined in [ITU-T G.8131] to prevent frequent operations of the protection switch due to an intermittent defect of the working transport entity.

As a consequence, the wait-to-restore timer of the APC process within the protection PE shall be configured via MTd_C_MI_PS_WTR.

12 Protection Procedures

Protection procedures for MPLS-TP PW dual-homing mechanisms are defined in section 4.2 of [IETF RFC 8185].

Some examples on how they apply to one-side and two-side dual-homing scenarios are provided in Appendix I.

13 External Commands

MPLS-TP dual-homing protection relies upon the external commands applied to the APC process, as defined in [ITU-T G.8131], to allow operator’s control of the working and protection transport entities’ switching state. In case of multiple protection switching requests, the priority logic defined in [ITU-T G.8131] is used to determine the switching states of the working and protection transport entities.

As a consequence, the external command shall be inputted to the APC process within the protection PE via MTd_C_MI_PS_ ExtCMD.

14 Failure Detection

The MPLS-TP PW layer OAM is used to monitor the status of the working PW, the protection PW and the DNI PW(s). Dual-homing nodes in the dual-homing protection domain shall support the PW OAM mechanisms as defined in Section 4.3 of [IETF RFC 6371] and [ITU-T G.8113.1] or [ITU-T G.8113.2].

The defect conditions on each MPLS-TP PW are detected as defined in [ITU-T G.8121] and [ITU-T G.8121.1] or [ITU-T G.8121.2].

Signal fail (SF) is declared on working and protection PW when the MPLS-TP trail termination sink (MT_TT_Sk) function in the MPLS-TP dual-homing protection domain detects a trail signal fail as defined in [ITU-T G.8121].

Signal degrade (SD) is declared on working and protection when the MPLS-TP trail termination sink (MT_TT_Sk) function in the MPLS-TP dual-homing protection domain detects a trail signal degrade as defined in [ITU-T G.8121].

DNI PW is declared to be in a Down state when the MPLS-TP trail termination sink (MT_TT_Sk) function detects a trail signal fail or a remote defect indication (RDI) condition as defined in [ITU-T G.8121].

A dual-homing node failure is regarded as the failure of the AC and of the two PWs attached to that dual-homing node.

Annex A

Forwarding state tables of protection switching

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

The state machines for MPLS-TP dual-homing protection are defined in section 4 of [IETF RFC 8185]. In order to achieve MPLS-TP dual-homing protection, the dual-homing nodes need to exchange the PW status and protection coordination requests to coordinate their behaviors.

In order to avoid potential mistakes in duplicating the state transition tables from [IETF RFC 8185], the tables are omitted in this Recommendation.

Appendix I

One-side and Two-side dual-homing protection examples

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

I.1 One-side dual-homing

One-side dual-homing protection is shown in Section 2.2.1 of [IETF RFC 8184] and in Figure 6-1.

When the local AC of node Z1 fails, nodes Z1 and Z2 follow the recovery procedures described in section 4.2 of [IETF RFC 8185] while node A does not perform any protection switching action. After the recovery procedures are completed, node A keeps forwarding the traffic between its local AC (A) and the working PW; node Z1 forwards traffic between the working PW and the DNI-PW; and node Z2 forwards traffic between the DNI-PW and its local AC (Z2).

When the working PW fails, nodes A, Z1 and Z2 apply the recovery procedures described in section 4.2 of [IETF RFC 8185]: in particular nodes A and Z2 uses the protection switching mechanisms defined in [ITU-T G.8131] to coordinate the activation of the protection PW. After the recovery procedures are completed, node A forwards traffic between its local AC(A) and the protection PW; node Z2 forwards traffic between the protection PW and the DNI-PW; and node Z1 forwards traffic between the DNI-PW and its local AC (Z1).

When node Z1 fails, nodes A and Z2 follow the recovery procedures described in section 4.2 of [IETF RFC 8185]: in particular they use the protection switching mechanisms defined in [ITU-T G.8131] to coordinate the activation of the protection PW. After the recovery procedures are completed, node A forwards the traffic between its local AC (A) and the protection PW; and node Z2 forwards traffic between the protection PW and its local AC (Z2).

I.2 Two-side dual-homing

Two-side dual-homing protection is shown in Section 2.2.2 of [IETF RFC 8184] and Figure 6-2.

When the local AC of node Z1 fails, nodes Z1 and Z2 follow the same recovery procedures described in section 4.2 of [IETF RFC 8185], which are independent on whether the other side is using or not using dual-homing, while nodes A1 and A2 do not perform any protection switching action. After the recovery procedures are completed, node A1 keeps forwarding traffic between its local AC (A1) and the working PW; node Z1 forwards traffic between the working PW and its DNI-PW (Z1-Z2), and node Z2 forwards traffic between its DNI-PW (Z1-Z2) and its local AC (Z2).

When the working PW fails, nodes A1 and A2, as well as nodes Z1 and Z2, follow the same recovery procedures described in section 4.2 of [IETF RFC 8185], which are independent on whether the other side is using or not using dual-homing: in particular nodes A2 and Z2 use the protection switching mechanisms defined in [ITU-T G.8131] to coordinate the activation of the protection PW. After the recovery procedures are completed, node A1 forwards traffic between its local AC (A1) and its DNI-PW (A1-A2); node A2 forwards the traffic between its DNI PW (A1-A2) and the protection PW; node Z2 forwards the traffic between the protection PW and its DNI-PW (Z1-Z2), and node Z1 forwards the traffic between its DNI-PW (Z1-Z2) and its local AC (Z1).

When node Z1 fails, node Z2 follows the same recovery procedures described in section 4.2 of [IETF RFC 8185], which are independent on whether the other side is using or not using dual-homing, while nodes A1 and A2 follows the same recovery procedure described above for the case of a working PW failure: in particular nodes A2 and Z2 uses the protection switching mechanisms defined in [ITU-T G.8131] to coordinate the activation of the protection PW. After the recovery procedures are completed, node A1 forwards traffic between its local AC (A1) and its DNI-PW (A1-A2); node A2 forwards the traffic between its DNI PW (A1-A2) and the protection PW, and node Z2 forwards traffic between the protection PW and its local AC (Z2).

Appendix II

Network Objectives

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

1) MPLS-TP dual-homing protection shall be capable of protecting against the following events:

   a) MPLS-TP PW layer failures, without relying on restoration on a particular server layer;

   b) Dual-homing edge node failures;

   c) Ingress and/or egress link failures, but how the edge nodes detect an ingress and/or egress link failure or coordinate with the client site to switch to another dual-homing ingress and/or egress link is out of the scope;

2) Transfer time (T_t) in response to a single failure should be less than 50 ms within the MPLS-TP network;

3) Support only bidirectional protection switching to ensure that forward traffic and reverse traffic of a protected service are always co-routed;

4) Reuse the OAM mechanisms as defined for MPLS-TP (e.g., see [ITU-T G.8113.1]);

5) Reuse the linear protection mechanism as specified in [ITU-T G.8131], and be capable to coexist with them;

6) The following externally initiated commands shall be supported (Requirement 76 of [IETF RFC 5654]): Lockout of Working, Lockout of Protection (Requirement 105 of [IETF RFC 5654]), Forced Switch, Manual Switch, Exercise and Clear.

7) 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 are the same as used in [ITU-T G.8121]).

8) Support the nesting of multiple levels of protection (such as linear protection in the server LSP layer). To achieve this, mechanism(s) that allow for coordination of protection activities (e.g., hold-off timer) shall be supported.

9) Avoid protection switching flapping (e.g., support of wait-to-restore timer);

10) Protection switching activation can be initiated by either end or both ends of the MPLS-TP dual-homing protection domain.

11) Both revertive and non-revertive protection switching should be supported.

12) Prioritized protection between signal fail (SF), signal degrade (SD) and operator requests should be supported.