Question(s): 12/15

**LIAISON STATEMENT**

Source: ITU-T Study Group 15
Title: Review of draft-ietf-mpls-tp-data-plane-03 (Ref #035.01)

**LIAISON STATEMENT**

For action to: IETF IESG
For comment to: IETF MPLS WG
For information to:

Approval: Agreed to at SG15 meeting (Geneva, 31 May – 11 June 2010)
Deadline: 30 July 2010

Contact: Malcolm Betts
ZTE
PRC
Tel: +1 678 534-2542
Email: malcolm.betts@zte.com.cn

ITU-T SG15 thanks the IETF MPLS WG for the liaison “Response to comments in LS173 - Comments on draft-ietf-mpls-tp-data-plane-02”. We accept the resolution of the first comment, however we have on additional comment and an alternative proposal for our original comment on the security section which are provided below.

We request that you address these comments and provide us a final version of the text that will be approved so that we can reach consensus to include this as a normative reference in draft revised Recommendation G.8110.1. WP3 has tentatively planned to hold an interim plenary meeting to consent G.8110.1 in November 2010.

---

MPLS
Internet-Draft
Intended status: Standards Track
Expires: November 13, 2010

MPLS Transport Profile Data Plane Architecture
draft-ietf-mpls-tp-data-plane-03

3.2. Sections
This change is intended to clarify that providing a multiplexing capability for a section layer is optional.

A section MAY be required to provide a mechanism for multiplexing MPLS with other protocols MUST provide a means of identifying the type of payload it carries. If the section is a data-link, link-specific mechanisms such as a protocol type indication in the data-link header MAY be used. If the section is an LSP, this information MAY be implied by the LSP label or, if the LSP payload is MPLS-labeled, by the setting

6. Security Considerations

This change is intended to clarify the difference between the peer and a neighbour, it also provides a description of the application scenario.

2. Any MPLS label processed at the receiving LSR, such as an LSP or PW label, has a label value that the receiving LSR has previously distributed to the peer (in a common sub-layer) beyond that immediate neighbour, the specific scenario being when labels for more than one sub-layer in the hierarchy has been allocated from a common label space AND the sub-layer of receipt does not correspond to the sub-layer of label distribution for the specific label value (i.e., when it is known that the path from the system to which the label was distributed to the receiving system is via that neighbour).

Further details of MPLS and MPLS-TP security can be found in [I-D.ietf-mpls-tp-framework] and [I-D.ietf-mpls-mpls-and-gmpls-security-framework].