INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

COM 15 – LS 005 – E

English only

Original: English

Question(s): 3, 9, 10, 12, 14/15

LIAISON STATEMENT

Source: ITU-T Study Group 15

Title: Recommendation ITU-T G.8131 revision – Linear protection switching for MPLS-TP networks

LIAISON STATEMENT

For action to: IETF MPLS WG

For comment to: -

For information to: -

Approval: Agreed to by Question 3, 9, 10, 12, 14/15 joint meeting (Hiroshima, 28 January – 1 February 2013)

Deadline: 1 June 2013

Contact: Ghani Abbas (Q9)
Ericsson
UK

Tel: +44 7710 370 367
Email: Ghani.Abbas@ericsson.com

Thank you for the reply liaison in response to our liaison titled "Recommendation ITU-T G.8131/Y.1382 revision - Linear protection switching for MPLS-TP networks" (IETF MPLSL 81-E).

We provide here some further background material on linear protection for your information.

The APS mechanism used to provide linear protection is a vitally important tool for transport network operators and has been standardized by ITU-T SG15 for the existing transport technologies such as SDH, OTN, and Ethernet. The linear protection Recommendations for those different technologies go to great lengths to ensure a consistent operational approach. A consistent operational approach simplifies staff training and means that one body of knowledge and experience can be applied to the operation of linear protection across multiple transport technologies.

In addition to the case of separate transport networks employing different technologies being run by one operational staff the economically attractive multi-layer and multi-technology converged transport system requires operational consistency. If operational behaviour differs in the MPLS-TP layer of such a multi-layer converged network, the possibility of miss-operation and incorrect inter layer configuration leading to service outages is increased.

Table-1 shows the operational differences among related technologies (OTN APS, Ethernet APS and MPLS-TP PSC), based on our interpretation of your liaison response. As shown in the table,

there are differences between MPLS-TP PSC specified in RFC6378 and OTN APS and Ethernet APS which have been standardized by ITU-T SG15.

Technology	Base Document	Mechanism	Priority	EXER	SD	MS-W
OTN	ITU-T G.873	APS	SFP>FS	YES	YES	YES
Ethernet	ITU-T G.8031	APS	SFP>FS	YES	YES	YES
MPLS-TP	IETF RFC6378	PSC	FS>SFP	NO	NO	NO

Table 1: Operational differences between OTN APS, Ethernet APS, MPLS-TP APS

We discussed the responses in your liaison regarding RFC6378 'MPLS Transport Profile (MPLS-TP) Linear Protection' at our meeting in Hiroshima. We provide herein responses to each of the numbered 'additional notes' in that liaison and we also document one new issue. For your convenience in this liaison we use the same numbering as used in your response and add new numbers for the new issues. In the material below we refer, again for convenience, to RFC 6378 as PSC and to G.808.1/G.8031 as APS.

We request that you review our response below and provide us with your feedback on each issue. We look forward to working with you to complete this work.

1. RFC4427 is categorised as an informational RFC. It 'defines a common terminology for Generalized Multi-Protocol Label Switching (GMPLS) based recovery mechanisms'.

GMPLS uses an out of band control plane so while the terminology from RFC4427 is useful some of the concepts may not be applicable when PSC/APS is used in the data plane.

Furthermore we do not find a clear requirement that captures the FS->SF-P priority issue. Please indicate to us where this requirement is captured.

The definition of forced switch in G.870, which G.808.1 is as follows:

3.2.29 forced switch for normal traffic signal #i (FS #i): A switch action initiated by an operator command. It switches normal traffic signal #i to the protection transport entity, unless an equal or higher priority switch command is in effect. ***When an APS signal is in use, an SF on the protection transport entity (over which the APS signal is routed) has priority over the forced switch.***

We also believe the 'alternative approach' described in the second part of your response will be operationally unacceptable. The co-existence of SF-P>FS and FS>SF-P in the same protection domain could create operational confusion. Please clarify what you mean by 'co-existence'.

We do not find a response to question 1.c in our liaison to you. Please re-examine that question and communicate your observations to us.

2. Thank you for acknowledging the issue we described and confirming our analysis of it. . Our hope is that interested participants will submit the necessary Internet-Drafts to accomplish this in accordance with the normal IETF process.. As input to that process we define the problem in

Appendix 1 of this liaison. We believe it is a comprehensive enough statement to form the basis of an Internet-Draft.

3. We believe requirement R84 of RFC5654 is not yet addressed in the PSC RFC but can be satisfied by EXER functionality.

We believe that the exerciser functionality described in Appendix II could form the basis of an Internet-Draft. Our hope is that interested participants will submit the necessary Internet-Drafts to accomplish this in accordance with the normal IETF process.

4. Thank you for clarifying the issue. We believe that our original liaison defines the problem sufficiently to form the basis of an Internet-Draft. Our hope is that interested participants will submit the necessary Internet-Drafts to accomplish this in accordance with the normal IETF process.

We take this opportunity to clarify the difference between SD and MS. SD is an *event* raised by an equipment function to invoke protection and we will define how that occurs in our recommendations. SD does need to be included in the PSC protocol and we note that can be done even in the absence of the description of how it is raised.

MS-W is a required operator command as described in RFC6378, section 3.1. Its description is given in RFC4427, sec 4.13

5. Thank you for your clarification of this matter.

6. Thank you for this clarification. We believe that it is appropriate to have such functionality defined in our recommendations and will do so.

7. Mismatch behavior is described for APS in section 11.4 of G.8031 as follows:

a. Bridge Type: If the Bridge Type configured at each end of the service is not the same, a Failure of Protocol (FOP) is declared.

b. Bi-Directional verses Uni-Directional Protection: in case of mismatch, the service operates in Uni-Directional Protection Switching mode.

c. Revertive verses Non-Revertive Protection: in case of mismatch, the service operates in Revertive Protection Switching mode.

In order to allow the development of interoperable implementations we recommend that, in the event of mismatch in the configuration of protection switching mode between the two ends, the default protection switching mode as specified in b. and c. above be required by RFC6378 or some other appropriate document. Our hope is that interested participants will submit the necessary Internet-Drafts to accomplish this in accordance with the normal IETF process.

8. Thank you for acknowledging the issue and for your suggestion. We believe that our original liaison defines the problem sufficiently to form the basis of an Internet-Draft, we also provide a description in Appendix III. Our hope is that interested participants will submit the necessary Internet-Drafts to accomplish this in accordance with the normal IETF process.

9. Thank you for this clarification. We believe that it is appropriate to have FR functionality defined in our Recommendations and will do so.

“'Freeze' command should be implemented to prevent any switch-over action from being taken as defined in RFC4427. Such a command therefore freezes the state of the protection group including the signalling being transmitted. Until the freeze is cleared, additional near end commands are rejected. Condition changes and received PSC information are ignored. When the Freeze command is cleared (Clear Freeze), the state of the protection group is recomputed based on the condition and received PSC information.”

The MS-W command should be implemented and we note your guidance that it should be documented along with necessary protocol extensions in an Internet-Draft for consideration by the MPLS working group. Our hope is that interested participants will submit the necessary Internet-Drafts to accomplish this in accordance with the normal IETF process.

10 Priority of Clear SF in PSC (RFC6378)

There is a technical issue with the priority level of Clear SF in the PSC based MPLS-TP linear protection defined in RFC 6378 [1].

The priority level of Clear SF can cause traffic disruption when a node that has experienced local signal fails on both working and protection paths is recovering from those failures. We provide a detailed description of this problem in Appendix IV of this liaison. To progress our work on linear protection we would appreciate it if you could address this issue.

Appendix I

One of the differences between the APS and PSC protocols is the setting of the "Request/state" field in the protocol message. In the APS protocol, if the priority of the local request is lower than that of the remote request received from a far-end node, then the local request is not sent to the far-end node. In this case, the "Request/state" field in the APS message is always filled with NR, DNR or RR. This is a consistent behaviour, i.e. this principle is applied in any situation.

However, in the PSC protocol, the "Request" field in the PSC message reflects the local request even when the priority of the local request is lower than that of the remote request received from a far-end node for some conditions. For example, if a near-end node detects a SF on a working path (SF-W) while it is in the "Protecting Administrative (PA)" state due to a remote Forced Switch (FS) command issued at the far-end node, the near-end node reflects its current request (SF-W) in the "Request" field of the PSC message and starts to send SF (1,1) to the far-end node. However, if the near-end node detects a SF on protection path (SF-P) instead of SF-W in the above example, the near-end node does not reflect its current request (SF-P) in the "Request" field of the PSC message and keeps sending NR (0,1) as if there is no SF-P detected.

This inconsistent definition of the protocol can cause the "Request" field of the PSC message to contain incorrect information as shown in Figure 1 and results in an unintended situation.

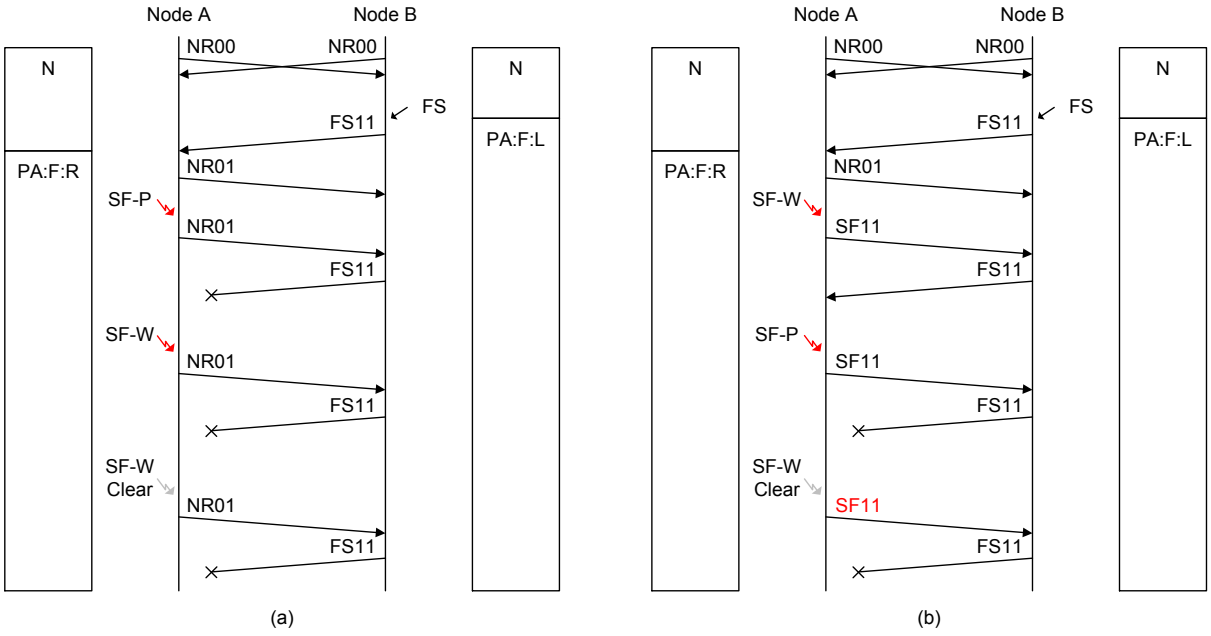

Figure 1

Figure 1(a) is the case where the PSC protocol operates as intended, and Figure 1(b) is the problematic case. The only difference between the two cases is the order in which SF-W and SF-P are detected at a node in PA:F:R state (Protecting Administrative state due to a remote FS).

In Figure 1(a), if node A detects SF-P while it is receiving FS (1,1) from node B, it ignores the detected SF-P and keeps sending NR (0,1). After that, if node A additionally detects SF-W, the detected SF-W does not enter to the PSC control logic because the priority of SF-W is lower than

that of SF-P, and node A keeps sending NR (0,1). Likewise, the SF-W clear event also does not enter the PSC control logic, and node A keeps sending the same message, NR (0,1).

On the other hand, in Figure 1(b), if node A detects SF-W first while it is receiving FS (1,1) from node B, the local request (SF-W) is reflected in the "Request" field of the PSC message, and node A starts to send SF (1,1) to node B. After that, if node A additionally detects SF-P, the detected SF-P becomes the highest local request and enters to the PSC control logic. However, the detected SF-P is ignored because node A is in PA:F:R state, and node A keeps sending the current PSC message, SF (1,1). Later, if SF-W is cleared, it does not trigger any action and node A keeps sending the same PSC message, SF (1,1). This means that node A is wrongly reporting SF-W through the "Request" field in the PSC message although there is no failure on the working path.

The mismatch between the "Request" field in the PSC message and the real local request can cause the protocol to operate incorrectly. Figure 2 shows a scenario after the case shown in Figure 1(b).

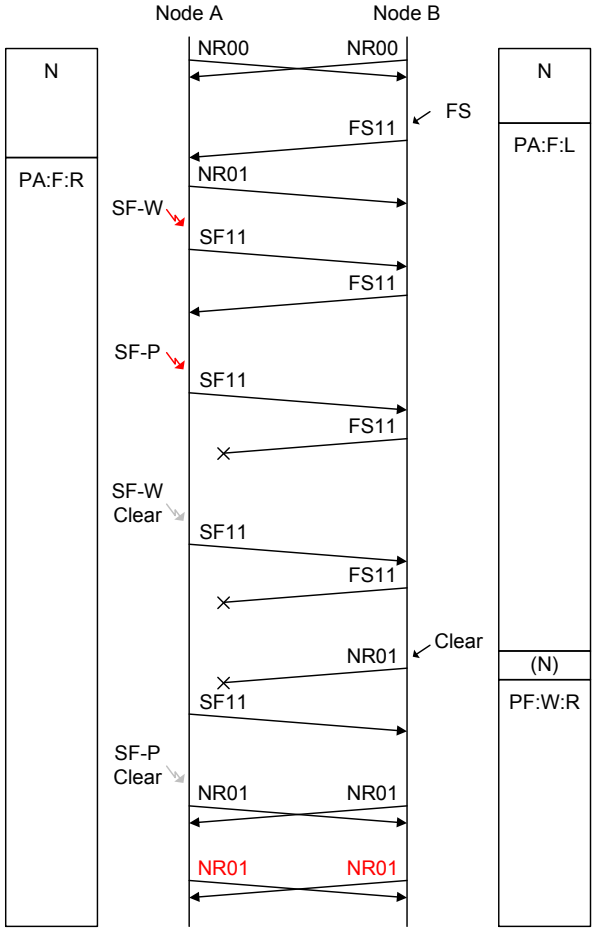

Figure 2

If an operator wants to resume the protection operation after SF-W is cleared at node A, he/she should issue a Clear command at node B to cancel FS command. The expected behaviour in this case is that both nodes goes into "Unavailable" state due to SF-P at node A and the normal traffic signal should be switched to the working path.

However, the current PSC protocol does not operate as expected. In Figure 2, if a Clear command is issued at node B, node B goes into Normal state as an intermediate state. Since the previous request

received from node A was SF (1,1), node B goes into “Protecting Failure (PF)” state due to a remote SF-W (PF:W:R), and starts to send NR (0,1) to node A.

The NR (0,1) is not delivered to node A because the protection path from node B to node A has failed. Later, if SF-P is cleared at node A, the SF clear event enters to the PSC control logic and node A starts to send NR (0,1).

According to the PSC protocol, the received NR (0,1) message is ignored when a node is in either PA:F:R or PF:W:R state. This means that both node A and B are sending NR (0,1) messages but remain on the protection path.

It is the expected and correct behaviour that in the revertive mode of operation, the normal traffic should be on the working path when there is no failure on the working path and no command requests to switch to the protection path..

Appendix II

This appendix indicates how IETF RFC6378 could be modified to address the Exercise function:

Exercise is a command to test if the APS 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 one can get a meaningful test by looking for a response.

In single-phased PSC protocol, the valid response to EXER message will be an RR with the corresponding FPath and Path signal numbers. The near end will signal a Reverse Request (RR) only in response to an EXER command from the far end.

The Exercise command shall be issued with the same requested and bridged signal numbers of the NR, RR or DNR request that it replaces. When Exercise commands are input at both ends, an EXER, instead of RR, is transmitted from both ends.

When the exercise command is cleared, it will be replaced with

— 1:1 bidirectional, revertive mode: NR if received PSC Request Field=NR, FPath=0, Data Path=0

— 1:1 bidirectional, revertive mode: RR if received PSC Request Field=EXER, Fpath=0, Data Path=0

— 1:1 bidirectional, non-revertive mode: DNR if received PSC Request Field=DNR, FPath=1, Data path=1

— 1:1 bidirectional, non-revertive mode: RR if received PSC Request Field=EXER, Fpath=0, Data Path=0

PSC Request field for Exercise as shown below:

(3) Exercise - indicates that the transmitting end point is exercising the protection channel and mechanism

The following priority inputs (9a, 9b) should be inserted:

```
9. WTR Expires (WTR timer)
```

9.a EXER

9.b RR

```
10. No Request (default)
```

PSC State Machine Tables

Part 1: Local input state machine

	OC	LO	SF-P	FS	SF-W	SFc	MS	WTRExp	Exercise
N	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i	E
UA:LO:L	N	i	i	i	i	i	i	i	i
UA:P:L	i	UA:LO:L	i	PA:F:L	i	[5]	i	i	i
UA:LO:R	i	UA:LO:L	[1]	i	[2]	[6]	i	i	i
UA:P:R	i	UA:LO:L	UA:P:L	PA:F:L	[3]	[6]	i	i	i
PF:W:L	i	UA:LO:L	UA:P:L	PA:F:L	i	[7]	i	i	i
PF:W:R	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	i	i	i
PA:F:L	N	UA:LO:L	i	i	i	i	i	i	i
PA:M:L	N	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	i	i	i
PA:F:R	i	UA:LO:L	i	PA:F:L	[4]	[8]	i	i	i
PA:M:R	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i	i
WTR	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	[9]	i
DNR	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i	[20]
Exercise	N	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i	i
RevReq	N	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i	E

extended states
E=Exercise
RR reverse request

State	REQ(FP,P)
E	EXER(0,0)
RR	RR(0,0)

[20] transition to E and send EXER(0,1)

Part 2: Remote messages state machine

	LO	SF-P	FS	SF-W	MS	WTR	DNR	NR	EXER	RR
N	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	i	RR	N
UA:LO:L	i	i	i	i	i	i	i	i	i	i
UA:P:L	[10]	i	[19]	i	i	i	i	i	i	i
UA:LO:R	i	i	i	i	i	i	i	[16]	i	i
UA:P:R	UA:LO:R	i	PA:F:R	i	i	i	i	[16]	i	i
PF:W:L	[11]	[12]	PA:F:R	i	i	i	i	i	i	i
PF:W:R	UA:LO:R	UA:P:R	PA:F:R	i	i	[14]	[15]	N	i	i
PA:F:L	UA:LO:R	i	i	i	i	i	i	i	i	i
PA:M:L	UA:LO:R	UA:P:R	PA:F:R	[13]	i	i	i	i	i	i
PA:F:R	UA:LO:R	i	i	i	i	i	DNR	[17]	i	i
PA:M:R	UA:LO:R	UA:P:R	PA:F:R	[13]	i	i	DNR	N	i	i
WTR	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	[18]	i	i
DNR	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	i	[21]	DNR
exercis	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	i	i	i
RevReq	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	i	E	N

[21] transition to RR and send RR(0,1)

Appendix III

Let us assume that two end nodes are operated in revertive mode and are experiencing a bidirectional signal fail on working path (SF-W).

When two end nodes clear the SF-W simultaneously right after transmitting SF(1,1) messages, each node transmits WTR(0,1) message and enters in the WTR state. Due to the propagation delay from the remote node to the local node, the SF(1,1) message transmitted from the remote node just before the Clear SF-W event can arrive while the local node is in WTR state.

When SF(1,1) message is arrived, the local node stops the WTR timer, transmits NR(0,1) message, and enters in a remote SF-W state, which is defined as (PF:W:R) state in RFC6378.

When WTR(0,1) message is arrived, according to the state transition defined in RFC6384, the local node make transition to WTR state and continue to send the current messages, which is NR(0,1) messages.

Now, the WTR timer has been cancelled, each node is in WTR state and keep sending NR(0,1) messages. The reversion is failed.

The sequence diagram of the aforementioned scenario is depicted in Figure 1.

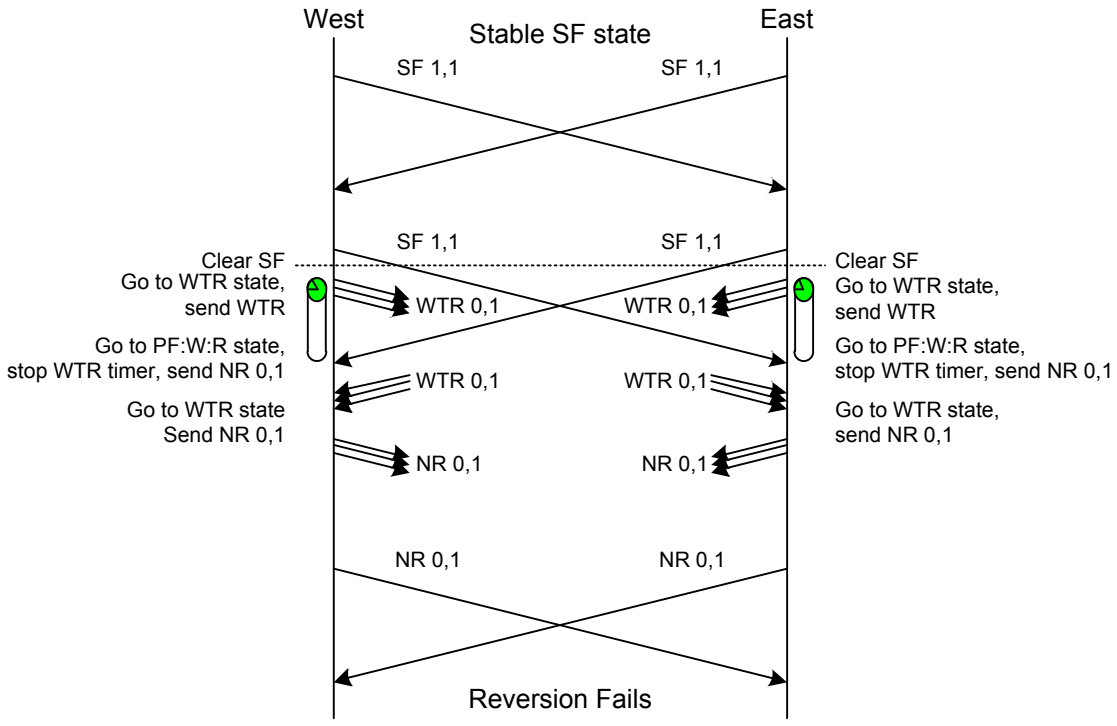

Figure 1. Reversion fails on simultaneous clear SFs

The "simultaneous clear SFs" in this Appendix means the two clear SF events at both ends occur within the propagation delay of the SF message from one end to the other end. It does not mean the two clear SF events occur exactly at the same instance.

Appendix IV

Table 1 shows the priorities of local requests as defined in the PSC RFC [1].

Request	Priority
Clear (operator command)	Highest
Lockout of protection	
Forced Switch	
Signal Fail on Protection	
Signal Fail on Working	
Signal Degrade on Working	
Clear Signal Fail/Degrade	
Manual Switch	
WTR Expires	
No Request	Lowest

Table 1. Priority list of local requests as defined in the PSC RFC.

The priority level of Clear SF can cause traffic disruption when a node has experienced a local signal fail on both working and protection paths and is recovering from these failures.

In Figure 1, a sequence diagram is depicted for the case of bidirectional signal fails. However, other cases with unidirectional signal fails can result in the same problem.

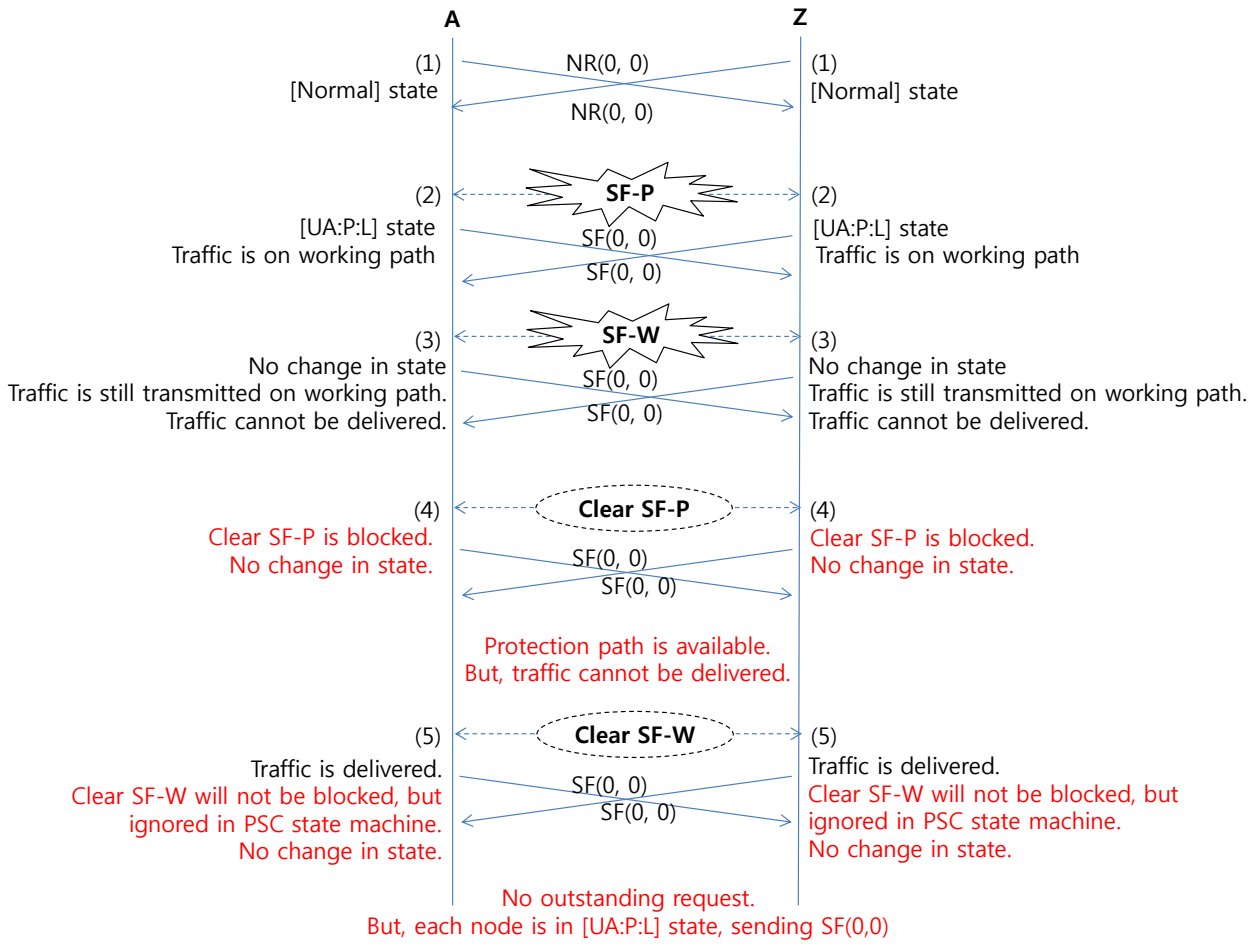

Figure 1. An example of sequence diagram showing the problem with the priority level of Clear SF

(1) There is no outstanding request and each end is in Normal state.

(2) When signal fail on protection (SF-P) occurs, each node enters into [UA:P:L] state, which means that the protection path is unavailable due to local SF on the protection path. Traffic is on working path.

(3) When signal fail on working (SF-W) occurs, each node remains in [UA:P:L] state as SF-W has a lower priority than SF-P. Traffic is still on the working path. Traffic cannot be delivered as both working and protection paths are experiencing signal fails.

(4) When the signal fail on protection is cleared, local “Clear SF-P” request cannot be presented to the PSC control logic, which takes the highest priority local request and runs PSC state machine, as the priority of “Clear SF-P” is lower than that of SF-W. Consequently, there is no change in state, and the selector and/or bridge keep pointing at the working path, which has signal fail condition.

Now, traffic cannot be delivered while the protection path is recovered and available.

It should be noted that the same problem will occur in the case that the sequence of SF-P and SF-W events is changed.

If we further continue with this sequence to see what will happen after SF-W is cleared,

(5) When the signal fail on working is cleared, local “Clear SF-W” request can be passed to the PSC control logic (state machine) as there is no higher priority local request, but this will be ignored in

the PSC control logic according to the state transition definition in the PSC RFC. There will be no change in state or protocol message transmitted.

As the signal fail on working is now cleared and the selector and/or bridge are still pointing at the working path, traffic delivery is resumed. However, each node is in [UA:P:L] state and transmitting SF(0,0) message, while there exists no outstanding request for protection switching. Moreover, any future legitimate protection switching requests, such as SF-W will be rejected as each node thinks the protection path is unavailable.

_____