Comment Disposition Tracking: Survivability Framework

http://tools.ietf.org/html/draft-ietf-mpls-tp-survive-fwk

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
1	Section 4.7	Title for section 4.7 is meshed networks but the description focuses on linear protection	Introduce new sections for use of linear protection in meshed networks and uses of other protection schemes in meshed networks	The review comment does not propose any new text. Section 4.7 is intended to consider protection techniques that can be applied in mesh networks. There are already subsections for various techniques of protection in meshed networks (linear protection, p2mp protection, shared mesh protection). The editors believe that all mechanisms have been covered and since the comment has not suggested any other protection techniques for use in mesh networks, this comment is not actionable.	OK
2	Section 4.3.2	The clarification of shared protection (4.3.2) is confusing since Shared mesh is overlaps with section 4.7.6 and e-e shared is introduced (added in 05 version), but n:m is not req in RFC5654 as described just before the e-e shared paragraph. Why is this paragraph is required? There are two types of protection (path or segment by shared).	1. Rename section 4.7.6 as “Shared Protection in Meshed Networks” 2. Rings do offer shared protection and thus should be mentioned	There is a very significant difference between the general concept of "shared protection" and the specific technique of "shared mesh protection". = "Shared protection" as a general technique can be applied in rings, mesh networks, and so on. Section 4.3.2 describes the general concept of shared protection. = "Shared mesh protection" can only be applied in mesh networks. This is why it is described only in a subsection of Section 4.7. The proposed rename of Section 4.7.6 would not be accurate as the section only describes shared mesh protection. It is noted that, as you remark, ring protection can share protection resources. Section 4.3.2 does not currently make reference to any topologies or protection techniques. We have added the following text to the end of paragraph 1 of Section 4.3.2: Shared protection can be applied in different topologies (mesh, ring, etc.) and can utilise different protection	In packet networks such as MPLS-TP the “degree” of sharing and the policy for sharing a resource are established when a protection path is set-up or when a new path is established for restoration. This should be described as above.

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
				mechanisms (linear, ring, etc.).	
	Section 4.7.2	Previous comment 63 resolution is notclear.	Last paragraph is ambiguous since reversion should be to the working channel rather than to working traffic, if reversion is enabled	We have deleted the words "the traffic from" from this paragraph.	OK
3	Section 4.7.4	The para starts.. An in-band, data-plane protocol is defined in [MPLS-TP-Linear-Protection] for this purpose.	Delete referencing a work in progress and in particular in the two sentences.	This comment is correct. The framework should not assume the solution provided in the current version of the document is complete. However, the framework can usefully indicate to the reader the correct place to look for the description of specific mechanisms. Therefore we have replaced the sentence as follows: An in-band, data-plane protocol for use in MPLS-TP networks will be documented in [MPLS-TP-Linear-Protection] for this purpose.	1. An in-band protocol is also required for Ring protection as well as for Linear protection: The modified text presumes that we will have different protocols (documented in different drafts). Given that, a more generic statement such as: "An in-band data-plane protocol is required to support protection switching in MPLS-TP networks. The definition of this protocol is for further study." Would be more appropriate. 2. ITU-T recommendations will make normative references to this RFC, so we must avoid any language such as "is defined in draft-work-in-progress" since this will force us to make the referenced draft a normative secondary reference when we complete the A.5 TD. This will block consent. The text proposed above will avoid this. Under the ITU-T A.5 rules we can not refer to draft documents.
4	Section 4.8	What is meant by interoperability? "Ensure complete interoperability with the mechanisms defined for arbitrary topologies to allow end-to-end protection". Protection domains are either nested or concatenated but not arbitrary overlapping	We propose deletion.	This document is obviously dependent on the MPLS-TP requirements documented in RFC 5654 and approved for publication by the ITU-T. We cannot rescind any of the requirements set out in that document. Requirement 91 of RFC 5654 states: 91 MPLS-TP MAY support recovery mechanisms that are optimized for specific network topologies. These mechanisms MUST be interoperable with the mechanisms defined for arbitrary topology (mesh) networks to enable protection of end-to-end transport paths.	We support your clarification of interoperability. In addition to that we propose to add some generic material regarding survivability strategy principles earlier in the document to provide an overall context. This could be inserted at the end of Section 1.1, then this generic text can be referred to from the end of second paragraph of Section 4.6 in v06: Proposed text: -- -- "The goal of a network survivability strategy is to maintain an

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
				See Section 4.6 of this draft for how this requirement is first captured in the survivability framework, and where the purpose of this requirement is clarified. In order to clarify the meaning of "interoperability", we have added the following sentence to the second paragraph of Section 4.6: In this context, 'interoperate' means that the use of one technique must not inhibit the use of another technique in an adjacent part of the network for use on the same end-to-end transport path, and must not prohibit the use of end-to-end protection mechanisms. We have added a reference to see R91 of [RFC5654] in Section 4.8.	acceptable level of end-to-end service performance during network and/or equipment fault(s). Survivability mechanisms can be deployed on an end-to-end basis, in a cascaded and/or nested manner, or involve a combination of these approaches. Major factors influencing the survivability architecture chosen include time in which the service is restored, traffic patterns, topology and types of faults. o End-to-end survivability supports end-to-end transport network survivability using a single mechanism. o For cascaded survivability the mechanisms are typically deployed in a chain, and each protection domain supports a particular survivability mechanism and protects only the faults that occur within its domain. o For nested survivability, multiple survivability mechanisms are deployed within a single domain that can protect against the same fault; such nesting is typically restricted to two mechanisms (often designated the primary and secondary “levels of defense”). In all cases, it is essential that a survivability strategy assures that each protection domain can appropriately perform its function - i.e., does not react to, or interfere with, failures occurring in other protection domains.” -- --
5	Section 4.1.1	Rather Wooly. Operator control uses the term “recovery action”.	1. Replace title with “Operator Commands” 2. Replace the following sentence “The operator can also be given control of recovery actions and” by “ The operator has	The editors feel that "Operator Control" is a wider term than "Operator Commands." The latter is a subset of the former. As explained in the first paragraph of Section 4.1.1, this section covers two elements of operator control: policies and actions. Changing the title as suggested would be confusing and would hide the element of policy discussed in this section. With regard to the second point in this comment, there are some issues with your proposed substitution (for example, we need to say "recovery" not "protection"). We have	Ok for point 1. Regarding point 2: we suggest the following text: -- -- “The operator can also issue commands to control protection actions and events as defined in G.808.1. Alternate (close to equivalent) actions can be performed for recovery actions and events.” ITU-T Recommendation G.808.1 defines generic linear protection (not restoration) for transport networks. It covers

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
			commands to invoke protection switching."	substituted the following sentence which we believe captures your comment while retaining the original intent of the text: The operator can also issue commands to control recovery actions and events.	wider protection schemes and transport netrwork objectives and this is the reason it is an appropriate reference -- --
6	Section 4.1.2	Last paragraph "This behavior ..". Management and control planes involvement are not needed.	Delete	Resolved as requested.	OK
7	Section 4.1.3	"Hover, in this context we are concerned with the use of these messages to control or trigger survivability actions".	1. Amend to read "However, in this context these messages are used to control or trigger survivability actions". 2. add exchange to OAM messages to read "OAM messages exchange"	Resolved as requested.	OK
8	Section 1.4	Requires clarification: the term "levels of protection". What is "level", transport layers, QoS levels, or SD levels?	Define the term level	This is a difficult comment to resolve. "Level" is a normal word in the English language and, indeed, you use it in your own text. When you ask if we mean "QoS level" you do not expect us to respond: what do you mean by "level" in this phrase? Our initial reaction was to assume that adding some examples would help to resolve your comment, but we see that the existing text already includes examples: The framework also describes the qualitative levels of the survivability functions that can be provided, such as dedicated recovery, shared protection, restoration, etc.	Your answer implies that "level" is used in the context of "type or mechanism". It may be more appropriate to relate "level" to availability and indicate that it is possible to use multiple protection types or mechanisms (e.g. segment protection plus nested end to end restoration) to improve the overall availability. We propose to replace "level" by "type" in the appropriate places.

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
				We cannot find any other way to clarify this, but we are open to suggestions.	
9	Section 2	Editorial: "the distinction and definitions made in [RFC4427] for the following three terms": Protection, Restoration, and Recovery. The column of "Restoration" is duplicate	Edit	Resolved as requested.	OK
10	Section 4.7.4	Too many details about specific mechanisms which are assumed to be in a solution draft.	Clarify	See also the resolution of your comment 3. There seems to be very little mention of solutions in this section. Most of the text refers to abstract mechanisms (such as CCV). Probably you are referring to the last two paragraphs in the section. The first of these is addressed per your comment 3. The second paragraph observes that the control plane can be used to provide some of the functions required (while noting that there are limitations to this) and since the control plane for MPLS-TP is already defined as being GMPLS, it gives reference to the existing GMPLS work. It is the purpose of a framework document to point at existing work. We have made some minor clarifications to the final paragraph to show that this paragraph is about the control plane.	Use the same text as proposed in comment 3 above.
11	Section 12.2	MPLS-TP-Linear-Protection] in the reference part is draft-ietf-mpls-tp-linear-protection, but a lot of issues are raised about this draft, in that case it is not proper to take draft-ietf-mpls-tp-linear-protection as the solution draft.	Do not reference documents that are not pre-existing RFCs as in some instances they pre-judge the solutions	The reference you mention is included as an Informative Reference. This is perfectly proper. You are correct that the solution contained in the current version of this document is not necessarily the final one that will be published as an RFC (see your comment 3, for a resolution of this issue). However, the solution adopted for linear protection in MPLS-TP will be published in the referenced document – it may be that the solution will be updated if there is discussion on the MPLS-TP mailing list. We would like to encourage you to continue to discuss the linear protection	Remove the referene to draft-ietf-mpls-tp-linear-protection (see comment 3 above) Remove references that assume or pre-judge solutions

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
				solutions on the MPLS-TP mailing list. We have made no change for this comment.	
12	Section 4.8	Requires clarification: "Reuse existing procedures and mechanisms for recovery in ring Topologies" . What is meant by "existing": are they the current ring protection mechanisms?		A good observation. Thank you. We should defer to RFC 5654 for this material. We have made substantial deletions and updated the text to read: The architecture and the mechanisms for ring protection are specified in separate documents. These mechanisms need to be evaluated against the requirements specified in [RFC5654] which includes guidance on the principles for the development of new mechanisms.	ok
Referring to previous comments (TD283/WP3)					
Gen 4	Fault isolation	This draft refers to fault isolation in a protection switching draft. Consequently, a reference should be made to the draft that describes the mechanism for fault isolation.		The only reference to isolation is in Section 6.3. In response to your previous comment, we changed the document to discuss "Fault Localization", and the remaining mention of isolation is intentionally specific to the process of isolating a specific location. There are no other references to fault isolation, so we cannot process your comment. We note that Section 6.3 ("Fault Localization") makes forward references to Section 6.4.3 for OAM mechanisms and to Section 6.5.3 for control plane mechanisms	OK
Gen 5	MTTR	MTTR is any repair time from sub-50 ms to as you mention "truck roll". It is used in determining the 5 nines of availability. So MTTR is certainly relevant		We do not disagree with you assertion about the importance of MTTR in providing availability for services carried over network. We believe that availability is built on a number of components including repair and recovery. This document is limited to a discussion of recovery. Repair techniques are out of scope for protocol specifications and, while they may be taken into account when provisioning networks or planning services, they are outside the scope of this document.	OK
	Section 4.3	Section 4.3 still mentions "cost", it should be deleted.		We assume you are referring to the original comments ItaloBus40 and ItaloBus41.	OK

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
				Your new comment is in error. The original comments were addressed and there is now no mention of "cost" in Section 4.3.	
63	Section 4.6.1.1	The text you have indicated refers to the restoration of the traffic, not to reversion. In the case of 1+1 protection, when the fault is repaired, the traffic is restored to the broken path (the old working path). It is then a choice whether there is reversion or not. No, when you restore the traffic to the broken path after repair you already revert to the original situation. In case non-reversion is provisioned the traffic is *NOT* restored to the broken path.		Section 4.6.1.1 is no longer a section in this document. We believe you are referring to Section 4.7.2 in the version of the document that you reviewed. Thank you for your comment. We have updated the final paragraph of the section to use tighter language and address your comment as follows: In both protection schemes, traffic flows end-to-end on the working entity after the conditions causing the switchover have been cleared. Data selection may return to selecting traffic from the working entity if reversion is enabled, and will require coordination of the protection state between the edges of the Protection Domain. To avoid frequent switching caused by intermittent defects or failures when the network is not stable, traffic is not selected from the working entity before the Wait-to-Restore (WTR) timer has expired.	OK
Comments on new text in draft-ietf-mpls-tp-survive-fwk-06					
A	general				Terminology of Span and Link According to the Rosetta stone span is synonymous with link. We propose to use consistently the same term for span recovery and/or link recovery in this draft. Currently, the document uses inconsistently span and link. This will cause confusion as they may give the perception that they are different. We suggest the use of only one of the terms throughout the document.
B	Section 4.2				We propose to keep the title the same as section 4.4 of RFC4427: “Recovery scope”

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
C	Section 4.2.1				The last paragraph of 4.2.1 states that in some cases span recovery is a type of segment recovery. 1. The difference between span (link) and segment recovery should be described. The text in the document implies that there is a difference between some types of span recovery and segment recovery. If this is the case we are asking the question please tell us. 2. The relationship between the Sub-Path Maintenance Entity (SPME) defined in the MPLS-TP Framework and Span Recovery as well as Segment Recovery should be described.
D	Section 4.3				Levels of Recovery This section describes the resource allocation for LSPs and also restoration and revertive-protection. There is one piece missing in MPLS-TP framework draft. It's about resource allocation during setting up of LSPs including both working LSPs and protection LSPs. Setting up LSPs and selecting protection/restoration scheme for the LSPs should be network planning and resource management issue. Proposed text" "Setting up LSPs and selecting a protection/restoration scheme for the LSPs using available resources sholud be a network planning (add ref) and a resource management (add ref) issue" .
E	Section 4.3.3				New text for extra traffic: It is our opinion that support for extra-traffic introduces extra complexity to the APS protocol (e.g., it requires a two-phase instead of a one-phase protocol exchange) on that basis it should be a non-normative requirement. We propose that the text starting with "This document

ITU-T Liaison Response (May 5) https://datatracker.ietf.org/liaison/889/				IETF Disposition (June 4) https://datatracker.ietf.org/documents/LIAISON/file1041.doc	Comment on Disposition (referring also to http://www.ietf.org/id/draft-ietf-mpls-tp-survive-fwk-06.txt)
#	Section	Comment Text	Proposed Resolution	Disposition	Proposal
					observes that extra traffic…" is moved to a non-normative Annex or Appendix. The intention is to make it clear that "Extra traffic" feature is not an option **.**
F	Section 4.3.3				This section states: "A protection tunnel is a hierarchical LSP". A tunnel is not an LSP, this should be corrected to align with the change from PST to SPME in the MPLS-TP Framework draft. The identifiers draft states that a LSP is named from the tunnel in which it resides so if the tunnel is the LSP how can the LSP name itself. The framework draft changed the term PST to SPME to avoid this confusion, the Survivability draft should make a similar change.
G	Section 4.4				The title is "Mechanism for protections", however this Section describes link-level protection, alternative path and segment and protection tunnels. These are not protection mechanisms but descriptions of protection in different MPLS-TP layers. A more appropriate title would be: "Protection layering"
H	Section 6				Describes in detail fault detecting, fault localization, fault reporting and testing for faults. These are all described in the OAM framework draft and out of scope for this draft, please refer to the OAM Framework draft. "It should be possible to take protective actions in a protection domain based on faults detected in the protection domain by the OAM mechanisms described in draft-OAM-framework."