INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

COM 15 – LS 2 – E

English only

Original: English

Question(s):	9/15	Madeira, 26-30 November 2007

LIAISON STATEMENT

Source:	ITU-T SG15 Q9/15
Title:	T-MPLS Ring Protection

LIAISON STATEMENT

To:	**IETF MPLS, CCAMP, PWE3 and L2VPN**
Approval:	**ITU-T SG15. Q9/15 meeting (Madeira, 26-30 November 2007)**
For:	**Information/comment**
Deadline:	**11/2/2008**

Contact:	Ghani Abbas Ericsson, Sweden	Tel: +44 115 850 1011 Fax: +44 115 850 1061 Email: Ghani.Abbas@ericsson.com

SG15 Q9 has nearly completed its work on a recommendation for T-MPLS Ring Protection - G.8132. It is targeted to consent this new recommendation in the next SG15 plenary meeting scheduled for Feb., 2008.

We have attached the latest draft for your information and comments.

Question(s):	9/15	**Meeting, date:**	Madeira, 26 – 30 November 2007
Study Group:	15 **Working Party:** 3	**Intended type of document**: WD	18r1_nd
Source:	Editors G.8132		
Title:	Draft ITU-T Recommendation G.8132 (T-MPLS shared protection ring)		

Contact:	Huub van Helvoort Huawei Technologies Co., Ltd. P.R.China	Tel: +31 36 5315076 Email: hhelvoort@huawei.com
Contact:	Igor Umansky Alcatel-Lucent Israel	Tel: +972 3 9202871 Email: igor.umansky@alcatel-lucent.com

Abstract

This document contains the latest draft of G.8132 (T-MPLS Shared Protection Ring). It is the result of drafting based on wd18 and other contributions presented in the Q9/15 Madeira meeting in November 2007.

CONTENTS

Draft ITU-T Recommendation G.8132

T-MPLS Shared Protection Ring (TM-SPRing)

Summary

<Mandatory material>

Keywords

T-MPLS, ring protection, wrapping, steering, APS

Introduction

1 Scope

This Recommendation specifies T-MPLS Shared Protection Ring (TM-SPRing) protection switching mechanisms and the APS protocol to be applied to T-MPLS layer networks as described in G.8110.1. The mechanisms defined herein protect T-MPLS sections and is designed to support point-to-point as well as point-to-multipoint T-MPLS connections.

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

[1] ITU-T Recommendation G.780 /Y.1351 (2004), *Terms and definitions for synchronous digital hierarchy (SDH) networks.*

[2] ITU-T Recommendation G.783 (2004), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks.*

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

[4] ITU-T Recommendation G.806 (2000), *Characteristics of transport equipment – Description methodology and generic functionality.*

[5] ITU-T Recommendation G.841 (1998), *Types and characteristics of SDH network protection architectures.*

[6] ITU-T Recommendation G.870/Y.1352 (2004), *Terms and definitions for Optical Transport Networks (OTN)*

[7] ITU-T Recommendation G.8114/Y.1373 (2007), *T-MPLS OAM mechanisms*

[8] ITU-T Recommendation G.8121 (2006), *Characteristics of Transport MPLS equipment functional blocks.*

[9] ITU-T Recommendation G.8110.1 (2006), *Architecture of Transport MPLS (T-MPLS) Layer Network.*

3 Definitions

<Check in ITU-T Terms and definitions database under http://www.itu.int/sancho/index.htm if the term is not already defined in another recommendation. It could be more consistent to refer to such a definition rather than redefine it>

The terms used in the sections below are as those defined in G.780/Y.1351:

3.1 bidirectional protection switching

3.2 drop-and-continue

The terms used in the sections below are as those defined in G.805:

3.3 signal degrade (SD)

3.4 signal fail (SF)

3.5 trail

The terms used in the sections below are as those defined in G.806:

3.6 defect

3.7 failure

The terms used in the sections below are as those defined in G.870/Y.1352:

3.8 APS protocol: 1-phase

3.9 Protection class

3.9.1 Trail protection

3.10 Switch

3.10.1 Forced Switch

3.10.2 Manual Switch

3.11 Component

3.11.1 Bridge

3.11.2 Switch

3.12 Architecture

3.12.1 non-revertive protection switching

3.13 Signals

3.13.1 Traffic signal

3.13.2 Normal traffic signal

3.13.3 Unprotected traffic signal

3.14 Timers

3.14.1 Hold-off time

3.14.2 Wait-to-restore time

Editors' note: add definition for 'span' term.

4 Abbreviations

<Include all abbreviations used in this Recommendation>

This Recommendation uses the following abbreviations:

APS	Automatic Protection Switching
CV	Connectivity Verification
EXER	Exercise
FS	Forced Switch
LP	Lockout of Protection
LW	Lockout of Working
MEG	Maintenance Entity Group
MEP	Maintenance Entity Point
MPLS	MultiProtocol Label Switching
MS	Manual Switch
NR	No request
OAM	Operation, Administration and Maintenance
PDU	Payload Data Unit
PS	Protection Switching
RR	Reverse Request
SD	Signal Degrade
SF	Signal Fail
SSF	Server SF
SPRing	Shared Protection Ring
TMC	T-MPLS Circuit
TMP	T-MPLS Path
T-MPLS	Transport MPLS
TMS	T-MPLS Section
WTR	Wait to Restore

5 Conventions

None.

6 Introduction

TM-SPRing consists of two layer networks: the T-MPLS Section layer and the T-MPLS Path layer, which is considered a client layer of the T-MPLS section layer.

The T-MPLS section layer is used for monitoring the connectivity between each two adjacent nodes (using T-MPLS OAM mechanisms) and transmitting the APS information. The architecture and operation of TM-SPRing equipment is described in Recommendation G.8121.

7 Network objectives

The following objectives shall be met:

1) The T-MPLS Section layer protects against any failure that is detected by the T-MPLS section OAM
2) Protected entities: p-t-p and p-t-mp T-MPLS connections.
3) Switch time: the completion time for protection against a single failure shall be less than 50 ms assuming a reference network with a 16 nodes ring of and less than 1200 km of fibre and no hold-off timer.

Editors' note: check for validity of this requirement.

4) Traffic types
   a) Normal traffic: this type of traffic must be protected against any single failure.
   b) Non-preemptable unprotected traffic: this type of traffic is not protected by the ring protection scheme.

NOTE – In the event of a failure on the ring, only the normal traffic, i.e., type a), is protected

5) Hold-off time: to avoid protection switching cascade in different network layers when a lower layer network protection mechanism is activated in conjunction with the T-MPLS layer protection scheme. Usage of hold-off timers allows the lower layer to restore working traffic before the T-MPLS layer initiates a protection action.
6) Wait to-restore time: to avoid flapping of the protection switching in case of unstable network failure conditions.
7) Extent of protection
   a) For a single failure, the ring will restore all normal traffic that would be passing through the failed location.
   b) The ring should restore all normal traffic, if possible, under multiple failure conditions.
8) APS protocol and algorithm
   a) The switching protocol shall be able to accommodate as a minimum up to 127 nodes on a ring.
   b) The APS protocol and associated OAM functions shall accommodate the capability to upgrade the ring (node insertion / removal), limiting the possible impact on existing traffic on the ring.
   c) All spans on a ring shall have equal priority in case of multiple failures.
   d) The APS 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 APS protocol must be reliable and robust enough to avoid any cases of missing protection switch requests as well as wrong interpretation of a request.
9) Traffic misconnections shall not be allowed when the protection switching event takes place.
10) Operation modes: Revertive switching shall be provided.

11) Protection switching modes: bidirectional protection switching shall be supported.

12) Manual control: The following externally initiated commands shall be supported: Lockout of Working, Lockout of Protection, Forced Switch and Manual Switch, Exerciser and Clear command.

13) Switch initiation criteria: The following automatically initiated commands shall be supported: Signal Failure, Wait-To-Restore, Reverse Request and No Request.

NOTE – Multiple ring protection schemes are for further study.

8 Functional model

The TM-SPRing functional model is illustrated in Figure 8-1. It represents the node state in a normal condition. It is shown that:

- Normal (protected) traffic as well as non-preemptable (unprotected) traffic are supported.
- Add, drop, drop-and-continue, pass-through connections can be normal or unprotected.
- The functional model proposed in this document supports label swapping along the ring.
- Pass-through protection connections in the protection connection function are established only on a failure event, which prevents the creation of the closed loop for protection connections in normal conditions.

The following symbols are used in Figure 8-1:

- TMS – T-MPLS Section layer
- TMSP – T-MPLS Section Protection sub-layer
- TMSP_C – T-MPLS section protection sub-layer Connection function
- TMP – T-MPLS Path layer

Editors' note: When the functional model will be introduced in G.8121 it shall be removed from this specification.

Editors' note: replace TMSP2fsh with TMSP_C

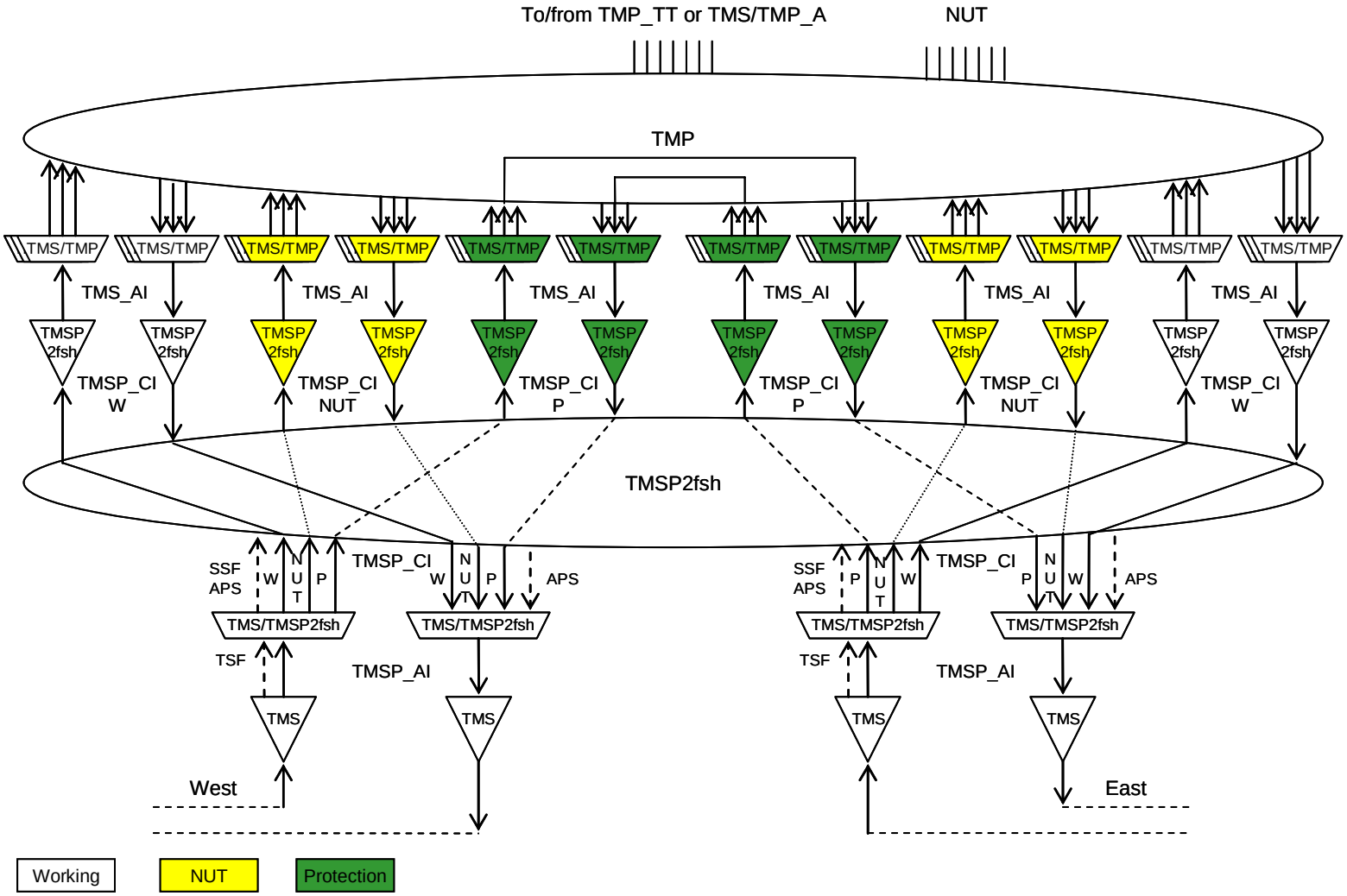


Figure 8-1 – T-MPLS Shared Protection Ring functional model

9 TM-SPRing - OAM model

9.1 Introduction

Each ring port in each ring node is configured as a TMS TM-MEP (Maintenance Entity Point). Each pair of ports on a span, i.e. each pair of MEPs in adjacent nodes, forms a MEG (Maintenance Entity Group). So there are *n* MEGs if there are *n* spans on the ring.

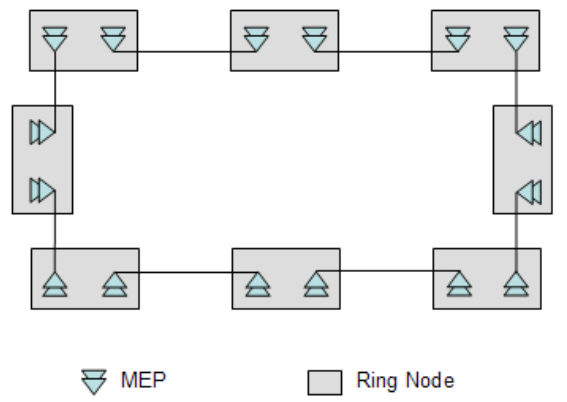


Figure 9-1/G.8132 – OAM Configuration for T-MPLS SPRing

T-MPLS SPRing has only one level of OAM functionality. Figure 9-1/G.8132 details the OAM configuration with one MEG level. The MEPs monitor the state of the T-MPLS section between adjacent nodes using the OAM mechanism defined in G.8114/Y.1373. CV is used to check the continuity and connectivity between each pair of MEPs in a MEG.

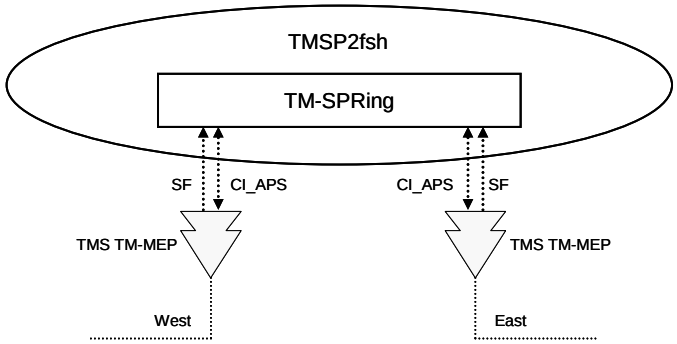


Figure 9-2/G.8132 – OAM Model for T-MPLS SPRing

Figure 9-2/G.8132 describes the T-MPLS SPRing OAM model in a ring node. The T-MPLS SPRing process accomplishes the T-MPLS SPRing protection switching and OAM APS packets processing in each node.

9.2 APS Process for T-MPLS SPRing

When the MEP does not detect any defects it sends periodically APS packets in West and East direction, indicating no switch request. The destination node information in APS packets is the Node ID of the adjacent node in the West or the East direction.

When a MEP detects a defect (i.e. SF), it will inform the T-MPLS SPRing process, and the T-MPLS SPRing process will generate CI_APS in the West and East directions, indicating the appropriate bridge request. The destination node information in APS packets is the Node ID of the node adjacent to the detected defect.

When a MEP receives the APS packets it will send APS information (CI_APS) to the T-MPLS SPRing process, the process checks the destination node information in the APS information field. If the destination node information matched the receiving node ID, the node terminates the APS flow and processes the APS information. Otherwise, if the destination node information indicates other node ID and there is no higher priority local request, the APS information is transferred unaltered to the next node in the ring.

10 Architecture types

T-MPLS Shared Protection Ring consists of two counter-rotating rings, transmitting in opposite directions relative to each other. T-MPLS switched rings require only two server layer section connections for each span of the ring. Each server layer section connection carries both working and protection traffic (in a ring failure event).

10.1 Wrapping

The Wrapping technique implies that the node that detects a failure sends a request through the APS protocol to the node adjacent to the failure. When the node detects a failure or receives a bridge request through APS protocol addressed to this node, normal traffic transmitted towards the failed span is switched to the opposite direction (away from the failure). This traffic travels the long way around the ring to the other switching node where it is switched back onto the working direction. The switching nodes restore normal traffic flow when the failure or APS protocol request is cleared.

An example of wrapping is provided in Appendix I.1.

10.2 Steering

The Steering technique implies that the node that detects a failure sends a request through the APS protocol to the node adjacent to the failure and all nodes in the ring process this APS information. In case of p-t-p connections, for each affected connection the source node (that adds traffic to the ring) and the sink node (that drops the traffic from the ring) perform switching from working to the protection direction, and restore normal traffic flow when the failure or APS protocol request is cleared.

An example of steering is provided in Appendix I.2.

NOTE – Steering is for further study.

NOTE – The p-t-mp connection protection by the steering mechanism is for further study.

11 Switching types

TM-SPRing supports only the bi-directional protection switching type. In bi-directional switching, both directions of the monitored T-MPLS section layer, including the affected direction and the unaffected direction, are switched to protection.

12 Operation Types

TM-SPRing supports only the revertive protection operation type, which implies that the service will always return to (or remain on) the working connection if the switch requests are terminated.

If local protection switching requests that have been active previously now have 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.

13 Failure detection

Link faults are detected via the server layer's SSF detection and the T-MPLS Section signal failure (SF) condition via CVv1 OAM. T-MPLS section OAM mechanisms are defined in Recommendation G.8114/Y.1373.

14 Traffic types

14.1 Bandwidth sharing

The bandwidth on each ring is shared so that part of ring capacity is guaranteed for the normal traffic and part is used for the protection traffic in case of failure on the ring. The protection part of the ring bandwidth rotating in one direction is used to carry the normal traffic from the ring rotating in other direction in case of failure. Part of ring bandwidth can also be dedicated to carry unprotected non-preemptable traffic.

14.2 Bandwidth and QoS considerations

The TM-SPRing protection mechanism provides for the connectivity restoration of the normal traffic affected by a ring failure. The protection mechanism itself does not distinguish between different types of QoS associated with the given connections. It is also not aware of the bandwidth allocated or guaranteed for the protected or unprotected connections.

In the T-MPLS ring, in order to guarantee the bandwidth and QoS of the connections, normal or unprotected, traffic management and engineering measures should be taken. For example, the bandwidth and QoS parameters allocated for each protection connection can be equal to the bandwidth and QoS parameters of the associated working connection.

NOTE – bandwidth and QoS parameters calculation and allocation for the normal and protection connections is out of scope of this Recommendation.

14.3 Point-to-point and point-to-multipoint traffic

Both point-to-point and drop-and-continue point-to-multipoint T-MPLS connections can be protected by TM-SPRing.

The APS protocol functionality as well as the node's reaction on different protection switching requests in case of ring failure is identical for p-t-p and p-t-mp traffic.

An example of p-t-mp traffic protection by wrapping is provided in Appendix I.3.

15 Automatic Protection Switching (APS) protocol

The TM-SPRing protection operation is controlled with the help of the T-MPLS Section OAM APS protocol. The APS processes in the individual nodes communicate by using T-MPLS section APS messages.

The APS protocol is intended to carry the ring status information and APS requests, both automatic and externally generated commands, between the ring nodes.

Each node on the ring shall be identified uniquely by assigning it a node ID. The maximum number of nodes on the ring supported by the APS protocol is 127. The node ID is independent of the order in which the nodes appear on the ring. The node ID is used to identity the source and destination nodes of each APS message.

Each node has a ring map maintained by a management application. The ring map contains information about the sequence of the nodes around the ring. The method of configuring the nodes with the ring maps is out of scope of this recommendation.

When no protection switches are active on the ring, each node dispatches periodically T-MPLS section OAM APS PDUs to the two adjacent nodes, indicating no switch request. When a node determines that a protection switching is required (see clause 17), it sends the appropriate bridge requests in both directions, i.e. West and East. See sub-clause 15.3 for a detailed description of the APS protocol operation.

'Destination node' is a node that is adjacent to a node that identified a failed span. When a node that is not the destination node receives a bridge request and it has no higher priority local request (see clause 19), it transfers the APS information as received. In this way, the switching nodes can maintain direct APS protocol communication on the ring.

Note that in the case of a bidirectional failure such as a cable cut, two nodes would detect the failure and send each other a bridge request in opposite directions.

- In rings utilizing the *wrapping protection*, when the destination node receives the bridge request, it performs the bridge & switch from/to the working connections to/from the protection connection.
- In rings utilizing the *steering protection*, when a ring switch is required, any node shall execute bridges and switches if its added/dropped traffic is affected by the failure. Determination of the affected traffic is performed by examining the APS bridge requests (indicating the nodes adjacent to the failure or failures) and the stored ring maps (indicating the relative position of the failure and the added traffic destined towards that failure).

NOTE – Steering is for further study.

When the failure has cleared and the WTR timer has expired, the nodes sourcing bridge requests will drop their respective bridge requests (tail end) and will source a bridge request carrying No Request code. The node receiving such a bridge request (head end) will drop its bridge & switch.

A switch shall be initiated by one of the criteria specified in clause 19. A failure of the APS protocol or controller shall not trigger a protection switch.

Ring switches can be preempted by higher priority bridge requests as defined in clause 19. For example, consider a ring switch that is active due to a manual switch request on the given span, and another ring switch is required due to a failure on another span. Then a ring bridge request will be generated, the former ring switch will be dropped, and the latter ring switch established.

Multiple ring switches can exist in the ring, resulting in the ring being segmenting into two or more separate segments. This may happen when several bridge requests of the same priority exist in the ring due to multiple failures or external switch commands.

Proper operation of the ring relies on all nodes having knowledge of the state of the ring (nodes and spans) so that nodes do not preempt a request unless they have a higher-priority request. In order to accommodate this ring state knowledge, during a bridge request the APS protocol shall be sent in both directions.

15.1 APS payload structure

The APS-specific information is transmitted within specific fields in the APS OAM PDU structure defined in ITU-T Recommendation G.8114. In this version of the Recommendation 4 octets in the APS PDU are used to carry APS-specific information. Note that in this version of the Recommendation, the TLV offset field has to be set to 0x04.

The structure and field values for the four APS data octets are defined in Table 15-1.

Table 15-1/G.8132 – TM-SPRing APS protocol payload structure

1								2								3								4							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
Destination node ID								Source node ID								Bridge request								Reserved							

Destination Node ID: The destination node ID is set to the value of the node ID for which the APS request is destined. The destination node ID is always that of an adjacent node (except for the default APS PDU, see Clause 15.3). Valid destination node ID values are 1-127.

Source node ID: The source node ID is set to the value of the node ID of the node generating the APS request. Valid source node ID values are 1-127.

Bridge Request code: A code consisting of four bits carrying the bridge request message from a tail-end node to the head-end node requesting the head-end to perform a bridge of the normal traffic signals. Bridge request codes are specified in Table 15-2 below.

Table 15-2/G.8132 – TM-SPRing APS protocol bridge request codes

Bits 4-1 (MSB … LSB)	Condition, State or external Request	Order of priority
1 1 1 1	Lockout of Protection (LP)	highest
1 1 0 1	Forced Switch (FS)	↑
1 0 1 1	Signal Fail (SF)	
0 1 1 0	Manual Switch (MS)	
0 1 0 1	Wait-To-Restore (WTR)	
0 0 1 1	Exerciser (EXER)	
0 0 0 1	Reverse Request (RR)	↓
0 0 0 0	No Request NR	lowest

15.2 APS protocol type

The protocol type for the TM-SPRing is a 1-phase protocol.

Support of acknowledgement mechanism by the 1-phase APS protocol by means of Reverse Request code is described in clause 15.3.1/G.8132. This should be considered as the means of verification of proper operation of the APS protocol (e.g., alarm can be sent to management), but should not affect the protection switching operation.

15.3 APS protocol operation

This subclause defines the rules to apply to each node participating in a single TM-SPRing algorithm instance. The operations described hereafter are assumed to be performed by an APS controller. Each node of the ring contains an APS controller. Its purpose is to handle the input parameters and provide output actions consistent with the rules described. Figure 15-1 illustrates the conceptual operation of a TM shared protection ring APS controller.

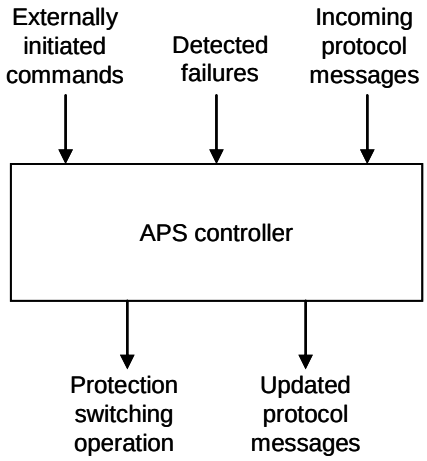


Figure 15-1/G.8132 – Conceptual TM Shared Protection Ring APS controller

The following general rule applies:

Rule G #1 – BRIDGE REQUEST VALIDATION

Rule G #1a: The information contained in APS PDU, 3rd byte shall be considered as a bridge request if:

– the 3rd byte bits indicate one of the bridge request codes.

15.3.1 Ring node APS state

There are three classes of ring node states: the idle state, the switching state, and the pass-through state.

15.3.1.1 Idle state

A node is in the idle state when it is sourcing and receiving NR code to/from both directions.

Rule I #1 – IDLE STATE SOURCED APS PDU:

Rule I #1a: Any node in the idle state shall source the APS PDU bytes in both directions as given in Table 15-3.

Table 15-3/G.8132 – APS PDU bytes' values sourced in the idle state

1st byte	=	Destination node ID
2nd byte	=	Source node ID
3rd byte	=	all 0 (NR)

Until the node has knowledge of the ring map, it shall behave as per Rule I-S #3.

NOTE – Signaling in the start-up state is for further study.

Rule I #2 – IDLE STATE RECEIVED APS PDU: Any node in the idle state shall terminate APS PDU flow in both directions.

15.3.1.2 Switching state

A node not in the idle or pass-through states is in the switching state. This includes the default signaling status, e.g. node start-up, where there is no ring map available.

Rule S #1 – SWITCHING STATE SOURCED APS PDU:

Rule S #1a: Any node in the switching state shall source APS PDU bytes as shown in Table 15-4:

Table 15-4/G.8132 – APS PDU bytes' values sourced by a node in the switching state

1st byte	=	Destination node ID
2nd byte	=	Source node ID
3rd byte	=	Bridge Request

Rule S #1b – SINGLE BRIDGE REQUEST AT A NODE: Any node in the switching state, shall source a bridge request in both directions. Exceptions to this can occur when there are more than one switch requests active at a node.

Rule S #1c - MULTIPLE BRIDGE REQUESTS AT A NODE: Whenever a node in the switching state terminates a new short-path bridge request from an adjacent node, of equal or higher priority than the bridge request it is currently executing, over the same span, it shall source a bridge request of the same priority on the corresponding long path. Whenever a node receives bridge requests on both short paths from its adjacent nodes, the long-path bridge request shall be signaled rather than the short-path reverse requests [See Figure 15-2 a]. This rule takes precedence over Rule S #1b in case of multiple bridge requests at the same node.

Rule S #1d - MULTIPLE BRIDGE REQUESTS AT A NODE: Whenever a node detects a local condition requiring a ring switch or an externally initiated command for a ring switch applied at that node, it shall always source over the short path a short-path ring bridge request as long as the ring bridge request is not pre-empted by a higher priority bridge request [See Figure 15-2 b]. This rule takes precedence over Rule S #1c. Note that whenever a node receives in one direction a short-path ring bridge request on one side and detects Signal Fail or an externally initiated command on the other side, it shall signal the bridge request associated with that condition [see Figure 15-2 c)].

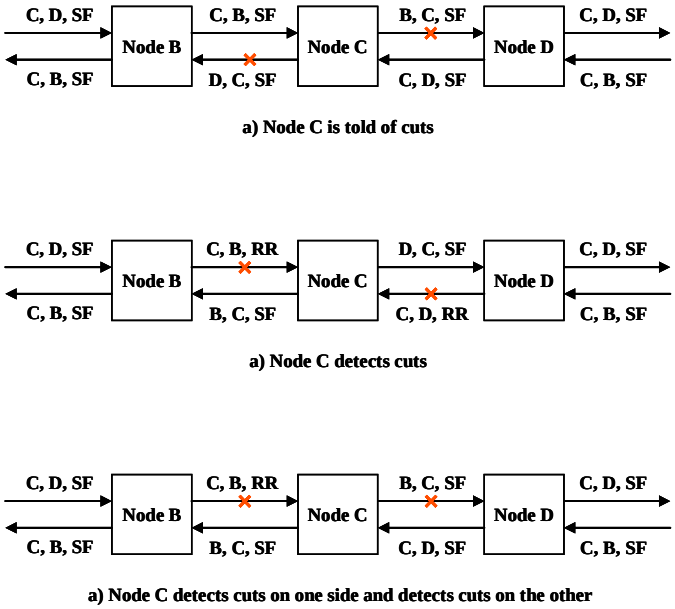


Figure 15-2/G.8132 – APS signaling in isolated node condition

Rule S #2 – SWITCHING STATE RECEIVED APS PDU: Any node in the switching state shall terminate APS PDU flow in both directions.

Rule S #3 – UNIDIRECTIONAL BRIDGE REQUEST ACKNOWLEDGMENT: As soon as it receives a bridge request from the short path, the node to which it is addressed shall acknowledge the bridge request by replying with the Reverse Request code on the short path, and with the received bridge request priority on the long path.

NOTE – This rule refers to the unidirectional failure detection: the reverse request should be issued only when the node does not detect the failure condition (i.e., head end), that is, it is not applicable when a failure is detected bidirectionally, because, in this latter case, both nodes send a bridge request for the failure on both paths (short and long).

Rule S #4 – ALLOWED COEXISTING PROTECTION SWITCHES:

Rule S #4a: The following switches are allowed to coexist:

– LP with LP;

– FS with FS (ring split into multiple subrings);

– SF with SF (ring split into multiple subrings);

– FS with SF (ring split into multiple subrings).

Rule S #4b: When multiple MS bridge requests over different spans exist at the same time, no bridge or switch shall be executed and existing switches and bridges shall be dropped. The nodes shall signal, anyway, the MS ring bridge request in APS PDU bytes. Multiple EXER bridge request can coexist in the ring.

Rule S #5 – LOSS OF RING BRIDGE REQUEST: If a node executing a ring bridge and switch receives invalid APS request it shall ignore it and keep bridge and switch on. If a node no longer receives a valid ring bridge request on the long path for a period of more than 3 times the normal APS period, it shall drop its ring bridge and switch, and shall signal and act based on its highest priority input.

Rule S #8 – WTR TERMINATION: Whenever a node in the WTR state drops its bridge and switch before the WTR timer expires, it shall immediately terminate the WTR and act based on its highest priority input.

Rule S #9 – A node in a ring switching state that receives the external command LW for the affected span shall drop its bridge and switch and shall signal NR for the locked span if there is no other request on another span. Node still may signal relevant bridge request for another span.

15.3.1.3 Pass-through state

A node is in the pass-through state when its highest priority APS request is a bridge request not destined to or sourced by it. The pass-through is bidirectional.

Rule P #1 – PASS-THROUGH STATE SOURCED AND RECEIVED APS PDU BYTES: When a node is in pass-through, it transmits on one side, the same APS request as it receives from the other side.

15.3.2 Ring node APS state transition rules

Subclause 15.3.1 described the three ring node states. This subclause describes the transition rules among these different states.

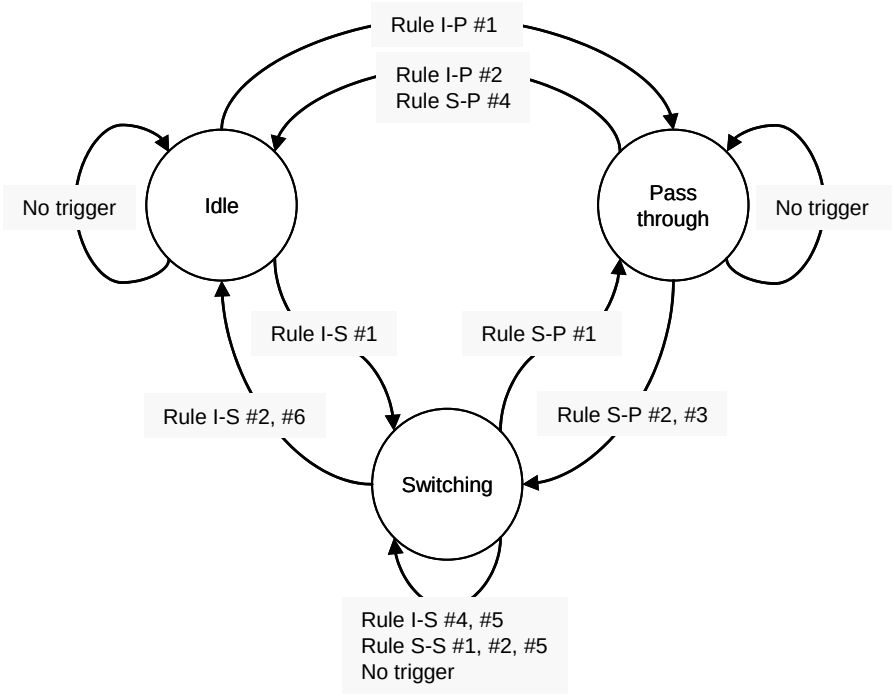


Figure -15-3/G.8132 – APS state machine for a single node

The following basic rules apply:

Rule Basic #1 – STATE TRANSITION TRIGGERS: All state transitions are triggered by an incoming APS request change, a WTR expiration, an externally initiated command, or locally detected T-MPLS section failure conditions.

Rule Basic #4 – APS requests due to a locally detected failure, an externally initiated command, or received APS request shall pre-empt APS requests in the prioritized order given in Table 15-2/G.8132, unless the bridge requests are allowed to coexist.

15.3.2.1 Transitions between the idle and pass-through states

Rule I-P #1 – TRANSITION FROM THE IDLE STATE TO THE PASS-THROUGH STATE:

Rule I-P #1a: The transition from the idle state to pass-through state shall be triggered by a valid APS request change, in any direction, from the No Request code to any other bridge request code, as long as the new bridge request is not destined for the node itself. Both directions move then into pass-through, so that, traffic entering the node through the protection connections are by-passed across the node.

Rule I-P #2 – TRANSITION FROM THE PASS-THROUGH STATE TO THE IDLE STATE: A node shall revert from any pass-through state to the idle state when it detects No Request codes in the incoming APS PDU from both directions. Both directions revert simultaneously from the pass-through state to the idle state.

15.3.2.2 Transitions between the idle and switching states

Rule I-S #1 – TRANSITION FROM THE IDLE STATE TO THE SWITCHING STATE:

Rule I-S #1a: Transition of an NE from the idle state to the switching state shall be triggered by one of the following conditions:

– a valid APS request change from the No Request (NR) code to any ring bridge request code received on either the long path or the short path and destined to that NE;

– an externally initiated command for that NE;

– the detection of a T-MPLS section layer failure at that NE.

Rule I-S #1b: Actions taken at a switching NE upon receiving a valid bridge request are:

– for FS bridge requests, the node shall check if there is any need for connections' squelching and in affirmative case, shall not perform bridge and switch, otherwise, it shall execute the bridge and switch;

– for SF bridge requests, the node shall check if there is any need for squelching and in affirmative case, shall not perform bridge and switch; otherwise, it shall, execute a bridge and switch;

– for all other bridge requests, except EXER and LP, the node shall execute a bridge and switch;

– for EXER, and LP, the node shall signal appropriate bridge request, but shall not execute the bridge or switch.

Rule I-S #2 – TRANSITION FROM THE SWITCHING STATE TO THE IDLE STATE: A node shall revert from the switching state to the idle state when it detects NR codes in APS PDU from both directions.

– At the tail end: When a WTR time expires or an externally initiated command is cleared at a node, the node shall drop its bridge and switch, shall transition to Idle state and signal the No Request code in APS PDU in both directions.

– At the head end: Upon reception of the No Request code, from both directions, the head-end node shall drop its bridge and its switch, shall transition to Idle state and signal the No Request code in both directions.

Rule I-S #3 – A node shall transmit the default APS code as shown in the Table 15-5/G.8132, until it is capable of proper APS signaling. The default APS code shall be used to indicate that the node can not properly signal APS PDU, and therefore cannot properly execute protection switching. The default APS code sourced by a node must have the Destination node ID equal to the Source node ID:

Table 15-5/G.8132 – default APS code structure

1st byte	=	Destination node ID = Self node ID
2nd byte	=	Source node ID= Self node ID
3rd byte	=	*NR for transmission* *Don't care for receiving*

Rule I-S #4 – A switching node receiving default APS code from any direction shall drop its bridge and switch and signal NR code in both directions.

Rule I-S #6 – If a switching node receives from any direction the APS bytes that it is sourcing, and receives no other APS request, it shall transition to the idle state. Otherwise, the switching node shall signal according to its highest priority input.

15.3.2.3 Transitions between switching states

The following transition rules apply:

Rule S-S #1 – TRANSITION FROM THE SWITCHING STATE TO THE SWITCHING STATE:

Rule S-S #1a: When an NE that is currently executing an SF switch receives another SF or FS bridge request not destined to that NE, the NE shall check if there is any need for squelching and squelch accordingly. The NE shall stop squelching when the isolation condition, affecting the node's adding/dropping T-MPLS connections is removed.

Rule S-S #1b: When an NE that is currently executing an FS switch receives another FS or SF bridge request not destined to that NE, the NE shall check if there is any need for squelching and squelch accordingly. The NE shall stop squelching when the isolation condition, affecting the node's adding/dropping T-MPLS connections is removed.

Rule S-S #1c: When an NE that is currently executing any ring switch receives a higher priority ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for the same span, it shall upgrade the priority of the ring switch it is executing to the priority of the received ring bridge request.

Editors' note: Rule S-S #2 seems to be irrelevant for 2 fiber ring and needs to be removed.

Rule S-S #3 – RING SWITCH CLEARING:

Rule S-S #3a: When a failure condition clears at a node, the node shall enter Wait-To-Restore and remain in Wait-To-Restore for the appropriate time-out interval, unless:

1) a different bridge request of higher priority than WTR is received; or
2) another failure is detected; or
3) an externally initiated command becomes active.

The node shall send out a WTR code on both the long and short paths.

Rule S-S #3b: When a node that is executing a switch in response to an incoming, SF bridge request (not due to a locally detected failure) receives a Wait-To-Restore code (unidirectional failure case), it shall send out RR code on the short path and the WTR on the long path.

Rule S-S #5 – A switching node that receives ring bridge requests destined to itself from both of its neighbors shall drop its bridge and switch.

Editor's note: this rule should be clarified.

15.3.2.4 Transitions between switching and pass-through states

Rule S-P #1 – SWITCH PRE-EMPTION RULES (Switching State to Pass-Through State):

Rule S-P #1e: When a node that is currently executing a ring switch receives a ring bridge request for a non-adjacent span of higher priority than the ring switch it is executing, it shall drop its bridge and switch immediately, then the node shall enter the pass-through state.

Editors' note: the rule1f was removed as it seems to be redundant to the 1e rule.

Rule S-P #2 – PASS-THROUGH TO SWITCHING TRANSITIONS:

Rule S-P #2a: The transition of a node from pass-through to switching shall be triggered by:

1) an equal, higher priority, or allowed coexisting externally initiated command;
2) the detection of an equal, higher priority, or allowed coexisting failure;
3) the receipt of an equal, higher priority, or allowed coexisting bridge request destined to that NE;

Rule S-P #3 – If a node that was in the pass-through state due to a SF or FS request on the ring, and the node is now sourcing a SF or FS bridge request (due to Rule S-P #2a), the node shall:

– determine if there is any need for squelching and in affirmative case, do not perform bridge and switch on T-MPLS connections destined to the isolated node(s);
– otherwise, it shall execute bridge and switch.

Rule S-P #4 – If a pass-through node receives from at least one direction an APS request that has itself as the source ID, it shall transition to Idle state and source No Request code in both directions.

Editor's note: consider moving this rule to Pass-through to Idle switching section.

16 Transmission and acceptance of APS signals

APS signals in the ring are transported over the ring in West and East directions, between the bridging (head end) and switching (tail end) nodes.

A new APS signal must be transmitted immediately when a change in the transmitted status occurs.

The first three APS signals should be transmitted as fast as possible so that fast protection switching is possible even if one or two APS signals are lost or corrupted. For fast protection switching within 50 ms, the interval of the first three APS signals is should be 3.3 ms. APS signals after the first three should be transmitted with the interval of 5 seconds.

17 Misconnection avoidance

The reason for possible misconnection when protection switching is activated due to a node failure or double fault in the ring is caused by the fact that the same protection connection is shared for restoration of different working connections.

The T-MPLS network characteristics (large number of available labels and the fact that labels are not associated with a fixed bandwidth) allow each normal connection in the ring to be protected by a dedicated protection connection.

In order to avoid possible misconnection, each protection connection must be uniquely associated with one and only one normal connection.

- For each normal connection, the dedicated protection connection in opposite direction is created and association between working and protection labels is defined at each node for each span.

17.1 Ring map and squelch table information

Each node on a ring shall maintain a ring map describing the ring connectivity, and a local squelch table indicating the source and destination of all added, dropped, and pass-through connections.

17.2 Squelching

The term “squelching” is inherited from the SDH application and is used in this context just to point to the equivalent action aimed to disable the ring switch in case of node(s) isolation. In TM-SPRing misconnections are implicitly avoided by connection label assignment. The only purpose of “squelching” in TM-SPRing is to avoid the occupation of protection bandwidth, in case of node(s) isolation.

T-MPLS connection squelching shall be performed at the switching nodes by NOT performing bridge and switch on the interested connections. When the source node is isolated it is also required to insert FDI packets towards access ring side (drop direction).

The switching node shall, by comparing node identifiers contained in crossing APS PDUs with the information contained in the ring map, identify which nodes are isolated. From this information and the squelch table, it shall identify which connections are added and dropped at these nodes and shall squelch them.

18 Label assignment

In the T-MPLS Shared Protection Ring no restrictions are applied to the labels allocation along the normal and protection connections (besides T-MPLS per platform and per interface label space requirements as described in appendix III/G.8110.1). However, at every node there must be a deterministic relation between the labels assigned for normal and protection connection in both West and East directions.

The T-MPLS connections are provisioned at every node that adds, drops or forwards the associated traffic through the TMP connection function which performs label swapping according to the configuration.

For each normal connection, the protection connection is established through the TMP connection function in the opposite direction forming a closed loop though all nodes in the ring. Labels assigned for the protection connection can be swapped at every node by the TMP connection function and the association with the working labels must be defined at every node in the ring in West and East directions.

19 Protection switching trigger mechanism

Protection switching action shall be conducted when:

1) they are initiated by operator control (e.g., manual switch, forced switch, and lockout of protection) without a higher priority switch request being in effect on addressed span or entire ring;
2) a T-MPLS Section SF is declared on the associated span and without a higher priority switch request (e.g., lockout of protection, forced switch) being in effect on addressed span or entire ring and the hold-off timer has expired; or
3) the wait to restore timer expires .

19.1 Manual control

Manual control of the protection switching function may be transferred from the network element to the network element by APS signal or applied to the network element by the network management system.

19.2 Signal fail declaration conditions

A T-MPLS Section Signal Fail (SF) is declared when the T-MPLS Section trail termination (TMS_TT_Sk) function detects a trail signal fail as defined in G.8121.

20 APS Switch initiation criteria

20.1 Manual control

Externally initiated commands are entered by the operator through the Network Management System (NMS) or the Craft interface. The externally initiated command may be transmitted to the appropriate node via the T-MPLS ring APS protocol.

20.1.1 Commands not signaled on the APS protocol

The following commands are not transferred by the APS PDU.

Clear: This command clears the externally initiated command and wait-to-restore timer (WTR) at the node to which the command was addressed. The node-to-node signaling following removal of the externally initiated commands is performed using the no-request code (NR).

Lockout of Working: This command prevents the normal traffic transported over the addressed span from being switched to the protection entity by disabling the node's capability of requesting the bridge for this span in case of failure. If any normal traffic is already bridged on the protection entity, the bridge is dropped. If no other bridge requests are active on the ring, the no-request code (NR**)** is transmitted. This command has no impact on any other span. If the node receives the bridge request from the adjacent node from any side it will perform the requested bridge. If the node receives the bridge request addressed to the other node in will go to the pass-through state.

20.1.2 Commands using the APS protocol

The following commands are transferred by the APS PDU:

Lockout of Protection (LP): This command prevents any protection activity and prevents using ring switches anywhere in the ring. If any ring switches exist in the ring, this command causes the switches to drop.

Forced Switch to protection (FS): This command performs the ring switch of normal traffic from the working entity to the protection entity for the span between the node at which the command is initiated and the adjacent node to which the command is directed. This switch occurs regardless of the state of the T-MPLS section for the requested span, unless it is satisfying a higher priority bridge request.

Manual Switch to protection (MS): This command performs the ring switch of the normal traffic from the working entity to the protection entity for the span between the node at which the command is initiated and the adjacent node to which the command is directed. This occurs if the T-MPLS section for the requested span is not satisfying an equal or higher priority bridge request.

Exercise - Ring (EXER): This command exercises ring protection switching on the addressed span without completing the actual bridge and switch. The command is issued and the responses (RR) are checked, but no normal traffic is affected.

20.2 Automatically initiated commands

Automatically initiated commands can be initiated based on T-MPLS section layer and equipment performance criteria and received bridge requests.

The node initiates the following bridge requests automatically:

Signal Fail (SF): This command is issued when the T-MPLS section detects signal failure condition. T-MPLS section SF condition is defined as presence of TSF generated by TM_TT_Sk T-MPLS trail termination function. The tail-end detects the failure and generates the bridge request.

Wait-To-Restore (WTR): This command is issued when T-MPLS section detects that the SF condition has cleared. It is used to maintain the state during the WTR period unless it is pre-empted by a higher priority bridge request. The Wait to Restore time may be configured by the operator in 1 minute steps between 0 and 12 minutes; the default value is 5 minutes.

Reverse Request (RR): This command is transmitted to the tail-end NE over the short path as an acknowledgment for receiving the ring bridge request.

Appendix I

Wrapping and Steering examples

I.1 Wrapping

Figure I-1 illustrates T-MPLS signal flow in normal and failure condition in the TM-SPRing utilizing the T-MPLS packet wrapping protection mechanism.

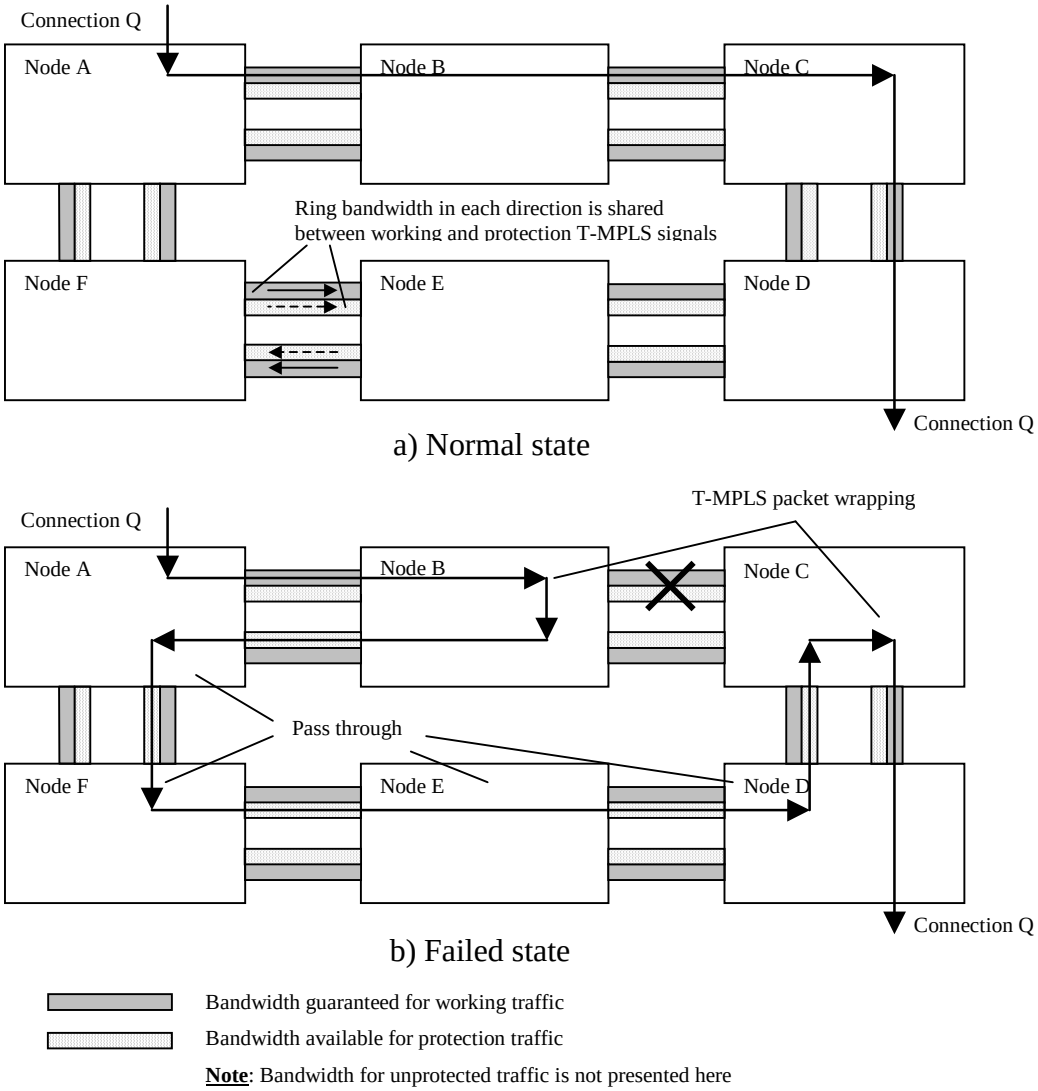


Figure I-1/G.8132 – T-MPLS shared protection ring – wrapping

Figures I-2 to I-5 illustrate the Working, Protection, NUT and APS signals connections for TMSP2fsh_C function (see G.8121), in normal operation and in a ring failure condition for the node not adjacent to the failure and node detected the failure on west or east side. Ring switch is triggered by the SF condition (relayed via CI_SSF TMS signal), the external commands and the information relayed via the APS PDU.

The West [East] NUT B connection points are always connected to the associated West [East] NUT A connection points.

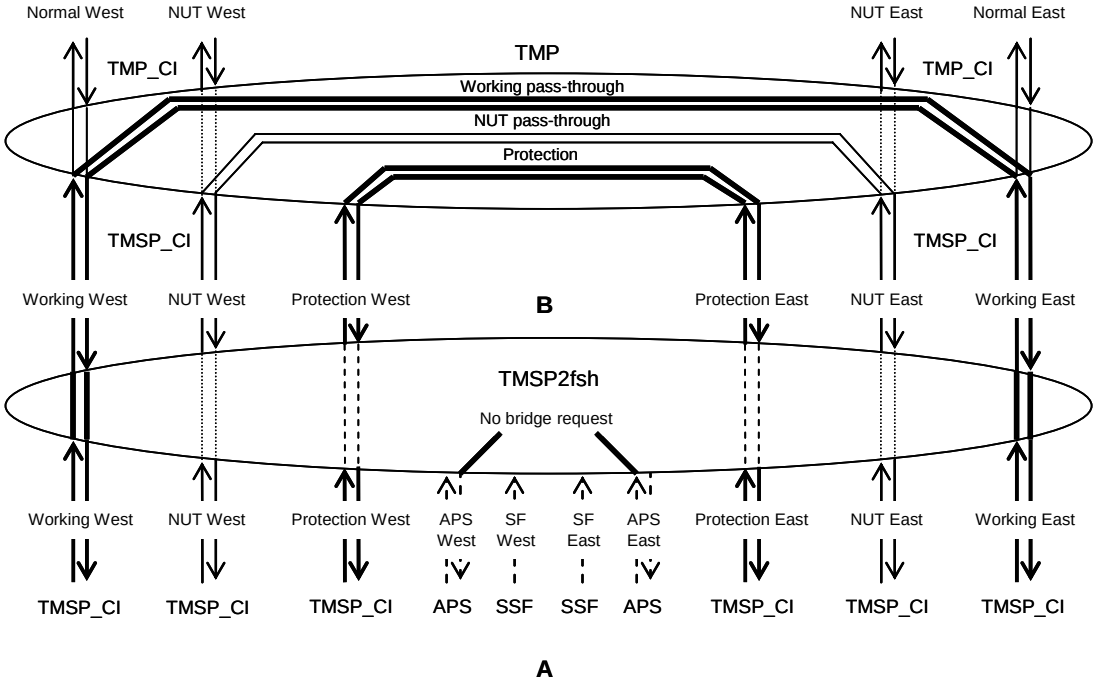


Figure I-2/G.8132 – Connection in the node without ring failures

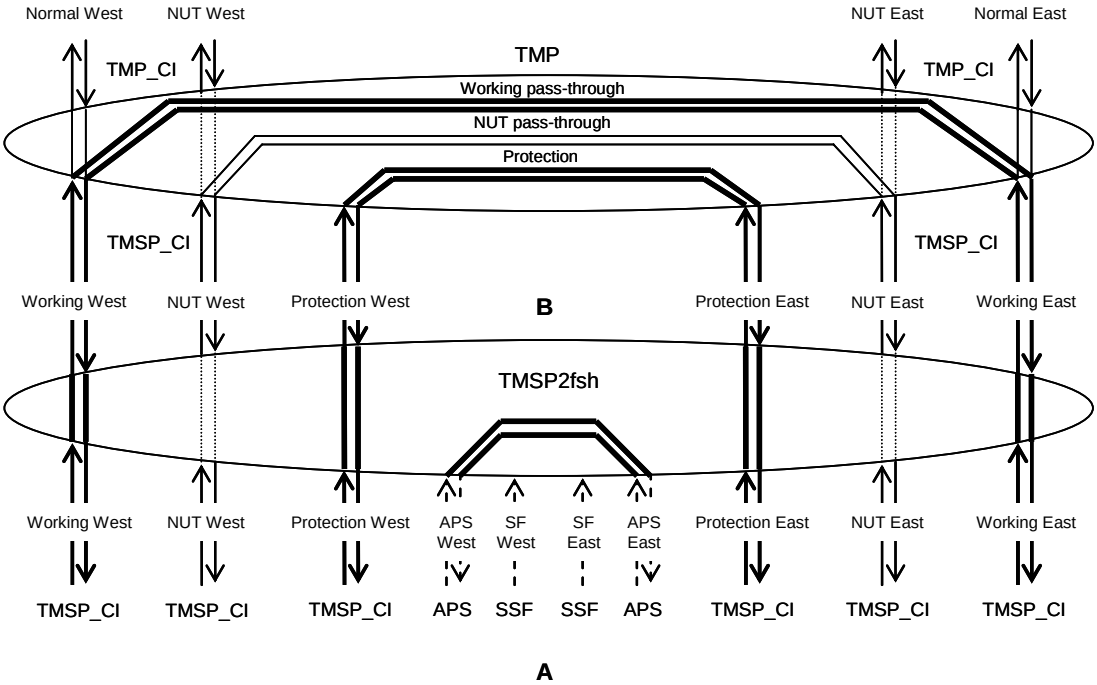


Figure I-3/G.8132 – Connections in the node not adjacent to the fault

Figures I-4 and I-5 illustrate the matrix configuration in case of failure. Solid lines represent the connections allowing the labels to be swapped by TMP_C matrix.

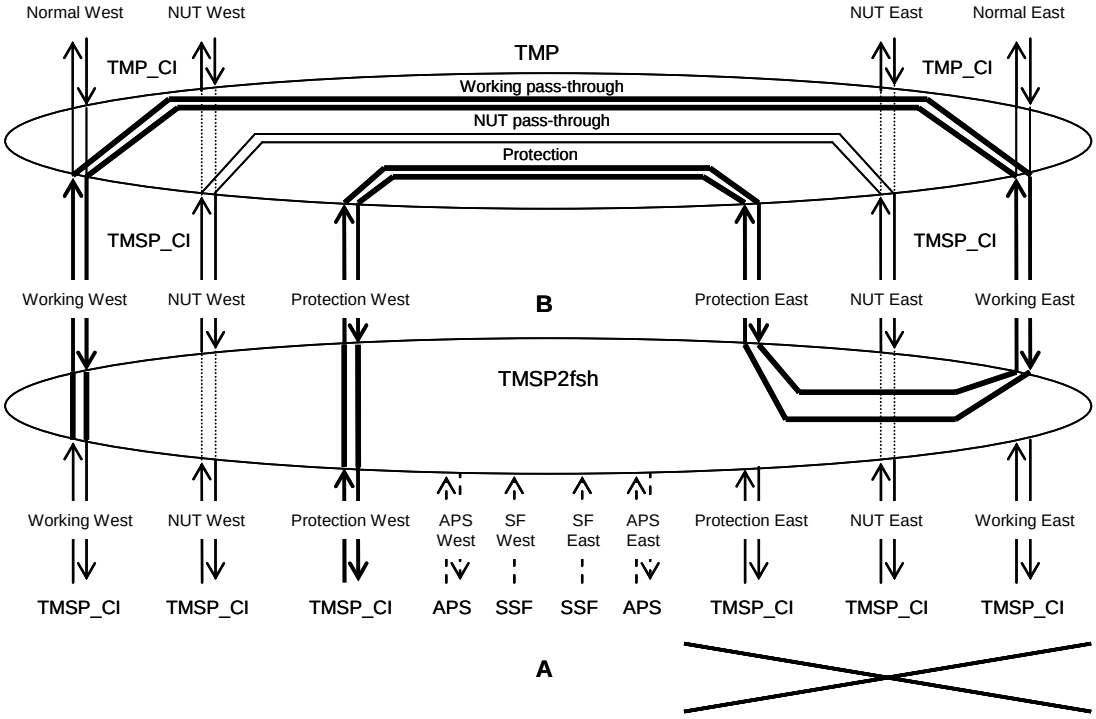


Figure I-4/G.8132 – Connections in the node adjacent to the fault on its East side

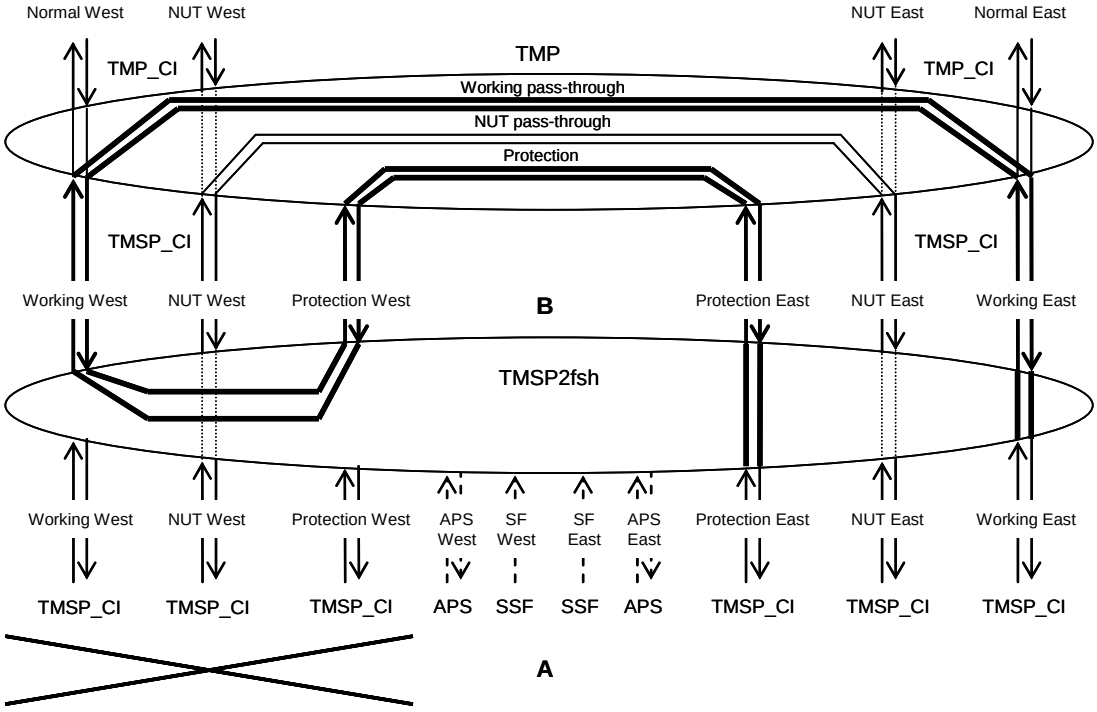


Figure I-5/G.8132 – Connections in the node adjacent to the fault on its West side

I.2 Steering

Figure I-6 illustrates T-MPLS signal flow in normal and failure condition in the TM-SPRing utilizing the T-MPLS packet steering protection mechanism.

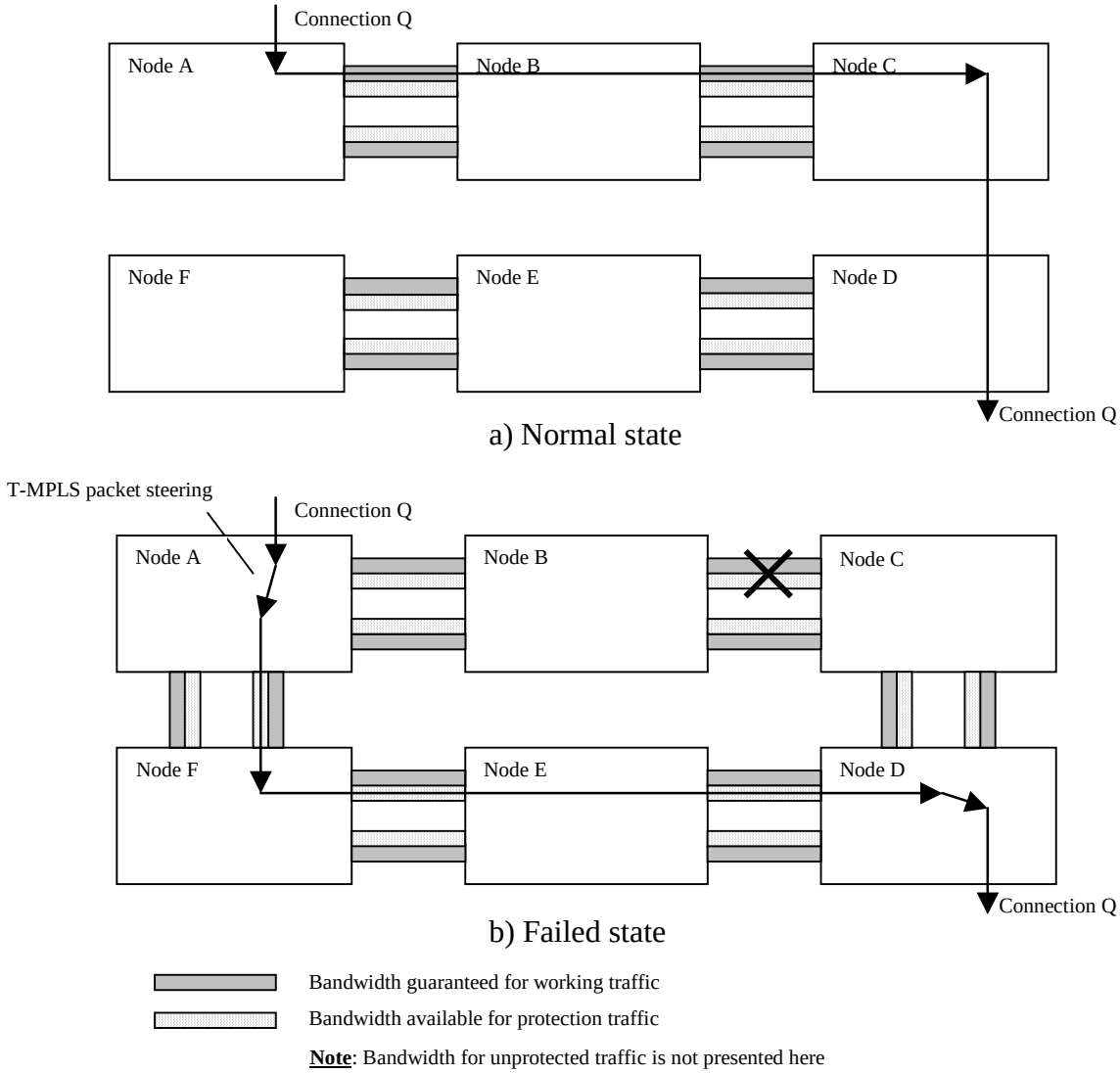


Figure I-6/G.8132 – T-MPLS shared protection ring – steering

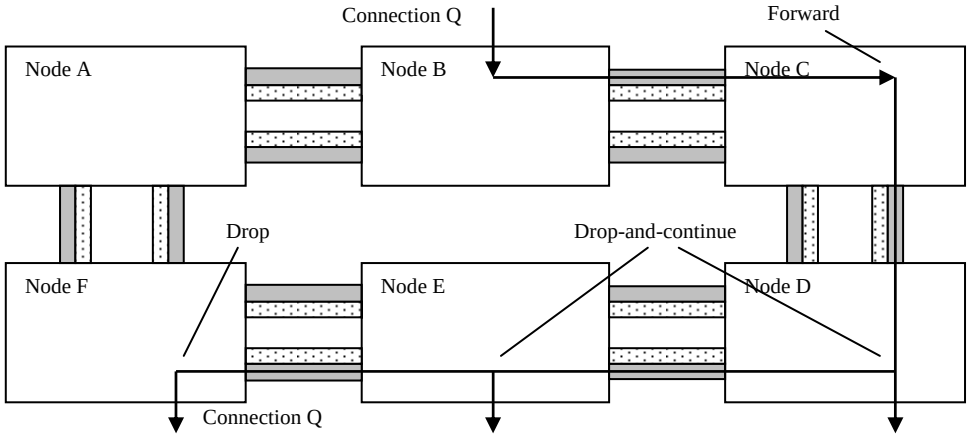
NOTE – Steering is for further study.

I.3 Wrapping protection for the p-t-mp connection example

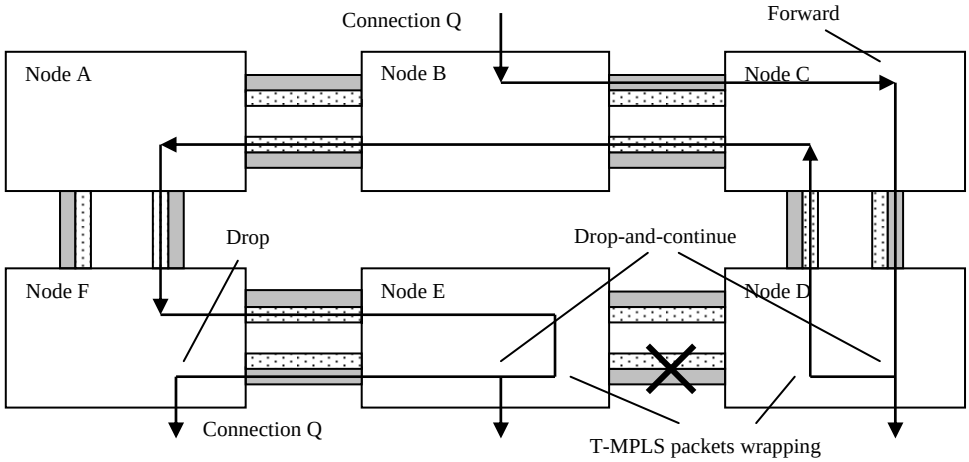
Figure I-7 illustrates the wrapping protection switching for multicast traffic in the ring. In this example Node B is the source node for the multicast connection Q. This connection is targeted to the Nodes D, E and F. Node C is configured to “forward”, Nodes D and E to “drop-and-continue” and Node F to “drop” operations.

In this example a failure occurs between the nodes D and E. As can be seen in the Figure I-7, the traffic will be restored at every node by wrapping protection operation just as it is done for p-t-p traffic (See Figure I-1).

APS protocol functionality as well as nodes reaction on different protection switching requests in case of ring failure for the T-MPLS shared protection rings will be identical for p-t-p and p-t-mp connections.



a) Normal state



b) Failed state

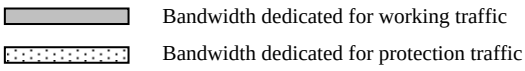


Figure I-7/G.8132 – T-MPLS shared protection ring – wrapping protection operation in case of p-t-mp connection

Appendix II

State transition tables

II.1 Reference scenarios

Figure II-1 represents the scenario when the Node n entered the initial state due to the local request on one side of the node and receives another local request from the same side. The Table II-1 summarizes the state transitions in this scenario.

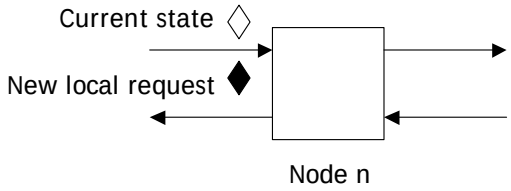


Figure II-1/G.8132 – Local request on the same side of the node

Figure II-2 represents the scenario when the Node n entered the initial state due to the local request on one side of the node and receives remote request. The Table II-2 summarizes the state transitions in this scenario.

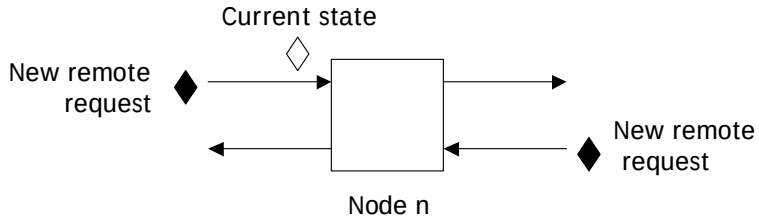


Figure II-2/G.8132 – Remote request addressed to the same node

Figure II-3 represents the scenario when the Node n entered the initial state due to the local request on one side of the node and receives remote request addressed to the other node. The Table II-3 summarizes the state transitions in this scenario.

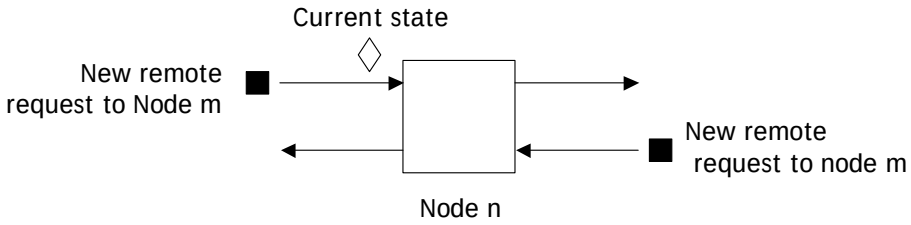


Figure II-3/G.8132 – Remote request addressed to the other node

II.2 Transition tables

Table II-1/G.8132 – State transitions for the node found in the switching state receiving another local request on the same span

State ◊ (caused by the local request)		Signaled APS	Another local request addressed to the same span ♦								
			a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
			LP [a]	**LW** [b]	**FS**	**SF**	**Recover from SF**	**MS**	**Clear**	**WTR expires**	**EXER**
A	Idle Working: no switch Protection: no switch	NR	→ C	→ D	→ E	→ F	N/A	→ G	N/A	N/A	→ I
B	Pass-trough Working: no switch Protection: pass through	N/A	→ C	→ B	O → E [c]	O → F [c]	N/A	O → G [c]	N/A	N/A	O
C	Switching – LP Working: no switch Protection: no switch	LP	N/A	O	O	O	N/A	O	→ A → F → B	N/A	O
D	Idle – LW Working: no switch Protection: no switch	NR	→ C	N/A	O	O	N/A	O	→ A → F	N/A	O
E	Switching – FS Working: switched Protection: switched	FS	→ C	→ D	N/A	O	N/A	O	→ A → F → B	N/A	O
F	Switching – SF Working: switched Protection: switched	SF	→ C	→ D	→ E	N/A	→ H	O	N/A	N/A	O
G	Switching – MS Working: switched Protection: switched	MS	→ C	→ D	→ E	→ F	N/A	N/A	→ A	N/A	O
H	Switching – WTR Working: switched Protection: switched	WTR	→ C	→ D	→ E	→ F	N/A	→ G	→ A	→ A	O
I	Switching – EXER Working: no switch Protection: no switch	EXER	→ C	→ D	→ E	→ F	N/A	→ G	→ A	N/A	N/A

NOTE 1 – "N/A" means that the event cannot happen for the State.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.

[a] During local LP command switches will be dropped.

[b] Relevant for the side of the node where the LW command is applied.

[c] The node will move to the new state only if local request has higher priority or requests are allowed to coexist.

Table II-2/G.8132 – State transitions for the node found in the switching state receiving remote request

State ◊ (caused by the local request)		Signaled APS [a]	Remote request addressed to this node ♦							
			a	**b**	**c**	**d**	**e**	**f**	**g**	**h**
			LP [b]	**FS**	**SF**	**MS**	**WTR**	**EXER**	**RR**	**NR**
A	Idle Working: no switch Protection: no switch	NR	→ C	→ E	→ F	→ G	N/A	→ I	N/A	(→ A)
B	Pass-trough Working: no switch Protection pass through	N/A	→ C	N/A [b] → E	N/A [b] → F	N/A [b] → G	N/A	N/A [b] → I	N/A	→ A
C	Switching – LP Working: no switch Protection: no switch	LP	(→ C)	O	O	O	N/A	O	(→ C)	N/A
D	Idle – LW Working: no switch Protection: no switch	NR	→ C	→ E	→ F	→ G	N/A	→ I	N/A	(→ D)
E	Switching – FS Working: switched Protection: switched	FS	→ C	(→ E)	(→ E)	O	N/A	O	(→ E)	N/A
F	Switching – SF Working: switched Protection: switched	SF	→ C	(→ F)	(→ F)	O	N/A	O	(→ F)	N/A
G	Switching – MS Working: switched Protection: switched	MS	→ C	→ E	→ F	(→ G) [c]	N/A	O	(→ G)	N/A
H	Switching – WTR Working: switched Protection: switched	WTR	→ C	→ E	→ F	→ G	(→ H)	O	(→ H)	→ A
I	Switching – EXER Working: no switch Protection: no switch	EXER	→ C	→ E	→ F	→ G	N/A	(→ I)	(→ I)	N/A

NOTE 1 – "N/A" means that the event cannot happen for the State.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

[a] If the node has moved to the state due to remote request addressed to this node, it signals actual bridge sate over the long path and RR over the short path.

[b] The command cannot be issued by another node when there is a higher priority request in the ring and commands are not allowed to coexist.

[c] The node will remain in the same state and will signal current state, but the switches will be dropped.

Table II-3/G.8132 – State transitions for the node found in the switching state receiving remote request addressed to the other node

State ◊ (caused by the local request)		Signaled APS [a]	Remote request addressed to the other node ■							
			a	**b**	**c**	**d**	**e**	**f**	**g**	**h**
			LP	**FS**	**SF**	**MS**	**WTR**	**EXER**	**RR** [b]	**NR** [b]
A	Idle Working: no switch Protection: no switch	NR	→ B	→ B	→ B	→ B	→ B	→ B	N/A	N/A
B	Pass-trough Working: no switch Protection pass through	N/A	(→ B)	N/A [c] (→ B)	N/A [c] (→ B)	N/A [c] (→ B)	N/A [c] (→ B)	N/A [c] (→ B)	N/A	N/A
C	Switching – LP Working: no switch Protection: no switch	LP	(→ C)	O	O	O	N/A	N/A	N/A	N/A
D	Idle – LW Working: no switch Protection: no switch	NR	→ B	→ B	→ B	→ B	→ B	→ B	N/A	N/A
E	Switching – FS Working: switched Protection: switched	FS	→ B	(→ E)	(→ E)	N/A [c]	N/A [c]	N/A [c]	N/A	N/A
F	Switching – SF Working: switched Protection: switched	SF	→ B	(→ F)	(→ F)	N/A [c]	N/A [c]	N/A [c]	N/A	N/A
G	Switching – MS Working: switched Protection: switched	MS	→ B	→ B	→ B	(→ G) [d]	N/A [c]	N/A [c]	N/A	N/A
H	Switching – WTR Working: switched Protection: switched	WTR	→ B	→ B	→ B	→ B	N/A	N/A [c]	N/A	N/A
I	Switching – EXER Working: no switch Protection: no switch	EXER	→ B	→ B	→ B	→ B	→ B	(→ I)	N/A	N/A

NOTE 1 – "N/A" means that the event cannot happen for the State.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

[a] If the node entered the state due to remote request addressed to this node, actual bridge sate is signaled over the long path, while RR is signaled over the short path.

[b] The node should never receive the RR or NR addressed to another node, since NR and RR are sent only over the short path to adjacent nodes.

[c] The command cannot be issued by another node when there is a higher priority request in the ring and commands are not allowed to coexist.

[d] The node will remain in the same state and will signal current state, but the switches will be dropped.