Reply to ITU Liaison Statement regarding MPLS-TP Linear Protection

The MPLS WG would like to acknowledge your LS (ITU COM 15 – LS 393 – E) regarding "Revision of Recommendation ITU-T G.8131 – Linear protection switching for MPLS-TP networks" and would like to continue the cooperation on this topic to complete the recommendations for linear protection in MPLS transport networks.

Regarding the comments and differences that were pointed out in your LS between existing APS protocols that have been developed by the ITU for other technologies and the PSC protocol defined for MPLS-TP in RFC6378 and that were raised in your LS we have the following feedback:

1. Regarding the higher priority of Forced Switch (FS) over Signal Fail on Protection (SF-P) – This order was defined to provide the function requested by Service Providers and for consistency with the IETF Recovery terminology as defined in RFC 4427. Specifically, RFC 4427 Section 4.13 clause defines "Forced switch-over for normal traffic", which is executed "unless an equal or higher priority switch-over command is in effect". Clause E defines "Manual switch-over for normal traffic", which is executed "unless a fault condition exists ... or an equal or higher priority switch-over command is in effect."

   Thus, RFC4427 differentiates between switch-over commands, i.e. lockout of protection, forced switch, manual switch, etc, and fault conditions, i.e. SF-W, SF-P, etc. Since an FS is executed unless there is a precluding switch-over command, and since MS is executed unless there is a precluding switch-over command or a fault condition, the FS must be executed even in the face of a fault condition. This requires that FS take precedence over SF-P.

   Additionally, the priority ordering defined for PSC allows a Forced Switch to be executed even in the face of SF-P, which is the difference between FS and a Manual Switch (MS). It is our understanding that Service Providers wish to have the option to control their networks regardless of the automatic switching protocol that is in operation and this requires that FS has the highest priority. We believe that one of the motivators in APS for SF-P having a higher priority than FS is to allow coordination of the reversion operation between the two endpoints in the presence of FS when the protection path is blocked. We consider that this requirement should be secondary to the delivery of the operator's specific FS request.

2. Regarding the point that APS uses a "no request" to suppress the local status and thereby inform the far end that its higher priority request is being acted upon – PSC also includes a mechanism to inform the far end of the consistency of the behavior based upon the coordination of the Path field. This mechanism is simpler than the one used in APS and operates by supplying the local status at all times so that the operator is able to get a more complete picture of the status of the network. This behavior may be beneficial to network operators and allow for future operational sophistication and flexibility.

3. Regarding the EXER function – This comment was raised during the IETF Last Call and was discussed with the individual that raised the comment. As a result of this discussion an

appendix (Appendix B) was added that suggests various ways of implementing the functionality that is required.

4. Regarding difference of priority between local and remote triggers – Our analysis that was conducted during the definition of the protocol did not indicate any different behavior for PSC as opposed to APS (G.8031 in particular) in this area and we await the results of your "further analysis".

5. Regarding priority of requests – PSC assigns priority to inputs that are either local triggers or remote requests as described in Section 4.3.2 of RFC6378 that seem to be the equivalent of "requests" in APS. During the analysis of the state transitions that was conducted in the development of RFC6378 no difference in behavior was identified. If you can identify for us a particular use case where the protection behavior is different, we will be able to address the issue specifically.

6. Regarding reporting of failures – RFC6378 does point out that when an inconsistency of the protocol is identified (see Sections 4.2.3 and 4.2.4) that a management alarm should be invoked. There is no complete definition of which alarm to invoke, because it was felt that this be best specified in a management document.

7. Regarding type mismatches – Section 4.2.4 of RFC6378 states "If there is an inconsistency between the two end points, i.e., one end point is configured for revertive action and the second end point is in non-revertive mode, then the management system SHOULD be notified." Could you indicate where the text that implies that the "service is not protected" appears in the RFC?

We hope that this addresses your concerns and can be used as the basis for the continued cooperation in the development of a consistent linear protection definition to the benefit of the industry.