INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG15-TD220/WP3

STUDY GROUP 15

Original: English

Question(s):	9/15	Geneva, 29 January – 9 February 2018

TD

Source:	Editors of G.8131
Title:	Draft Amendment 3 to Recommendation G.8131
Purpose:	Discussion

Contact:	Jeong-dong Ryoo ETRI Republic of Korea	Tel: +82 42 860 5384 E-mail: ryoo@etri.re.kr
Contact:	Lei Wang China Mobile R. P. China	Tel: +86-15801696688-37077 E-mail: wangleiyj@chinamobile.com

Keywords: APC, APS, PSC, bridge, selector, SNC protection, MPLS-TP

Abstract: This document provides Draft Amendment 3 to G.8131 (2014).

Recommendation ITU-T G.8131/Y.1382

Linear protection switching for MPLS transport profile

Amendment 3

Summary

Recommendation ITU-T G.8131/Y.1382 provides architecture and mechanisms for subnetwork connection (SNC) protection switching for MPLS transport profile (MPLS-TP) networks. It describes the SNC protection architectures type, the uni- and bidirectional switching types and the revertive/non-revertive operation types. It defines an automatic protection coordination protocol used to coordinate both ends of the protected domain.

Amendment 1 provided the format of APC specific information, and descriptions about management (MI) signals and trail protection architecture.

Amendment 2 to Recommendation ITU-T G.8131/Y.1382 (2014) provided:

– Support for pseudowire (PW) protection.

– Modifications to the references of terms related to new Recommendation ITU-T G.808

Amendment 3 provides updates on the following:

– Initialization behaviour,

– State transition modification, and

– Operation related to state transition table lookup.

Keywords

APC, APS, PSC, bridge, selector, SNC protection, MPLS-TP.

Recommendation ITU-T G.8131/Y.1382

Linear protection switching for MPLS transport profile

Amendment 3

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T G.8131/Y.1382 (2014) plus its Amendments 1 (2016) and 2 (2016).

1 Scope

This Recommendation provides architecture and mechanisms for linear protection switching for MPLS transport profile (MPLS-TP) networks.

The automatic protection coordination protocol, and 1+1 and 1:1 protection architecture are defined in this Recommendation. Other protection architecture types are for further study.

This Recommendation describes the protection switching functionality for point-to-point connections using the automatic protection switching (APS) mode defined in [IETF RFC 7271].

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.780] Recommendation ITU-T G.780/Y.1351 (2010), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

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

[ITU-T G.806] Recommendation ITU-T G.806 (2012), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T G.808] Recommendation ITU-T G.808 (2016), *Terms and definitions for network protection and restoration.*

[ITU-T G.808.1] Recommendation ITU-T G.808.1 (2014), *Generic protection switching – Linear trail and subnetwork protection*.

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

[ITU-T G.8031] Recommendation ITU-T G.8031/Y.1342 (2011), *Ethernet linear protection switching.*

[ITU-T G.8110.1] Recommendation ITU-T G.8110.1/Y.1370.1 (2011), *Architecture of the Multi-Protocol Label Switching transport profile layer network.*

[ITU-T G.8121] Recommendation ITU-T G.8121/Y.1381 (2013), *Characteristics of MPLS-TP equipment functional blocks*.

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

[IETF RFC 6378] IETF RFC 6378 (2011), *MPLS Transport Profile (MPLS-TP) Linear Protection.*

[IETF RFC 7271] IETF RFC 7271 (2014), *MPLS Transport Profile (MPLS-TP) Linear Protection to Match the Operational Expectations of Synchronous Digital Hierarchy, Optical Transport Network, and Ethernet Transport Network Operators*.

[IETF RFC 7771-A] IETF RFC 7771 (2016), *Switching Provider Edge (S-PE) Protection for MPLS and MPLS Transport Profile (MPLS-TP) Static Multi-Segment Pseudowires; Appendix A – Optional Linear Protection Approach.*

[IETF RFC 8234] IETF RFC 8234 (2017), *Updates to MPLS Transport Profile (MPLS-TP) Linear Protection in Automatic Protection Switching (APS) Mode*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 1+1 protection architecture [ITU-T G.808]

3.1.2 1:n protection architecture [ITU-T G.808]

3.1.3 1-phase [ITU-T G.808]

3.1.4 2-phase [ITU-T G.808]

3.1.5 3-phase [ITU-T G.808]

3.1.6 active transport entity [ITU-T G.808]

3.1.6 APS protocol [ITU-T G.808]

3.1.7 bidirectional protection switching [ITU-T G.780]

3.1.8 bridge [ITU-T G.808]

3.1.9 defect [ITU-T G.806]

3.1.10 failure [ITU-T G.806]

3.1.11 forced switch [ITU-T G.808]

3.1.12 hold-off time [ITU-T G.880]

3.1.13 manual switch [ITU-T G.808]

3.1.14 non-revertive (protection) operation [ITU-T G.808]

3.1.15 normal traffic signal [ITU-T G.808]

3.1.16 permanent bridge [ITU-T G.808]

3.1.17 protected domain [ITU-T G.808]

3.1.18 protection [ITU-T G.808]

3.1.19 protection group [ITU-T G.808]

3.1.20 protection transport entity [ITU-T G.808]

3.1.21 revertive (protection) operation [ITU-T G.808]

3.1.22 selector [ITU-T G.808]

3.1.23 selector bridge [ITU-T G.808]

3.1.24 signal degrade (SD) [ITU-T G.806]

3.1.25 signal fail (SF) [ITU-T G.806]

3.1.26 standby transport entity [ITU-T G.808]

3.1.27 subnetwork connection protection [ITU-T G.808]

3.1.28 switch [ITU-T G.808]

3.1.29 trail [ITU-T G.805]

3.1.30 trail protection [ITU-T G.807]

3.1.31 transport entity [ITU-T G.805]

3.1.32 unidirectional protection switching [ITU-T G.780]

3.1.33 wait-to-restore time [ITU-T G.808]

3.1.34 working transport entity [ITU-T G.808]

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 PSC protocol: A means to coordinate the two ends of the protected domain via the exchange of a single message as defined in [IETF RFC 6378].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACH	Associated Channel Header
APC	Automatic Protection Coordination
APS	Automatic Protection Switching
dFOP	Failure of Protocol defect
DNR	Do-not-Revert
DPath	Data Path
EXER	Exercise
FPath	Fault Path
FS	Forced Switch

G-ACh	Generic Associated Channel
LO	Lockout of protection
LSP	Label Switched Path
MPLS-TP	MPLS Transport Profile
MS	Manual Switch
MS-P	Manual Switch to Protection transport entity
MS-PW	Multi-Segment Pseudowire
MS-W	Manual Switch to Working transport entity
MT_C	MPLS-TP Connection
MT_CP	MPLS-TP Connection Point
MT_TT_Sk	MPLS-TP Trail Termination Sink
NR	No Request
OAM	Operations, Administration and Maintenance
OC	Operator Clear
OTN	Optical Transport Network
PDU	Protocol Data Unit
PSC	Protection State Coordination
PT	Protection Type
PW	Pseudowire
RR	Reverse Request
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SD-P	Signal Degrade on Protection transport entity
SD-W	Signal Degrade on Working transport entity
SF	Signal Fail
SF-P	Signal Fail on Protection transport entity
S-PE	Switching Provider Edge
SF-W	Signal Fail on Working transport entity
SNC	Subnetwork Connection
SNCP	Subnetwork Connection Protection
SNC/S	SNCP with Sublayer monitoring
SS-PW	Single-Segment Pseudowire
TLV	Type Length Value
T-PE	Terminating Provider Edge
WTR	Wait-to-Restore

5 Conventions

In this Recommendation, the term automatic protection coordination (APC) protocol is used to describe the means to coordinate the two ends of the protected domain via the exchange of a single message and represents the protection state coordination (PSC) protocol in automatic protection switching (APS) mode as defined in [IETF RFC 7271]. This protocol is developed to provide the same operator control and experience of APS protocol by modifying and enhancing the PSC protocol as described in [IETF RFC 6378].

6 Protection architecture and characteristics

Protection switching is a fully allocated protection mechanism that can be used on any topology. It is fully allocated in the sense that the route and bandwidth of the protection connection is reserved for a selected working connection. To be effective under all possible failures of the working connection however, the protection connection must be known to have complete physical diversity over all common-failure modes. This may not always be possible. Also, this might require the working connection not to follow its shortest path.

This version of the Recommendation describes the MPLS-TP subnetwork connection protection with sublayer monitoring (SNC/S) protection architecture for both LSP and PW sublayers. It also supports MPLS-TP trail protection architecture for both LSP and PW sublayers. Other types are for further study.

6.1 MPLS-TP protection architecture

6.1.1 MPLS-TP SNC protection

MPLS-TP subnetwork connection protection (SNCP) is used to protect a section of a connection (e.g., that section where two separate routes are available) within an operator's network or multiple operators' networks. Two independent subnetwork connections exist, which act as working and protection transport entities for the (protected) normal traffic signal.

6.1.1.1 SNC/S protection

The MPLS-TP sublayer trail termination functions (i.e., tandem connection termination functions) generate/insert and monitor/extract the MPLS-TP operations, administration and maintenance (OAM) information to determine the status of the working and protection MPLS-TP sublayer trails. See also [ITU-T G.8110.1]. Automatic protection coordination (APC) protocol information is transported over the protection subnetwork connection (SNC). The 1+1 unidirectional protection can work with or without APC protocol.

6.1.2 MPLS-TP trail protection

MPLS-TP trail protection is used to protect a MPLS-TP trail within an operator's network or multiple operators' networks. It is a dedicated end-to-end protection architecture. The MT trail termination functions generate/insert and monitor/extract the end-to-end MPLS-TP OAM information to determine the status of the working and protection transport entities. See also [ITU-T G.8110.1]. APC information is transported over the protection trail except for the case of 1+1 unidirectional switching without APC communication.

The details of the atomic functions for APC processing are described in [ITU-T G.8121].

6.2 Switching types

The protection switching types can be a unidirectional switching type or a bidirectional switching type.

6.2.1 Unidirectional switching type

In unidirectional switching, only the affected direction of the connection is switched to protection; the selectors at each end are independent. This type is applicable for 1+1 MPLS-TP SNC/S protection. Unidirectional switching can protect two unidirectional failures or degradations in opposite directions on different entities.

6.2.2 Bidirectional switching type

In bidirectional switching, both directions of the connection, including the affected direction and the unaffected direction, are switched to protection. For bidirectional switching, APC protocol is required to coordinate the two endpoints.

6.3 Operation types

The protection operation types can be a non-revertive operation type or a revertive operation type.

1+1 protection is often provisioned as non-revertive operation, as the protection is fully dedicated in any case, and this avoids a second "glitch" to the normal traffic signal. There may, however, be reasons to provision this to be revertive operation (e.g., so that the normal traffic signal uses the "short" path except during failure conditions. Certain operator policies also dictate revertive operation even for 1+1).

1:1 protection is usually revertive operation. In revertive operation the protection transport entity can be used for extra traffic during normal operation. Although it is possible to define the protocol in a way that would permit non-revertive operation for 1:1 protection, however, since the working transport entity is typically more optimized (i.e., from a delay and resourcing perspective) than the protection transport entity, it is better to revert and glitch the normal traffic signal when the working transport entity is repaired.

In general, the choice of revertive/non-revertive operation will be the same at both ends of the protection group. However, a mismatch of this parameter does not prevent interworking; it just would be peculiar for one side to go to wait-to-restore (WTR) state for clearing of switches initiated from that side, while the other goes to do-not-revert (DNR) state for its switches.

Revertive/non-revertive operation of the protection switching process shall be configured via MT_C_MI_PS_OperType (for SNC/S) or via MTp_C_MI_PS_OperType (for trail protection).

6.3.1 Non-revertive operation

In non-revertive types, the service will not be switched back to the working transport entity if the switch requests are terminated.

In non-revertive operation, normal traffic signal is allowed to remain on the protection transport entity even after a switch reason has cleared. This is generally accomplished by replacing the previous switch request with a DNR request, which is low priority.

6.3.2 Revertive operation

In revertive types, the service will always return to (or remain on) the working transport entity if the switch requests are terminated. In the case of clearing a command (e.g., Forced switch (FS)), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of a WTR timer, which is used to avoid chattering of selectors in the case of intermittent defects.

In revertive operation, under conditions where normal traffic signal is being transmitted via the protection transport entity and when the working transport entity is restored, if local protection switching requests have been previously active and now become inactive, a WTR state is entered. This state normally times out and becomes a Normal state after the WTR timer has expired.

Then, reversion back to select the working transport entity occurs. The WTR timer deactivates earlier if any local or remote request of higher priority pre-empts this state.

6.4 Protection switching trigger mechanism

Protection switching action shall be conducted when:

- initiated by operator control (e.g., Manual switch (MS), Forced switch (FS) and Lockout of protection (LO)) without a higher priority switch request being in effect;
- Signal fail (SF) or Signal degrade (SD) is declared on the active transport entity and the hold-off timer has expired, and any higher priority switch request is not in effect;
- the WTR timer expires (in revertive operation) without a higher priority switch request being in effect; or
- in the bidirectional 1+1 and 1:1 architecture, the received automatic protection coordination protocol requests to switch and it has a higher priority than any other local request.

6.4.1 Manual control

Manual control of the protection switching function may be transferred from the element or network management system.

6.4.2 Signal fail or signal degrade declaration conditions

Protection switching will occur based on the detection of certain defects on the transport entities (working and protection) within the protected domain. How these defects are detected is the subject of [ITU-T G.8121]. For the purpose of the protection switching process, a transport entity within the protected domain has a condition of OK, failed (Signal fail (SF)), or degraded (Signal degrade (SD)).

In SNC/S protection switching:

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

Signal degrade (SD) is declared when the MT_TT_Sk function in the protected domain detects a trail signal degrade as defined in [ITU-T G.8121].

6.5 Provisioning mismatches

With all of the options for provisioning of the protection groups, there are opportunities for mismatches between the provisioning at the two ends. These provisioning mismatches take one of the several forms:

- Mismatches where proper operation is not possible.
- Mismatches where one or both sides can adapt their operation to provide a degree of interworking in spite of the mismatch.
- Mismatches that do not prevent interworking. An example is the revertive/non-revertive mismatch discussed in clauses 6.3 and 8.1.3.
- See section 12 of [IETF RFC 7271] for the provisioning mismatches and how they are handled.

7 Protection group commands and state

7.1 End-to-end commands

These commands are applied to the protection group as a whole. When a protection switching protocol is present, these commands except Clear are signalled to the far end of the connection. In bidirectional switching, these commands affect the bridge and selector at both ends.

Lockout of protection (LO): Fixes the selector position to the working transport entity. This command prevents the selector from switching to the protection transport entity when it is selecting the working transport entity. This command switches the selector from the protection transport entity to the working transport entity when it is selecting the protection connection.

Forced switch (FS): Switches the selector from the working transport entity to the protection transport entity, unless a higher priority switch request (i.e., LO, SF-P) is in effect.

Manual switch to protection (MS-P): Switches the selector from the working transport entity to the protection transport entity, unless an equal or higher priority switch request (i.e., LO, SF-P, FS, SF-W, SD-W, SD-P or MS-W) is in effect.

Manual switch to working (MS-W): Switches the selector from the protection transport entity to the working transport entity, unless an equal or higher priority switch request (i.e., LO, SF-P, FS, SF-W, SD-W, SD-P or MS-P) is in effect.

Exercise: Exercises the protection switching protocol. The signal is chosen so as not to modify the selector or the bridge.

Clear: Clears all the end-to-end switch commands listed above and the WTR state. This command is not a request sent by APC protocol to the other endpoint.

7.2 Local commands

These commands apply only to the near end of the protection group. Even when a protection switching protocol is supported, they are not signalled to the far end.

Freeze: Freezes the state of the protection group. Until the Freeze command is cleared, additional near end commands are rejected. Condition changes and received protection switching information are ignored. When the Freeze command is cleared, the state of the protection group is recomputed based on the condition and received protection switching information. Because the Freeze command is local, if it is issued at one end only, a failure of protocol can occur as the other end is open to accept any operator command or a fault condition.

Clear freeze: Clears the local Freeze command.

7.3 States

The information on the state of the protected domain is maintained by each network element within the protected domain. The state information would include information of the current state of the protected domain, an indication of the cause for the current state and an indication if the state is related to a remote or local condition.

The protected domain states are as follows:

- Normal state: Both the protection and working transport entities are fully allocated and active. The normal traffic signal is being transported over (or selected from) the working transport entity and no trigger events are reported within the domain.

- Unavailable state: The protection transport entity is unavailable – either as a result of the LO command or a failure or degradation condition detected on the protection transport entity.
- Protecting failure state: The working transport entity has reported a failure or degradation condition and the normal traffic signal is being transported (or selected) on the protection transport entity.
- Switching administrative state: The operator has issued a command switching the normal traffic signal either to the protection transport entity (FS, MS-P) or back to the working transport entity (MS-W).
- Exercise state: The operator has issued the Exercise command testing if the protocol communication is operating correctly.
- Wait-to-restore (WTR) state: The protected domain is recovering from an SF or SD condition on the working transport entity that is being controlled by the WTR timer.
- Do-not-revert (DNR) state: The protected domain has recovered from an SF or SD condition, but the operator has configured the protected domain not to automatically revert to the Normal state upon recovery. This state is entered not only when a failure condition on the working transport entity is cleared, but also when an operator command that requested switch-over, such FS or MS-P, is cleared. The protected domain remains in this state until the operator issues MS-W command followed by the Clear command to revert to the Normal state or there is a new trigger to switch to a different state.

The extended form of the state information, which indicates the cause for the current state and the origin (local or remote) of the cause as well as the current protection domain states (e.g., Unavailable due to local LO command, switching administrative due to remote FS) is shown in Annex A.

7.3.1 Local and remote state

An end may be in a given state as a result of either a local request or as a result of receiving APC information from the far end. If the state is entered as a result of a local request, then the state is considered a local state. If the state is entered as a result of a remote message, in the absence of a local request having equal or higher priority, then the state is considered a remote state.

In any instance where the end has both local and remote requests that cause the protected domain to enter the same state, then the state is considered a local state, regardless of the order in which the indicators were processed. If, however, the end has local and remote indicators that would cause the protected domain to enter different states, e.g., a local SF on working and a remote LO message, then the request with the higher priority (see clause 8.2) will be the deciding factor and the source of that indicator will determine whether it is local or remote. In the given example, the result would be a remote Unavailable state transmitting protocol messages that indicate an SF condition on the working transport entity and that the protection transport entity is not being used to transport protected traffic.

8 Automatic protection coordination protocol

The only switching type that does NOT require the APC protocol is 1+1 unidirectional switching. With a permanent bridge at the head end and no need to coordinate selector positions at the two ends, the tail end selector can be operated entirely according to defects and commands received at the tail end.

Bidirectional switching always requires the APC protocol.

8.1 Automatic protection coordination specific information structure

APC specific information is transmitted over the generic associated channel (G-Ach) as described in [IETF RFC 5586].

The format of the APC specific information over the four-octet associated channel header (ACH) is shown in Figure 2 of [IETF RFC 6378]. All reserved bits should be transmitted as 0 and ignored on reception. The Capabilities TLVs defined in section 9.1 of [IETF RFC 7271] must be carried in the optional type length value (TLV) field. The Capabilities TLVs must be set to show that all five capabilities should be used.

Table 8-1 describes code points and values for the APC specific information.

Table 8-1 – The field values in the APC specific information

Field	Value	Description
Version (V)	1	Version of the protocol. For this recommendation, the value is 1.
	Others	For future use.
Request	14	Lockout of protection (LO)
	12	Forced switch (FS)
	10	Signal fail (SF)
	7	Signal degrade (SD)
	5	Manual switch (MS)
	4	Wait-to-restore (WTR)
	3	Exercise (EXER)
	2	Reverse request (RR)
	1	Do-not-revert (DNR)
	0	No request (NR)
	Others	For future use and ignored upon receipt.
Protection type (PT)	3	Bidirectional switching using a permanent bridge.
	2	Bidirectional switching using a selector bridge.
	1	Unidirectional switching using a permanent bridge.
	0	For future use.
Revertive (R)	0	Non-revertive operation.
	1	Revertive operation.
Fault path (FPath)	0	Indicates that the protection transport entity is identified to be in a fault condition or is affected by an administrative command, or that no fault or command is in effect on both transport entities.
	1	Indicates that the working transport entity is identified to be in a fault condition or is affected by an administrative command.
	2-255	For future extensions and ignored upon receipt.
Data path (DPath)	0	Indicates that the protection transport entity is not transporting user data traffic (in 1:1 architecture) or transporting redundant user data traffic (in 1:1 under SD-P condition or in 1+1 architecture).

Table 8-1 – The field values in the APC specific information

Field	Value	Description
	1	Indicates that the protection transport entity is transmitting user traffic replacing the use of the working transport entity.
	2-255	For future extensions and ignored upon receipt.

In the APC specific information, the values of "Request", "FPath" and "DPath" can be changed to provide protection switching against defects and operator commands. All the other values remain the same as configured by the operator.

The remaining fields in the APC specific information are to indicate the Capabilities TLVs information. The description on the Capabilities TLVs can be found in section 9 of [IETF RFC 7271]. For the protocol operation in this Recommendation, the fields of the Capabilities TLVs information should be set as follows:

- TLV length: This field indicates the number of bytes included in the Capabilities TLV information. This value should be set to 8.
- Capabilities TLV type: The value of this field is 1.
- Capabilities TLV length: The value of this field is the length of the Flags field in octets. This value should be set to 4.
- Flags: This value should be set to 0xF8000000. A different value of this field is not supported in this Recommendation.

If the Capabilities TLVs information in the received APC message is not equal to that in the most recent transmitted message, this indicates a capabilities TLV mismatch. When this happens, the node alerts the operator and should not perform any protection switching until the operator resolves the mismatch in the Capabilities TLVs information.

8.1.1 Request

The requests are signalled between two end points of the protected domain. The highest priority condition, command or state in the near end is always reflected in the Request field of the transmitted protocol messages. The near end will signal reverse request (RR) only in response to an EXER command from the far end.

8.1.2 Protection type

The Protection type (PT) field indicates the currently configured protection architecture type. Two bits indicate permanent/selector bridge type and uni/bidirectional switching type.

If the value of the PT field of one side is 2 (i.e., selector bridge) and the value of PT field of the other side is 1 or 3 (i.e., permanent bridge), then this will result in a defect.

If the bridge type matches but the switching type mismatches, i.e., one side has PT=1 (unidirectional switching) while the other side has PT=2 or 3 (bidirectional switching), then the node provisioned for bidirectional switching should be fall back to unidirectional switching to allow interworking.

The protection type of the protection switching process shall be configured via MT_C_MI_PS_ProtType (for SNC/S) or via MTp_C_MI_PS_ProtType (for trail protection). Either 1+1 or 1:1 switching type can be supported in linear protection, and the bridge type may be a selector bridge or a permanent bridge.

The valid configurations of the MI_PS_ProtType are specified in Table 8-2:

Table 8-2 – Valid configurations of the protection type

MI_PS_ProtType	Protection type valid configuration	**PT value**
1_PLUS_1_UNIDIRECTIONAL_NO_APS	1+1 unidirectional, no APC communication	See Note
1_PLUS_1_UNIDIRECTIONAL_WITH_APS	1+1 unidirectional w/APC communication	1
1_PLUS_1_BIDIRECTIONAL_WITH_APS	1+1 bidirectional w/APC communication	3
1_FOR_1_BIDIRECTIONAL_WITH_APS	1:1 bidirectional w/APC communication	2
NOTE – In case of 1+1 unidirectional with no APC communication, APC messages are not exchanged, so there is no PT value assigned.		

8.1.3 Revertive

The Revertive (R) field indicates that the transmitting end point is configured to work in either revertive or non-revertive operation. If the R information mismatches, one side will clear switches to WTR and the other will clear to DNR. The two sides will interwork and the traffic is protected according to the state transition definition given in Annex A.

8.1.3.1 Revertive operation

In revertive operation of unidirectional protection switching, in conditions where normal traffic signal is being received via the protection transport entity, if the local protection switching requests have been previously active and now become inactive, the WTR state is entered and indicated on the transmitted Request information and maintains the switch.

In the case of bidirectional protection switching, the WTR state is entered only when there is no higher priority of request received from the far end than that of the WTR.

This state normally times out and becomes the Normal state after the WTR timer has expired. The WTR timer is deactivated earlier if any local request of higher priority pre-empts this state.

A switch to the protection entity may be maintained by the WTR state or by a remote request (WTR or other) received via the Request information. Therefore, in a case where a bidirectional failure for a working entity has occurred and subsequent repair has taken place, the bidirectional reversion back to the working transport entity does not take place until both WTR timers at both ends have expired.

8.1.3.2 Non-revertive operation

In non-revertive operation of unidirectional protection switching, in conditions where normal traffic signal is being transmitted via the protection entity, if local protection switching requests have been previously active and now become inactive, the DNR state is entered and indicated on the transmitted Request information and maintains the switch, thus preventing reversion back to the released bridge/selector position in non-revertive operation under no request conditions.

In the case of bidirectional protection switching operation, the DNR state is entered only when there is no higher priority of request received from the far end than that of the DNR.

8.1.4 Fault path

The Fault path (FPath) field indicates which transport entity (i.e., working or protection) is identified to be in a fault condition or affected by an administrative command, when a fault or command is indicated by the Request field to be in effect. When a local node has neither a local fault nor a local command for both transport entities, the local node sets this value to be 0 (zero).

8.1.5 Data path

The Data path (DPath) field indicates which data is being transported on the protection transport entity. Under normal conditions, the protection transport entity (especially, in 1:1 or 1:n architecture) does not need to carry any user data traffic. If there is a failure or degrade condition on the working transport entity, then that working transport entity's data traffic will be transported over the protection transport entity.

Note that this field dictates the positions of both selector and bridge.

8.2 Priorities of local and remote requests

The priorities for both local and remote requests are defined as follows from highest to lowest:

- Clear (local only)
- Lockout of protection (local and remote)
- Clear signal fail or degrade (local only)
- Signal fail on protection (local and remote)
- Forced switch (local and remote)
- Signal fail on working (local and remote)
- Signal degrade on either protection or working (local and remote)
- Manual switch to either protection or working (local and remote)
- WTR timer expires (local only)
- WTR (remote only)
- Exercise (local and remote)
- Reverse request (remote only)
- Do-not-revert (remote only)
- No request (remote and local)

Note that the "local only" requests are not signalled to the far end. Likewise, the "remote only" requests do not exist in the local Request logic (see clause 8.6) as local inputs. For example, the priority of WTR only applies to the received WTR message, which is generated from the far end. The far end that is running the WTR timer in the WTR state has no local request.

The remote SF and SD on either working or protection and the remote MS to either working or protection are indicated by the values of the Request and Fault path (FPath) fields in the APC specific information.

The remote request from the far end is assigned a priority just below the same local request except no request (NR) and the equal priority requests, such as SD and MS. Since a received NR message needs to be used in the state transition table lookup when there is no outstanding local request, the received remote NR request has a higher priority than the local no request. For the equal priority requests, see clause 8.7.

8.2.1 Signal fail of the protection transport entity

Signal fail (SF) on the protection transport entity has a higher priority than any defect that would cause a normal traffic signal to be selected from protection. In a 1-phase protection protocol, an SF on the protection transport entity (over which the protocol message is routed) has priority over the

FS. LO command has higher priority than SF-P: during failure conditions, lockout status shall be kept active.

8.3 APC initiation criteria

The following switch initiation criteria exist:

1) An externally initiated command (Clear, LO, FS, MS, EXER);
2) an automatically initiated request (SF, SD) associated with a protected domain;
3) a state (WTR, RR, DNR) of the protection switching function; or
4) an internally initiated request (WTR timer expires).

8.4 APC protocol type

There are two basic requirements for protection switching protocols:

1) The prevention of misconnections.
2) The minimization of the number of communication cycles between A and Z ends of the protected domain, in order to minimize the protection switching time. The communication may be once (Z → A), twice (Z → A and A → Z), or three times (Z → A, A → Z and Z → A). This is referred to as 1-phase, 2-phase and 3-phase protocols.

To keep balance between saving operational time, reducing protocol complexity and facilitating application, the suggested protocol types for the different protection architectures are shown in Table 8-3.

Table 8-3 – Protocol types related to protection architectures

Protocol type	Protection architecture
No protocol	1+1 unidirectional
1-phase protocol	1+1 bidirectional, 1:1 bidirectional

NOTE – The use of a "1-phase" protocol implies that the "label distribution policy" assigns a unique label value per path, in such a way that it avoids different label switched paths (LSPs) to access the protection resource (even in transient phases) with the same label. A unique label per path allows avoiding misconnections.

The protocol for MPLS-TP linear protection is defined as the 1-phase and the details are in clause 8.6.

8.5 Transmission and acceptance of APC messages

APC messages are transported via the protection transport entity only, being inserted by the head end of the protected domain and extracted by the tail end of the protected domain.

A new APC message must be transmitted immediately when a change in the transmitted status occurs.

The first three APC messages should be transmitted as fast as possible only if the protection switching information to be transmitted has been changed so that fast protection switching is possible even if one or two APC messages are lost or corrupted. For the fast protection switching in 50 ms, the interval of the first three automatic protection coordination messages should be no longer than 3.3 ms. The APC messages after the first three should be transmitted with a default interval of 5 seconds.

If no valid APC specific information is received, the last valid received information remains applicable except in case of SF condition on the protection transport entity.

If a protection end point receives an APC message from the working entity, it should ignore this information, and should detect the failure of protocol defect for the local network element (see clause 8.15).

8.6 1-phase APC protocol

8.6.1 Principle of operation

Figure 8-1 illustrates the principle of the MPLS-TP linear protection switching algorithm. This algorithm is performed in the network elements at both ends of the protected domain. Bidirectional switching is achieved by transmitting local switching requests to the far end via the Request and Fault path fields in the protection switching information (see Table 8-1). The transmitted "Data path" in the fourth octet of the protection switching information contains the local bridge/selector status information; a persistent mismatch between both ends may thus be detected and leads to an alarm.

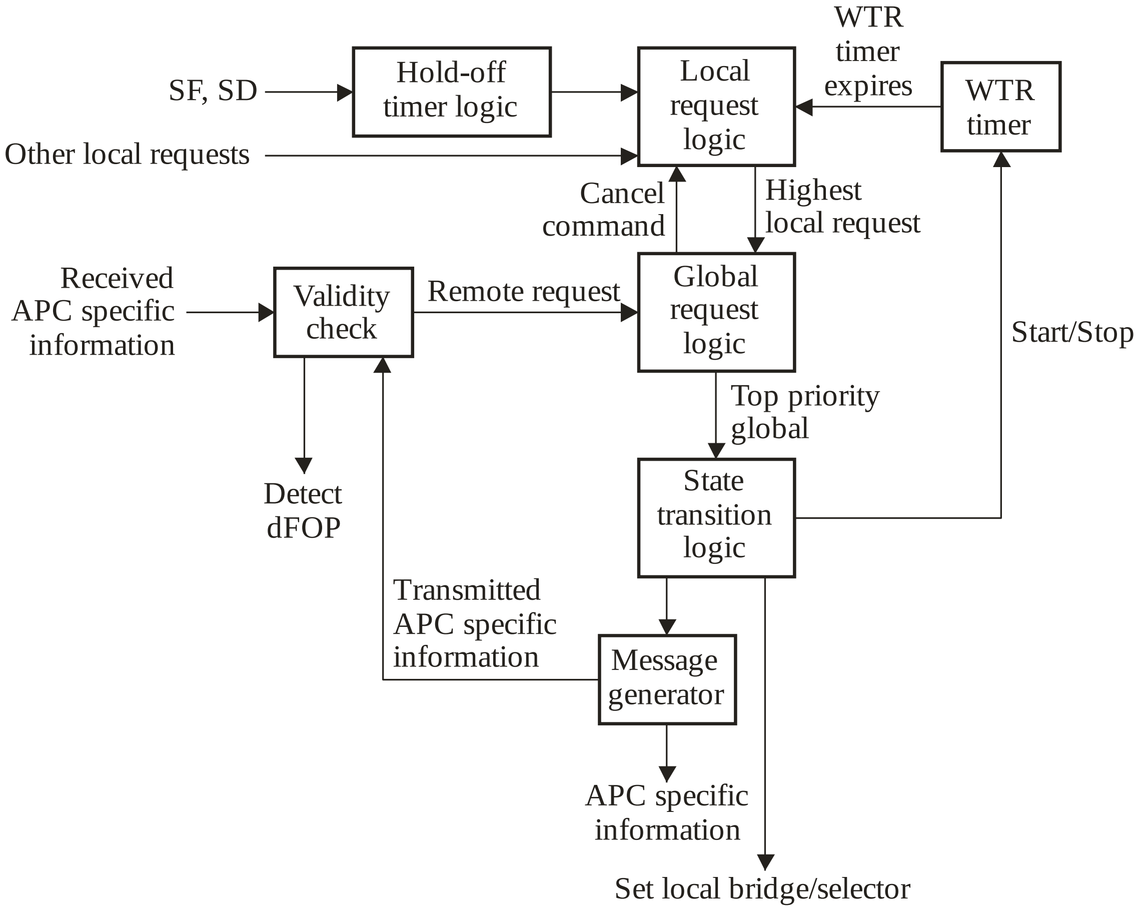

Figure 8-1 – Principle of MPLS-TP linear protection switching algorithm

In detail, the functionality is as follows (see Figure 8-1):

At the local network element, one or more local protection switching requests (as listed in clause 8.2) may be active. The "local request logic" determines which of these requests is of highest priority, using the order of priority given in clause 8.2. This highest priority local request (highest local request) is passed to the "global request logic", that will determine the higher priority request (top priority global request) between the highest local request and the last received remote request. When a remote request comes to the global request logic, the top priority global request is determined between this remote request and the highest local request which is present. For the detailed description on the priority evaluation, see clauses 8.2 and 8.7. The top priority global request is used to determine the state transition, which is described in Annex A.

If the provisioned hold-off timer value is non-zero, when the "hold-off timer logic" receives new SF/SD, it does not report this information to the "local request logic" immediately. Instead the hold-off timer will start (see clause 8.11).

The local network element receives information from the network element of the far end via the protocol message. The received protocol message is subjected to the "validity check" (see clause 8.15).

The state transition is calculated in the "state transition logic" based on the top priority global request and the state transition tables defined in Annex A, as follows:

a) If the top priority global request, which determines the state transition, is the highest local request, then the local state transition table should be used to decide the next state. Otherwise, the remote state transition table should be used.

b) If in a remote state, the highest local defect condition (SF-P, SF-W, SD-P or SD-W) should always be reflected in the Request and FPath fields.

c) For the end currently in a local state, if the top priority global request is changed to Clear or clearance of signal fail or degrade causing the next state to be Normal, WTR or DNR, then all the local and remote requests should be re-evaluated as if the node is in the state specified in the footnotes to the state transition tables, before deciding the final state. If there are no active requests, the end enters the state specified in the footnotes to the state transition tables. This re-evaluation is an internal operation confined within the local node, and the protocol messages are generated according to the final state.

d) The WTR timer is started only when the node which has recovered from a local failure or degradation enters the WTR state. A node which is entering into the WTR state due to a remote WTR message does not start the WTR timer. The WTR timer will be stopped when any local or remote request triggers the state change out of the WTR state.

e) When the local SF-P is cleared and the priorities of the local and remote requests are re-evaluated, the last received remote message may no longer be valid due to the previous failure of the protection path. Therefore, the last received message must be treated as if it were NR and only the local request shall be evaluated.

The top priority global request will be exactly the same with the top priority local request in the case of unidirectional protection switching because the received protection switching information should not affect the operation of the unidirectional protection switching.

The "message generator" generates APC specific information as described in clause 8.5 and Annex A.

The bridge/selector position of the local network element is determined by the final state calculated in the state transition logic. See also clauses 8.8 and 8.9 for the control of the bridge and the selector.

Note that the linear protection switching algorithm commences immediately every time one of the input signals (see Figure 8-1) changes, i.e., when the status of any local request changes, or when a different APC specific information is received from the far end. The consequent actions of the algorithm are also initiated immediately, i.e., change the local bridge/selector position (if necessary), transmit a new APC specific information (if necessary), or detect failure of protocol defect (dFOP) if the protection switching is not completed within a period specified in clause 8.15.

8.7 Equal priority requests

As stated in clause 8.2, the remote request from the far end is assigned a priority just below the same local request. However, for equal priority requests, such as SD and MS, the priority is evaluated as described in this clause.

For equal priority local requests, a first-come, first-served rule is applied. Once a local request appears in the local request logic, a subsequent equal priority local request requesting a different action, i.e., the action results in the same Request value but a different FPath value, will have a lower priority. Furthermore, in the case of MS command, the subsequent local MS command requesting a different action will be cancelled.

When the priority is evaluated in the global request logic between the highest local request and a remote request, the following equal priority resolution rules are defined:

a) If two requests request the same action, i.e., the same Request and FPath values, then the local request is considered to have a higher priority than the remote request.

b) When the highest local request comes to the global request logic, if the remote request that requests a different action exists, then the highest local request is ignored and the remote request remains to be the top priority global request. In the case of MS command, the local MS command requesting a different action will be cancelled.

c) When the remote request comes to the global request logic, if the highest local request that requests a different action exists, then the top priority global request is determined by the following rules:

   - For MS requests, the MS-W request is considered to have a higher priority than the MS-P request. The end that has local MS-W request maintains the local MS-W request as the top priority global request, but the other end that has local MS-P request clears the MS-P command and internally generate "Clear" request.
   - For SD requests, the SD on the standby transport entity (the transport entity from which the selector does not select the user data traffic) is considered as having higher priority than the SD on the active transport entity (the transport entity from which the selector selects the user data traffic) regardless of its origin (local or remote message). The end that has the SD on the standby transport entity maintains the local SD on the standby transport entity request as the top priority global request. The other end that has local SD on the active transport entity uses the remote SD on the standby transport entity as the top priority global request to lookup the state transition table. The differentiation of the active and standby transport entities is based upon which transport entity had been selected for the user data traffic at the time when each end detected its local SD.

8.8 Control of bridge

In 1+1 architectures, the normal traffic signal is permanently bridged to the protection transport entity. The Data path (DPath) field indicates that either the protection transport entity is transmitting user traffic replacing the use of the working transport entity (DPath=1) or the protection transport entity is transporting redundant user data traffic (DPath=0).

In 1:1 architectures, the normal traffic signal is bridged to either the working or the protection transport entity. Under SD condition, the normal traffic signal is duplicated and fed to both the working and the protection transport entities.

When a local or remote SD occurs on either the working transport entity or the protection transport entity, the end duplicates user data traffic and feed to both the working transport entity and the protection transport entity. The packet duplication continues as long as any SD condition exists in the protected domain. The packet duplication continues in the WTR state in revertive operation and stops when the WTR state ends. In non-revertive operation, the packet duplication stops when the SD condition is cleared.

8.9 Control of selector

In 1+1 unidirectional architectures, the selector is set entirely according to the highest priority local request.

In 1+1 and 1:1 bidirectional architectures, the normal traffic signal will be selected from the protection entity when the Data path (DPath) field indicates that the protection transport entity is transmitting user traffic replacing the use of the working transport entity (i.e., when DPath=1). If DPath=0, the normal traffic signal will be selected from the working transport entity.

8.10 Acceptance and retention of local requests

A local request indicating a defect, such as SF-P, SF-W, SD-P and SD-W, SHALL be accepted and retained persistently in the local request logic as long as the defect condition exists. If there is any higher priority local request than the local defect input, the higher priority local request is passed to the global logic as the highest local request, but the local defect input cannot be removed but remains in the local request logic. When the higher priority local request disappears, the local defect will become the highest local request if the defect condition still exists.

Clear command, clearance of SF or SD and WTR timer expires requests are not persistent. Once they appear to the local request logic and complete the operation, they will disappear.

LO, FS, MS, and EXER commands will be rejected if there is any higher priority local request in the local request logic. If a new higher-priority local request (including an operator command) is accepted, any previous lower-priority local operator command should be cancelled. When any higher-priority remote request is received, a lower-priority local operator command should also be cancelled. The cancelled operator command is forgotten and will never return, unless the operator reissues the command.

Each external command shall be input to the protection switching process via MT_C_MI_PS_ExtCMD (for SNC/S) or via MTp_C_MI_PS_ExtCMD (for trail protection).

8.11 Hold-off timer

In order to coordinate timing of protection switches at multiple layers or across cascaded protected domains, a hold-off timer may be required. The purpose is to allow either a server layer protection switch to have a chance to fix the problem before switching at a client layer, or to allow an upstream protected domain to switch before a downstream domain.

Each end should have a provisionable hold-off timer. The suggested range of the hold-off timer is 0 to 10 seconds in steps of 100 ms.

When a new defect or more severe defect occurs at the active transport entity, this event will not be reported immediately to protection switching if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the hold-off timer expires, it will be checked whether a defect still exists on the trail that started the timer. If it does, that defect will be reported to protection switching. The defect need not be the same one that started the timer.

The hold-off timer of the protection switching process shall be configured via MT_C_MI_PS_HoTime (for SNC/S) or via MTp_C_MI_PS_HoTime (for trail protection).

8.12 Wait-to-restore timer

In revertive operation, to prevent frequent operation of the protection switch due to an intermittent defect, a failed working transport entity must become fault-free. After the failed working transport entity meets this criterion, a fixed period of time shall elapse before a normal traffic signal uses it again. This period, called WTR period, may be configured by the operator in 1-minute steps between 5 and 12 minutes; the default value is 5 minutes. An SF or SD condition will override the WTR.

In revertive operation, when the protection is no longer requested, i.e., the failed working transport entity is no longer in SF or SD condition (and assuming no other requesting transport entities), the WTR state will be entered and the WTR timer will be started. This state is indicated in the Request field as WTR and the local end maintains the normal traffic signal on the protection transport entity. This state shall normally time out and become the Normal state. The WTR timer is stopped before it expires when any request of higher priority pre-empts this state.

The wait-to-restore timer of the protection switching process shall be configured via MT_C_MI_PS_WTR (for SNC/S) or via MTp_C_MI_PS_WTR (for trail protection).

8.13 Exercise operation

EXER is a command to test if the protection switching protocol communication is operating correctly. It is lower priority than any "real" switch request. It is only valid in bidirectional switching, since this is the only place where you can get a meaningful test by looking for a response.

The EXER command shall be issued with the same FPath and DPath values of the NR, RR or DNR request that it replaces. The valid response will be an RR with the corresponding FPath and DPath values. When EXER commands are input at both ends, an EXER, instead of RR, is transmitted from both ends. When the EXER command is cleared, it will be replaced with NR or RR if the DPath value is 0 and DNR or RR if the DPath value is 1.

8.14 Signal degrade processing

The protection switching controller does not care which monitoring method is used, as long as it can be given information for the transport entities within the protected domain. Some monitors or network layers may not have an SD detection method. Where this is the case, there is no need to use a different protection switching protocol: it would simply happen that an SD would not be issued from equipment that cannot detect it. Where a protection protocol is used, the implementation should not preclude the far end from declaring an SD over the protection protocol, even if the monitor at the near end cannot detect SD.

Signal degrade (SD) on the protection transport entity has the same priority as SD on the working transport entity. As a result, in case a SD condition affects both transport entities, the first SD detected is not overridden by the second SD detected. In case SD is detected simultaneously either as local or far end requests on both working and protection transport entities, SD on the standby transport entity is considered as having higher priority than SD on the active transport entity, and the normal traffic signal continues to be selected from the active transport entity (i.e., no unneeded protection switching is performed).

In the previous paragraph, "simultaneously" relates to the occurrence of SD on both the active and standby transport entities at input to the protection switching process at the same time, or as long as a SD request has not been confirmed by the remote end in bidirectional protection switching. When a local node that has transmitted a SD message receives a SD message that indicates a different DPath value than the DPath value in the transmitted SD message, both the local and the remote SD requests are considered to occur simultaneously.

It should be noted that the descriptions on the global priority logic in Clauses 8.6 and 8.7 and the state transition logic in Annex A have already incorporated the signal degrade processing stated in the preceding paragraphs.

8.15 Failure of protocol defects

"Failure of protocol" situations for protection types requiring protection protocol are as follows:

- Fully incompatible provisioning (the bridge type mismatch described in clause 8.1.2 and the Capabilities TLV mismatch described in clause 8.1);
- Working/Protection configuration mismatch (described in clause 8.5);
- Lack of response to a bridge request (i.e., no match in sent "Data path" and received "Data path") in case of bidirectional switching for > 50 ms.
- No protocol message is received on the protection transport entity during at least 3.5 times the long message interval (e.g., at least 17.5 seconds) and there is no defect on the protection transport entity.

Fully incompatible provisioning and working/protection configuration mismatch are detected by receiving only one automatic protection coordination frame. Detection and clearance of the defects are defined in [ITU-T G.8121]

If an unknown request or a request for an invalid Data/Fault path number is received, it will be ignored.

9 Application architectures

Working and protection transport entities for the protection switching process shall be configured via MT_C_MI_PS_WorkingPortId and MT_C_MI_PS_ProtectionPortId (for SNC/S) or via MTp_C_MI_PS_WorkingPortId and MTp_C_MI_PS_ProtectionPortId (for trail protection).

9.1 Unidirectional 1+1 SNC/S protection switching

The unidirectional 1+1 SNC/S protection switching architecture is as shown in Figure 9-1. In the case of unidirectional protection switching operation as described here, protection switching is performed by the selector at the sink (Node Z) of the protection domain based on purely local information. The normal traffic signal is permanently bridged to working and protection connection (transport entity) at the source (Node A) of the protection domain. The server/sublayer's trail termination and adaptation functions are used to monitor and determine the status of the working and protection connection.

Unidirectional 1+1 SNC/S protection can be either revertive or non-revertive.

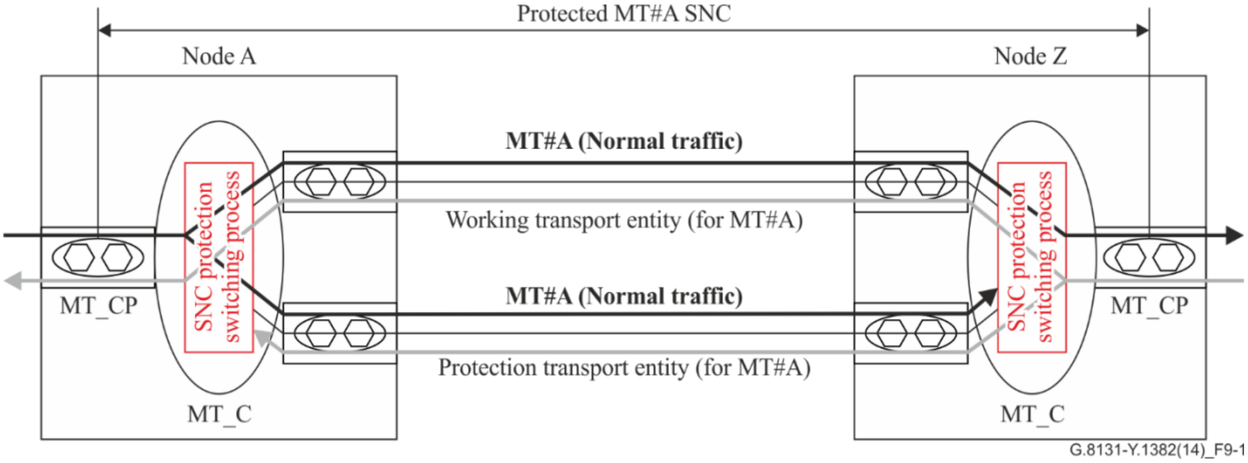
Protected MT#A SNC
Node A
Node Z
MT#A (Normal traffic)
Working transport entity (for MT#A)
MT#A (Normal traffic)
Protection transport entity (for MT#A)
SNC protection switching process
SNC protection switching process
MT_CP
MT_CP
MT_C
MT_C
G.8131-Y.1382(14)_F9-1

Figure 9-1 – Unidirectional 1+1 SNC/S protection switching architecture

For example, if a unidirectional defect (in the direction of transmission from node A to node Z) occurs for the working transport entity as shown in Figure 9-2, this defect will be detected at the sink of the protection domain at node Z and the selector at node Z will switch to the protection transport entity. Now, the protected traffic from node Z to node A flows on the protection transport entity, while the protected traffic from node A to node Z still flows on the working transport entity.

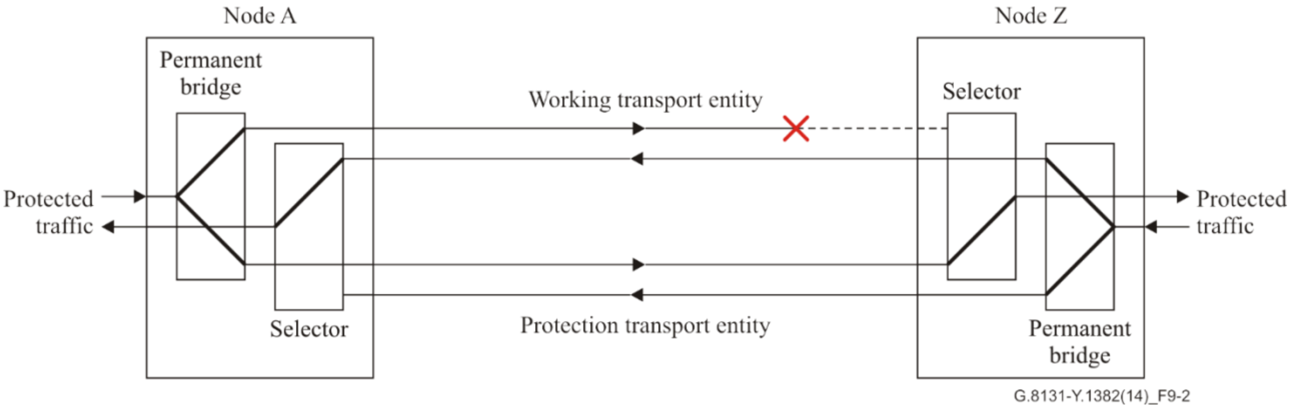

Figure 9-2 – Unidirectional 1+1 SNC/S protection switching working transport entity fails

Figure 9-3 shows a case where the working transport entity fails in one direction (A-to-Z) and the protection transport entity fails in the opposite direction (Z-to-A). Unidirectional protection switching can protect this type of double defect scenarios.

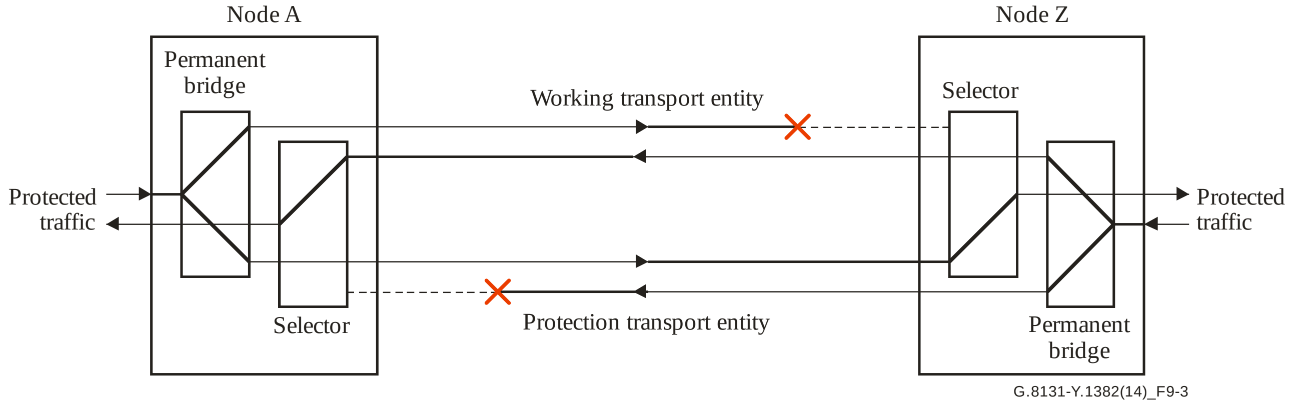

Figure 9-3 – Unidirectional 1+1 SNC/S protection switching working and protection connections fail in opposite direction

9.2 Bidirectional 1+1 SNC/S protection switching

The bidirectional 1+1 SNC/S protection switching architecture is as shown in Figure 9-4. In the case of bidirectional protection switching operation as described here, the protection switching is performed by the selectors at both sides of the protection domain based on local or near-end information and the automatic protection coordination protocol information from the other side or far end. The normal traffic signal is permanently bridged to working and protection connection at the source (Node A) of the protection domain. The server/sublayer's trail termination and adaptation functions are used to monitor and determine the status of the working and protection connection.

Bidirectional 1+1 SNC/S protection can be either revertive or non-revertive.

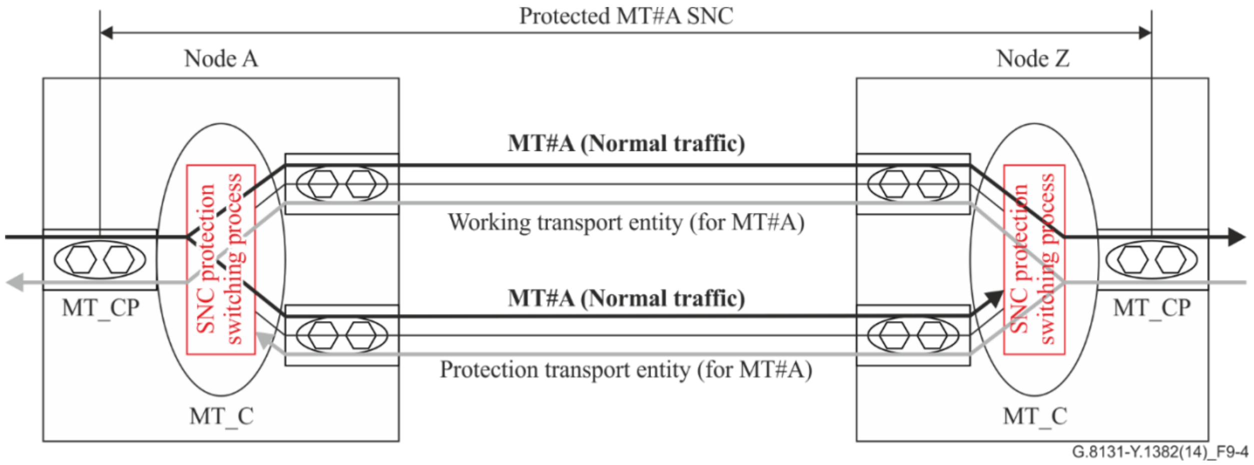
Protected MT#A SNC
Node A
Node Z
MT#A (Normal traffic)
Working transport entity (for MT#A)
MT#A (Normal traffic)
Protection transport entity (for MT#A)
SNC protection switching process
SNC protection switching process
MT_CP
MT_CP
MT_C
MT_C
G.8131-Y.1382(14)_F9-4

Figure 9-4 – Bidirectional 1+1 SNC/S protection switching architecture

For example, if a unidirectional defect (in the direction of transmission from node A to node Z) occurs for the working transport entity as shown in Figure 9-5, this defect will be detected at node Z. The APC protocol is initiated. The protocol is as follows:

- Node Z detects the defect;
- The selector at node Z switches to the protection transport entity A-to-Z;
- The APC message sent from node Z to node A requests a protection switch;
- After node A validates the priority of the protection switch request, the selector at node A is switched to the protection transport entity Z-to-A;

- Then, the APC message sent from node A to node Z is used to inform node Z about the switching;
- Now, the traffic flows on the protection transport entity in both directions (A-to-Z and Z-to-A).

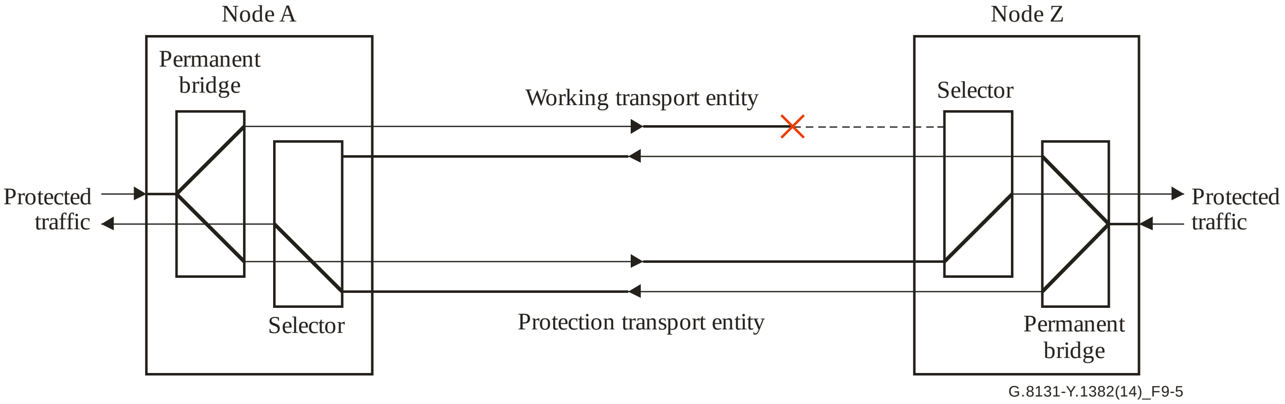

Figure 9-5 – Bidirectional 1+1 trail protection switching working connection A-to-Z fails

9.3 Bidirectional 1:1 SNC/S protection switching

The bidirectional 1:1 SNC/S protection switching architecture is as shown in Figure 9-6. In the case of bidirectional protection switching operation as described here, the protection switching is performed by both the selector bridge at the source and the selector at the sink side of the protection domain based on local or near-end information and the APC protocol information from the other side or the far end. The server/sublayer's trail termination and adaptation functions are used to monitor and determine the status of the working and protection connection.

Bidirectional 1:1 SNC/S protection can be either revertive or non-revertive.

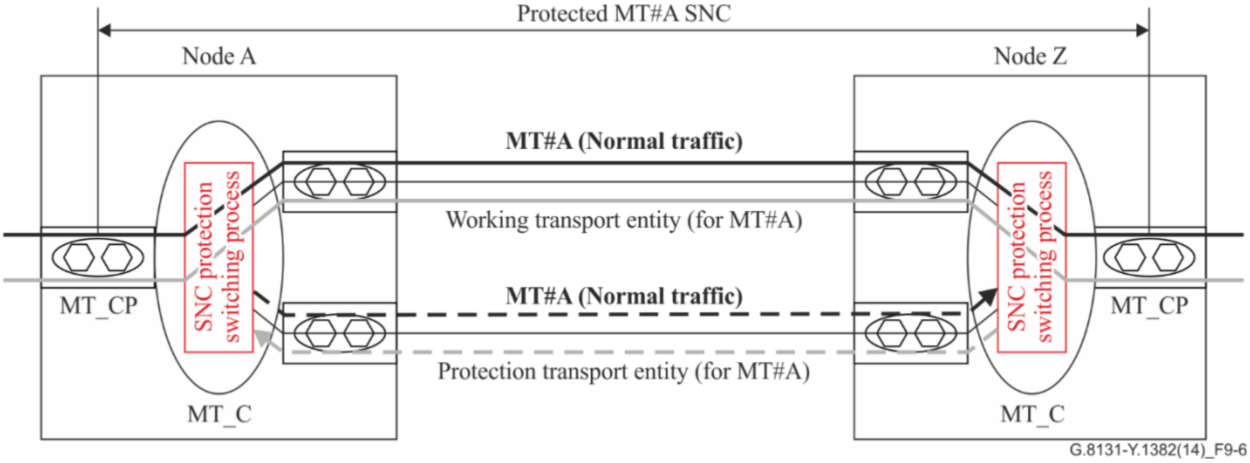
Protected MT#A SNC
Node A
Node Z
MT#A (Normal traffic)
Working transport entity (for MT#A)
MT#A (Normal traffic)
Protection transport entity (for MT#A)
SNC protection switching process
SNC protection switching process
MT_CP
MT_CP
MT_C
MT_C
G.8131-Y.1382(14)_F9-6

Figure 9-6 – Bidirectional 1:1 SNC/S protection switching architecture

For example, if a SF in the direction of transmission from node Z to node A occurs for the working transport entity Z-to-A as shown in Figure 9-7, this defect will be detected at node A. The APC protocol is initiated. The protocol is as follows:

- Node A detects the SF defect;

- The selector bridge at node A is switched to the protection transport entity A-to-Z (i.e., in the A to Z direction the normal traffic signal is sent on the protection transport entity A-to-Z) and the selector at node A switches to the protection transport entity Z-to-A;
- The APC message sent from node A to node Z requests a protection switch;
- After node Z validates the priority of the protection switch request, the selector at node Z is switched to the protection transport entity A-to-Z and the selector bridge at node Z is switched to the protection transport entity Z-to-A (i.e., in the Z-to-A direction the normal traffic signal is sent on the protection transport entity Z-to-A);
- Then, the APC message sent from node Z to node A is used to inform node A about the switching;
- Now, the traffic flows on the protection connection.

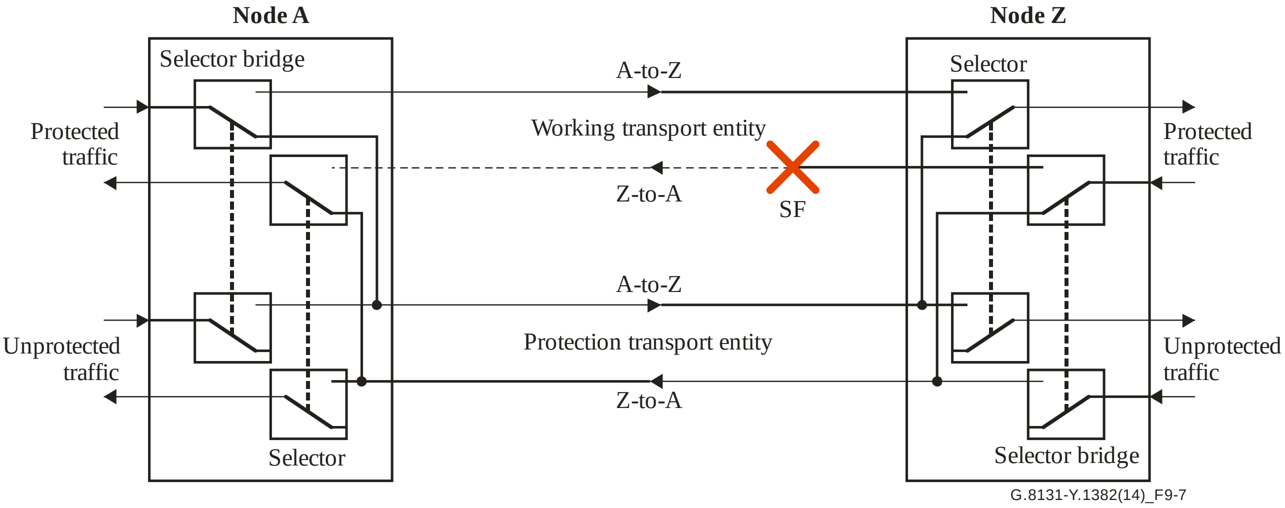

Figure 9-7 – Bidirectional 1:1 SNC/S protection switching working connection Z-to-A fails

In case that protection switching is triggered by SD, the selector bridge at each end node duplicates the protected traffic to both working and protection transport entities so that each end node can select the protected traffic from the protection transport entity while it can persistently detect the SD condition from the working transport entity. This duplication continues until the defect condition is confirmed to be cleared at the end node. For example, if SD in the direction of transmission from node Z to node A occurs for the working transport entity Z-to-A as shown in Figure 9-8, this defect will be detected at node A. The APC protocol is initiated. The protocol is as follows:

- Node A detects the SD defect;
- The selector bridge at node A duplicates the protected traffic to both the working and protection transport entities A-to-Z and the selector at node A switches to the protection transport entity Z-to-A;
- The APC message sent from node A to node Z requests a protection switch;
- After node Z validates the priority of the protection switch request, the selector at node Z is switched to the protection transport entity A-to-Z and the selector bridge at node Z duplicates the protected traffic to both the working and protection transport entities Z-to-A;
- Then, the APC message sent from node Z to node A is used to inform node A about the switching;
- Now, the traffic flows on the protection transport entity.

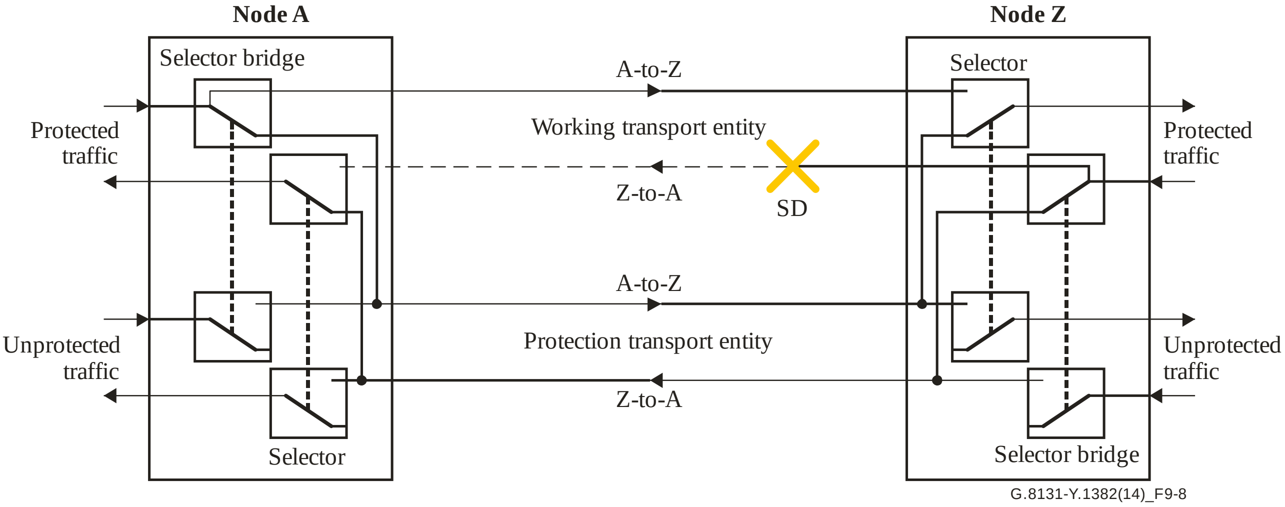

Figure 9-8 – Bidirectional 1:1 SNC/S protection switching working transport entity Z-to-A degrades

If the SD detected at node A in Figure 9-8 is cleared, the protected domain will go either WTR or DNR state depending on the operation type. If the protected domain is configured as revertive operation, the selector bridges at node A and node Z in Figure 9-8 keep duplicating the protected traffic to both the working and protection transport entities until the state is changed from WTR to Normal. If the protected domain is configured as non-revertive operation, the state of the protected domain will go to the DNR state, and the selector bridges at node A and node Z are connected only to the protection transport entity as shown in Figure 9-9.

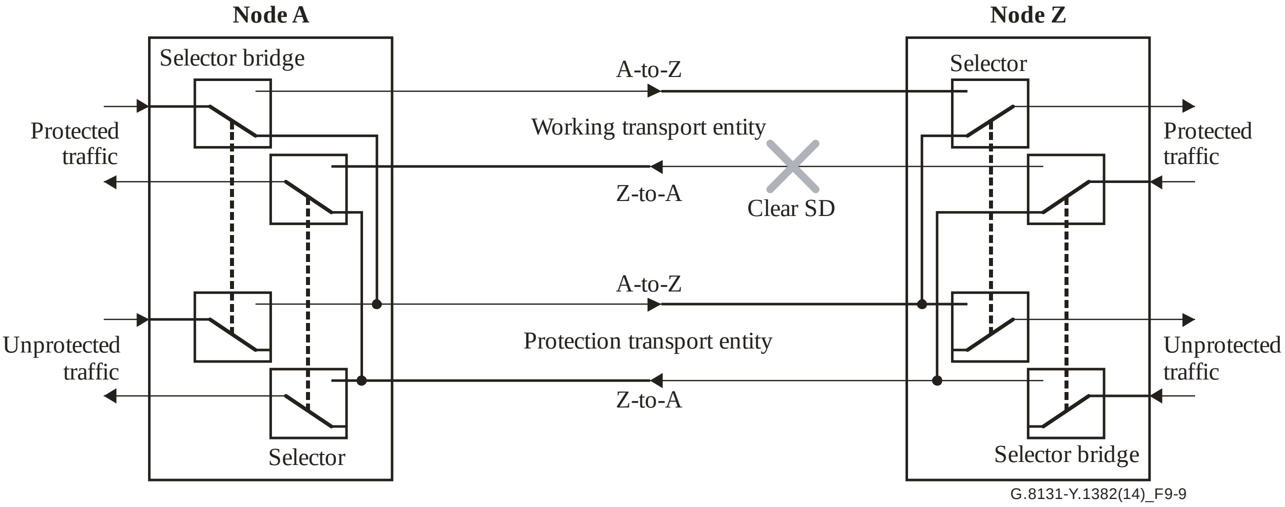

Figure 9-9 – Bidirectional 1:1 SNC/S protection switching working transport entity Z-to-A recovers from degradation (in non-revertive operation)

The ability of the protection switching process to trigger protection switching upon SD shall be configured via MT_C_MI_PS_SD_Protection (for SNC/S) or via MTp_C_MI_PS_SD_Protection (for trail protection). MI_PS_SD_Protection accepts the values enabled and disabled. The default value of MI_PS_SD_Protection shall be disabled.

NOTE – MT_C_MI_PS_SD_Protection and MTp_C_MI_PS_SD_Protection are recommended to be set to enabled only when both ends can trigger protection switching upon SD. If SD capability is unknown at the far end then it is expected that the operator would set the MT_C_MI_PS_SD_Protection or the MTp_C_MI_PS_SD_Protection to disabled at the local end.

9.4 Relationship with ITU-T G.8131 (2007)

This Recommendation enhances the behaviour defined in G.8131 (2007) (that is consistent with the behaviour of ITU-T G.8031 (2006)) by adding support for the MS-W, SD and EXER functions (that is consistent with [ITU-T G.8031]). The format of the APS-specific information used in ITU-T G.8131 (2007) is the same as the format of the APS-specific information defined in clause 11.1, Figure 11.2 of [ITU-T G.8031] except that the reserved field is bits 1-8 of byte 4 (i.e., the one-bit "T" field is not used). In the case where the protocol data unit (PDU) formats of this Recommendation and that of ITU-T G.8131 (2007) are present in an operator's network, these PDU formats are sufficiently different to allow detection of any network misconfiguration.

9.5 Pseudowire protection

The MPLS-TP linear protection switching mechanisms defined in this Recommendation can be used to provide end-to-end protection for pseudowires (PWs) carried over MPLS-TP LSPs as defined in [IETF RFC 7771-A]. This enables a uniform operational approach for protection at LSP and PW layers and an easier management integration for networks that already implement the MPLS-TP linear protection. Both Single-Segment Pseudowire (SS-PW) and Multi-Segment Pseudowire (MS-PW) are supported.

The protected domain of a point-to-point PW consists of two terminating PEs (T-PEs) and the transport entities that connect them (see Figure 9-10).

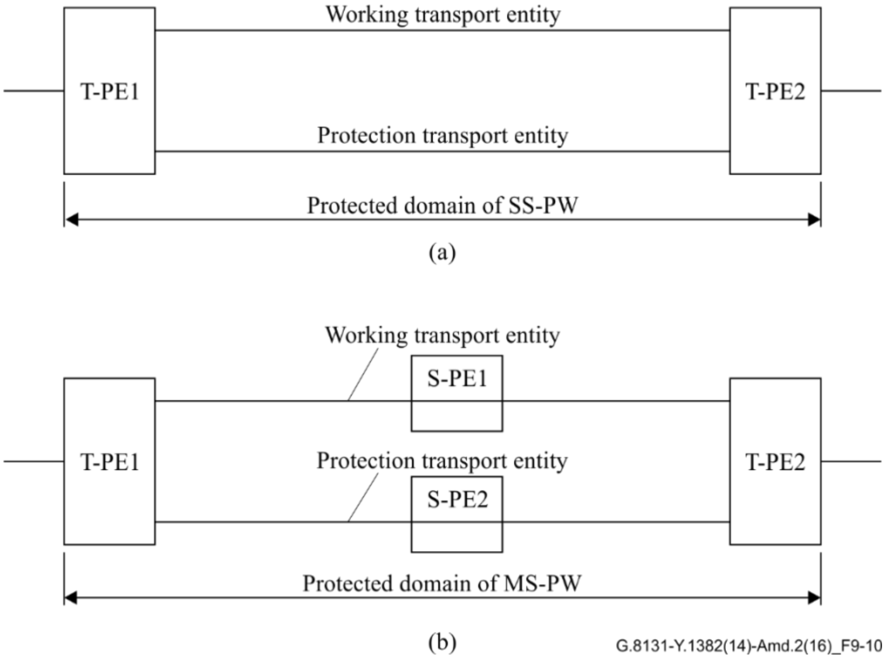
Working transport entity
T-PE1
T-PE2
Protection transport entity
Protected domain of SS-PW
(a)
Working transport entity
S-PE1
T-PE1
Protection transport entity
T-PE2
S-PE2
Protected domain of MS-PW
(b)
G.8131-Y.1382(14)-Amd.2(16)_F9-10

Figure 9-10 – Protected domain of (a) SS-PW; (b) MS-PW

9.5.1 Encapsulation of the APC protocol for pseudowires

The APC protocol is used to coordinate the two ends of the protected domain to provide protection against defects on the transport entities within the protected domain. In the case of MS-PW, the APC protocol can also protect failed S-PE. Linear protection protects an LSP or PW end-to-end and if a failure is detected, switches traffic over to another transport entity available.

Obviously, the protected entity does not need to be of the same type as the protecting entity. For example, it is possible to protect a link by a path. Likewise, it is possible to protect an SS-PW with an MS-PW, and vice versa.

From an APC protocol point of view, it is possible to view an SS-PW as a single-hop LSP and an MS-PW as a multiple-hop LSP. Thus, this provides end-to-end protection for the SS-PW or MS-PW. The G-ACh carrying the APC specific information is placed in the label stack directly beneath the PW label. The APC protocol will then work as specified in this Recommendation.

10 Security aspects

This Recommendation does not raise any security issues that are not already present in either the MPLS-TP architecture or in the architecture of its client layer protocols.

Protection switching could enhance the security of MPLS-TP networks as it will automatically switch traffic from defective connections that may have been misbranched or misconfigured into other connections, onto proper working connections. This will prevent customers' traffic being exposed to other customers.

Annex A

State transition tables of protection switching

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

For the sake of clarity of the state transition tables, the states listed in clause 7.3 are extended as in Table A.1. Each state corresponds to the transmission of a particular set of Request, FPath and DPath values. Table A.1 also lists the message that is generally sent in each particular state. If the message to be sent in a particular state deviates from the table below, it is noted in the footnotes to the state transition tables (see [IETF RFC 7271]).

Table A.1 – Extended states and protocol messages transmitted in the state

State	Description	Request(FP, P)
N	Normal state	NR (0, 0)
UA:LO:L	Unavailable state due to local LO command	LO (0, 0)
UA:P:L	Unavailable state due to local SF-P	SF (0, 0)
UA:DP:L	Unavailable state due to local SD-P	SD (0, 0)
UA:LO:R	Unavailable state due to remote LO message	Highest local request(local FPath, 0)
UA:P:R	Unavailable state due to remote SF-P message	Highest local request(local FPath, 0)
UA:DP:R	Unavailable state due to remote SD-P message	Highest local request(local FPath, 0)
PF:W:L	Protecting failure state due to local SF-W	SF (1,1)
PF:DW:L	Protecting failure state due to local SD-W	SD (1,1)
PF:W:R	Protecting failure state due to remote SF-W message	Highest local request(local FPath,1)
PF:DW:R	Protecting failure state due to remote SD-W message	Highest local request(local FPath,1)
SA:F:L	Switching administrative state due to local FS command	FS (1, 1)
SA:MW:L	Switching administrative state due to local MS-W command	MS (0, 0)
SA:MP:L	Switching administrative state due to local MS-P command	MS (1, 1)
SA:F:R	Switching administrative state due to remote FS message	Highest local request(local FPath,1)
SA:MW:R	Switching administrative state due to remote MS-W message	NR (0, 0)
SA:MP:R	Switching administrative state due to remote MS-P message	NR (0, 1)
WTR	Wait-to-restore state	WTR (0, 1)
DNR	Do-not-revert state	DNR(0, 1)
E::L	Exercise state due to local EXER command	EXER (0, x), where x is the existing DPath value when Exercise command is issued.
E::R	Exercise state due to remote EXER message	RR (0, x), where x is the existing DPath value when RR message is generated.
NOTE – FP = Fault Path, P = Path		

In order to avoid potential mistakes in duplicating the state transition tables from [IETF RFC 7271], the tables are omitted in this Recommendation.

See section 11.1 for the state transition by local requests and section 11.2 for the state transition by far end requests in [IETF RFC 7271]. For the 1+1 unidirectional switching, see section 11.3 of [IETF RFC 7271].

Note that the remote state transition table in [IETF RFC 7271] has been updated by Section 4.2 of [IETF RFC 8234].

Note that the description of the letter ‘i’ in the state transition tables has been updated. See Section 4.3 of [IETF RFC 8234].

Note that operator clear (OC) used in the state transition tables in [IETF RFC 7271] is the same as the "Clear" command in this Recommendation.

Appendix I

Operation example of MPLS-TP linear protection protocol

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

Operation examples of MPLS-TP linear protection protocol are shown in Appendix D of [IETF RFC 7271]. The examples are shown for the following scenarios:

(1) 1:1 bidirectional protection switching (revertive operation) – Unidirectional SF case,

(2) 1:1 bidirectional protection switching (revertive operation) – Bidirectional SF case – Inconsistent WTR timers, and

(3) 1:1 bidirectional protection switching – R bit mismatch.

Appendix II

Format of APC specific information

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

For the convenience of the reader, Figure 2 of [IETF RFC 6378] and Figure 1 of [IETF RFC 7271] are bound, and the format of the APC specific information with ACH is shown in Figure II.1.

<table>
<tr><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td><td colspan="8">4</td></tr>
<tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td colspan="4">0001</td><td colspan="4">Version (0)</td><td colspan="8">Reserved (0)</td><td colspan="16">Channel Type (0x0024)</td></tr>
<tr><td colspan="2">V (1)</td><td colspan="4">Request</td><td colspan="2">PT</td><td>R</td><td colspan="7">Reserved (0)</td><td colspan="8">Fault Path</td><td colspan="8">Data Path</td></tr>
<tr><td colspan="16">TLV Length (8)</td><td colspan="16">Reserved (0)</td></tr>
<tr><td colspan="16">Capabilities TLV Type (1)</td><td colspan="16">Capabilities TLV Length (4)</td></tr>
<tr><td colspan="32">Flags (0xF8000000)</td></tr>
</table>

Figure II.1 – Format of APC specific information over G-ACh

Appendix III
Initialization behaviour of MPLS-TP linear protection protocol

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

When MPLS-TP linear protection switching algorithm is (re-)initialized, including both cold and warm reboots, it should follow the initialization behaviour described in Section 4.1 of [IETF RFC 8234].

____