PBB-TE Segment Protection Requirements:

Focus on the Distinction between *Infrastructure* Segment Protection and *Data Path* Segment Protection

Bob Sultan (bsultan@huawei.com)
Ben Mack-Crane
Deng Zhusheng

March 2009 IEEE 802.1 Plenary Vancouver, BC, Canada

Purpose of this Presentation

- Two distinct protection types have been introduced under the heading of Segment Protection;
- These are _Infrastructure_ Segment Protection (ISP) and _Data Path_ Segment Protection (DPSP);
- At the last meeting, it was suggested that the two types (and associated solutions) could be evaluated in separate charts;
- This would allow work on the two types to proceed without confusion;

Purpose of this Presentation (continued)

- This will also simplify each chart by reducing the number of columns needed to compare solutions;
- For each of the two types, an independent evaluation can be made as to the requirements and solutions;
- If both types are to be addressed, they are sufficiently similar to be grouped in the same PAR and described in a single amendment;
- This presentation is intended to verify that people have a common understanding of the two types of segment protection.

Infrastructure Segment Protection
# (1 hop example)
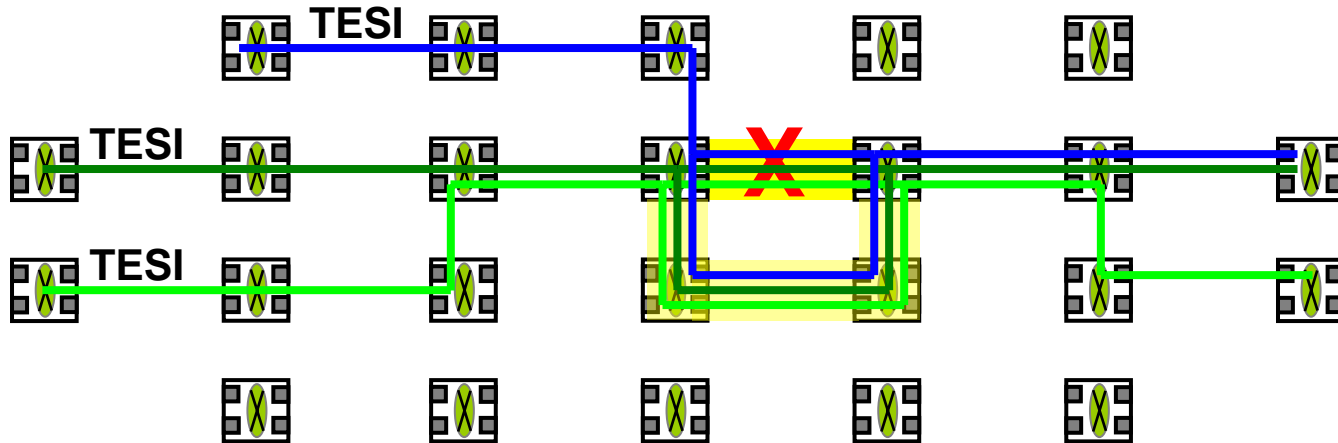
- Provision *segment* of network to be protected;
- Provision *backup* segment providing protection;
- Detect failure on protected segment;
- TESIs carried on backup segment.
- Protect specific link prone to failure due to flood, earthquake, vandalism, etc.

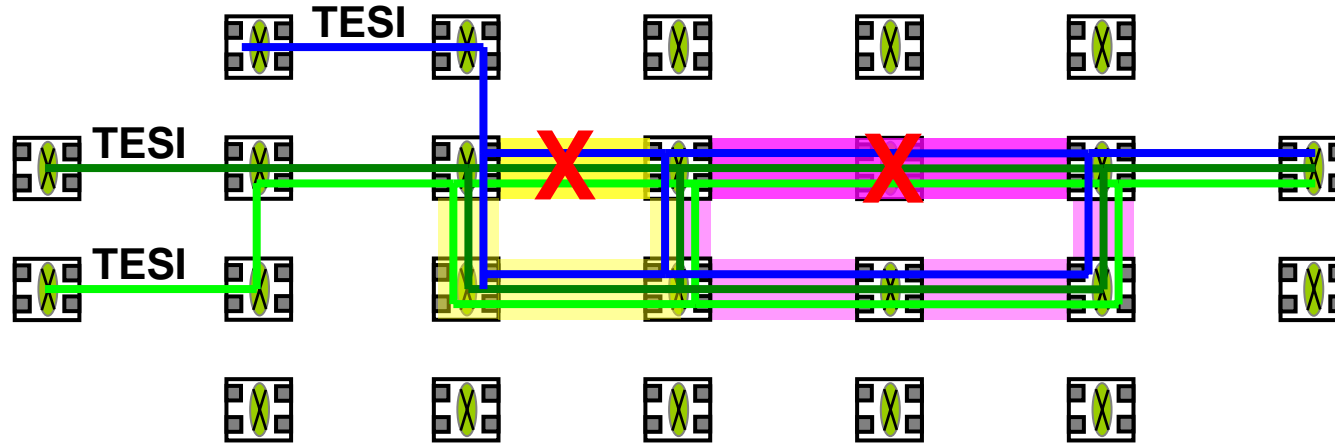# Infrastructure Segment Protection
(2 hop example)
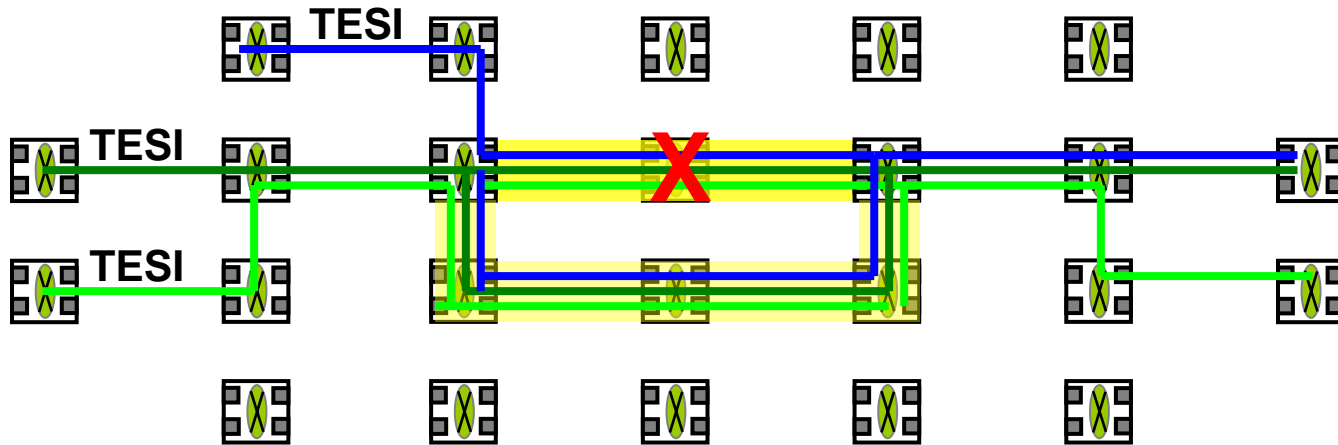
- Protects against failure of a specific segment of the network, including failure of a bridge;
- Protects set of TESIs crossing the segment;

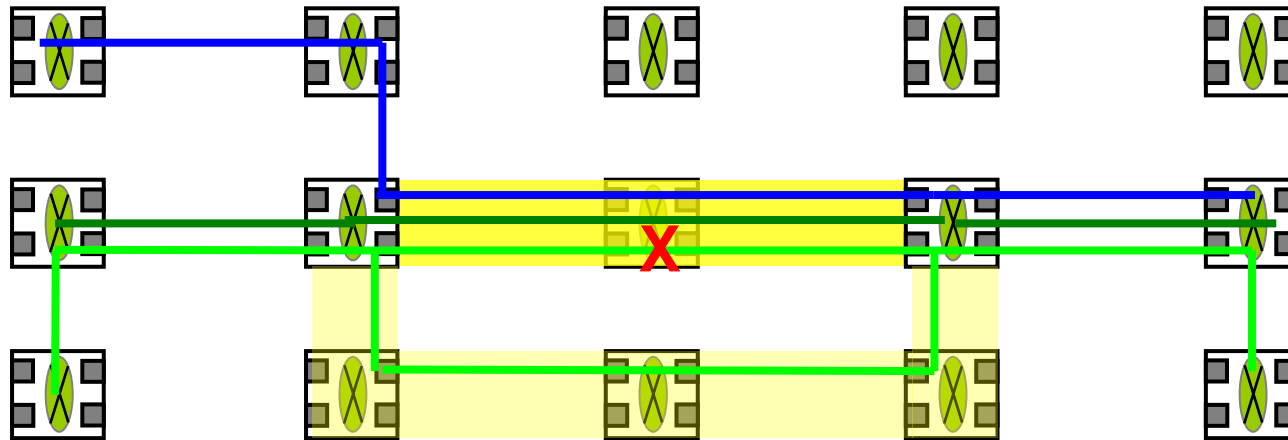# Independent Segment Protection Domains
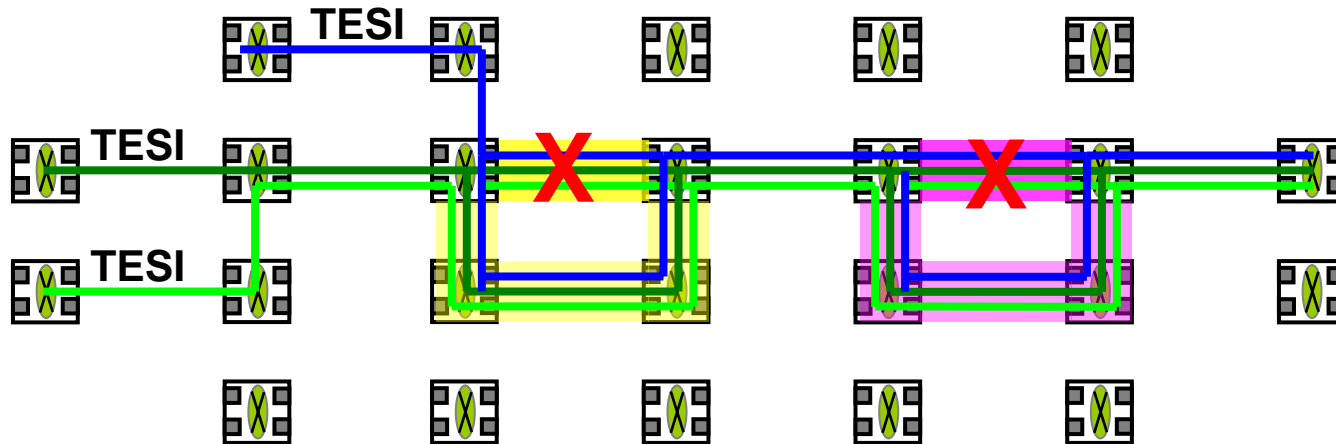
- Provision *independent* protection domains
- TESIs survive failure in *each* domain

Adjacent Segment Protection Domains

- Provision *adjacent* protection domains
- TESIs survive failure in one domain
- TESIs survive failure in both domains
- NOTE: The figure shows 'no backtracking' when both segments fail. While this improves performance and may be necessary with some solutions, this is not a requirement.

Data Path Segment Protection

- Provision segment protection domain
- Fault in FDB or other provisioning fault affecting an individual TESI
- *Only failed TESI* shifted to backup segment
- Requires monitoring *each individual* TESI at segment endpoints

Two Distinct Segment Protection Functions

1. *Infrastructure:* Protect *all* traffic (TESIs) associated with a protected segment from a failure of that segment. After failure, traffic is carried on the backup segment (requires monitoring *per segment*)

2. *Data Path:* Protect *each* TESI associated with a segment from a failure of *that TESI* within the segment. After failure, traffic associated with the failed TESI(s) is carried on the backup segment (requires monitoring *per TESI* associated with the segment)

•   We do *not* currently see a strong requirement for Data Path Segment Protection but we certainly invite more data on this.

And now….

- **Does anyone have questions about the difference between *Infrastructure* Segment Protection and *Data Path* Segment Protection as described?**

Infrastructure Segment Protection Solutions

- **Redirection**: change FDB outbound port value; one advantage is that frame is not modified;
- **Triple MAC** (client/server):   segment endpoints deploy BEB function; segments appear as TESIs; 1:1 TESI protection is deployed; this probably requires little or no new standards content; cost of two MAC encapsulations;
- **Triple Q**: stack additional VLAN tag; requires frame modification; reduces number FDB entries required as forwarding is determined by VID; requires additional tag.

Infrastructure Segment Protection Benefits

- Address the relatively high failure rate of particular links or bridges within a network.
- Address the likelihood of concurrent failures occurring in different segments of a network.
- Allow maintenance activities to be performed independently in different segments of the network.
- Allow maintenance activities to be performed in one segment of a network without disabling protection in another segment.
- Localize changes in traffic distribution due to failure or maintenance actions.
- Provide an efficient means of protecting portions of a PtMP TESI.

Requirements Still In Discussion

- **Degree of end-to-end integrity required**
- **M:1 segment protection**
- **Data Path Segment Protection**

Going Forward

- **We think we can iron-out these issues by May meeting.**

- **We have clearly described a number of solutions; may be able to agree on one as a direction by May.**

- **Consider motion to authorize pre-circulation of Segment Protection Draft PAR in case we resolve issues by May meeting.**