PBB-TE Segment Protection

David W. Martin

January 12-16th, 2009

New Orleans, LA

v00
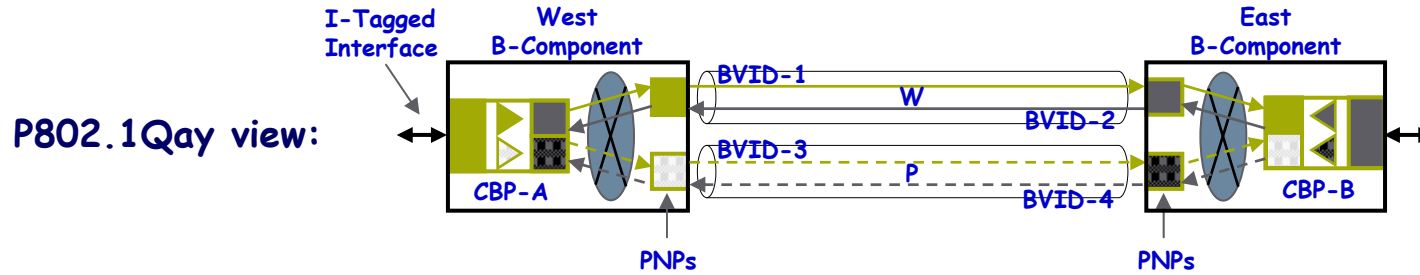
Contents

- ➢ **Problem Statement**
- ➢ **Segmentation Approach**
- ➢ **Segment Protection Options**
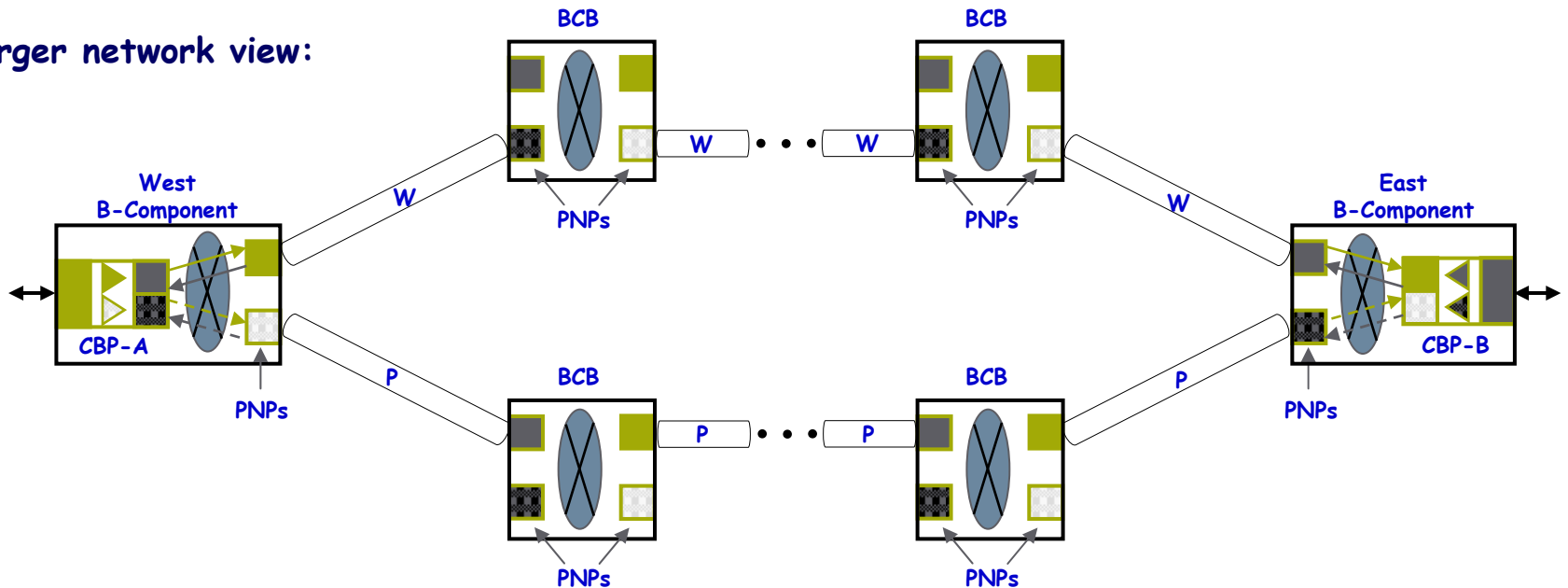- ➢ **Conclusions**

Problem Statement

➢ **For any connection oriented end-to-end path protection scheme (aka trail protection), as the total media length and the amount of intermediate equipment increases so does the probability of simultaneous failures (i.e., within a 4hr MTTR window) along both the working and protection paths, eventually impacting the corresponding availability target (e.g., 99.999% or 5min/yr downtime)**

➢ **PBB-TE P802.1Qay 1:1 protection falls into the above category**

➢ **September 2008 (Seoul) presentation* provided requirements from two Service Providers in India for a PBB-TE local repair mechanism to mitigate the above problem**
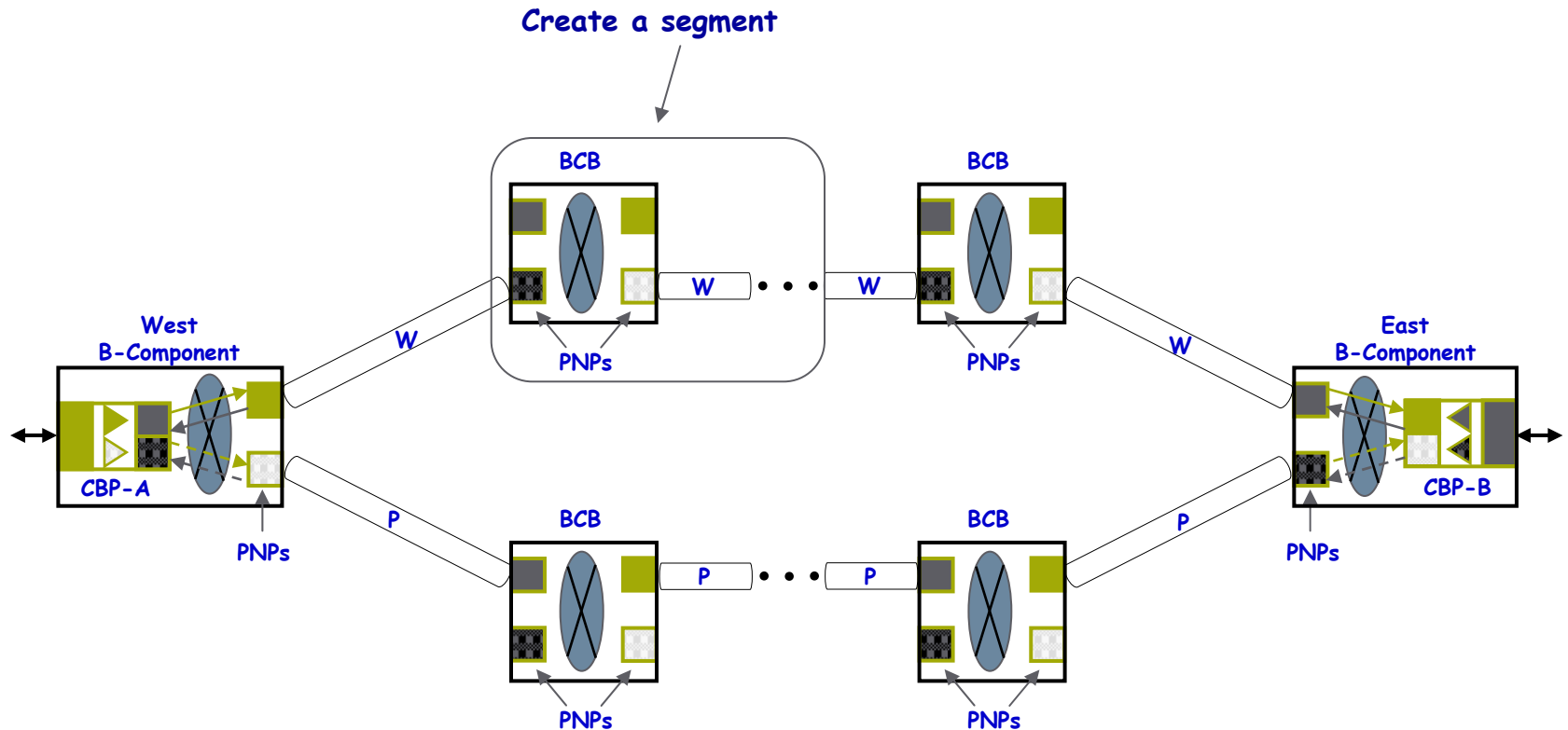
MTTR = Mean Time To Repair   * new-Protection-Vinod-Case-for-Segment-Protection-0908-v1.pps

PBB-TE Protected Domain: Expanded View

P802.1Qay view:

Larger network view:

General Segmentation Approach

- ➢ **The general solution is to split up the end-to-end paths and provide some type of local repair on a segment in order to improve overall availability**
- ➢ **Another benefit is maintenance domain independence if operator requests are supported as well as automatic (fault) requests**

Contents

# 1:1 Infrastructure Segment Protection Switching

PBB-TE "Infrastructure Segment" Definition
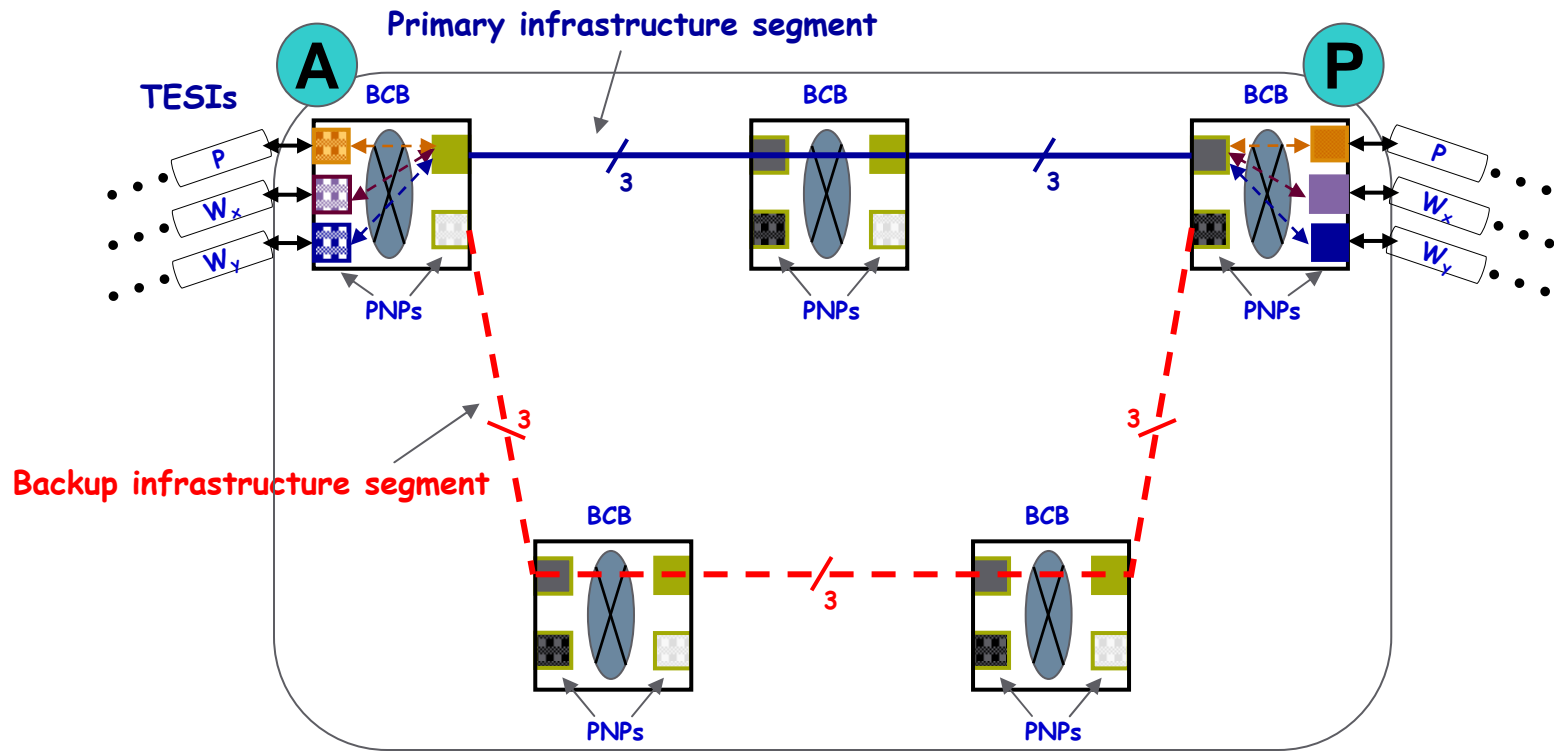
- ➢ **Primary infrastructure segment (the protected entity) is the common underlying infrastructure between the PNPs on nodes A and P**
- ➢ **Backup infrastructure segment is pre-established by provisioning the FDBs of nodes along a diverse route for the same set of TESIs / <B-DA, B-VID>'s**

PBB-TE Infrastructure Segment Integrity
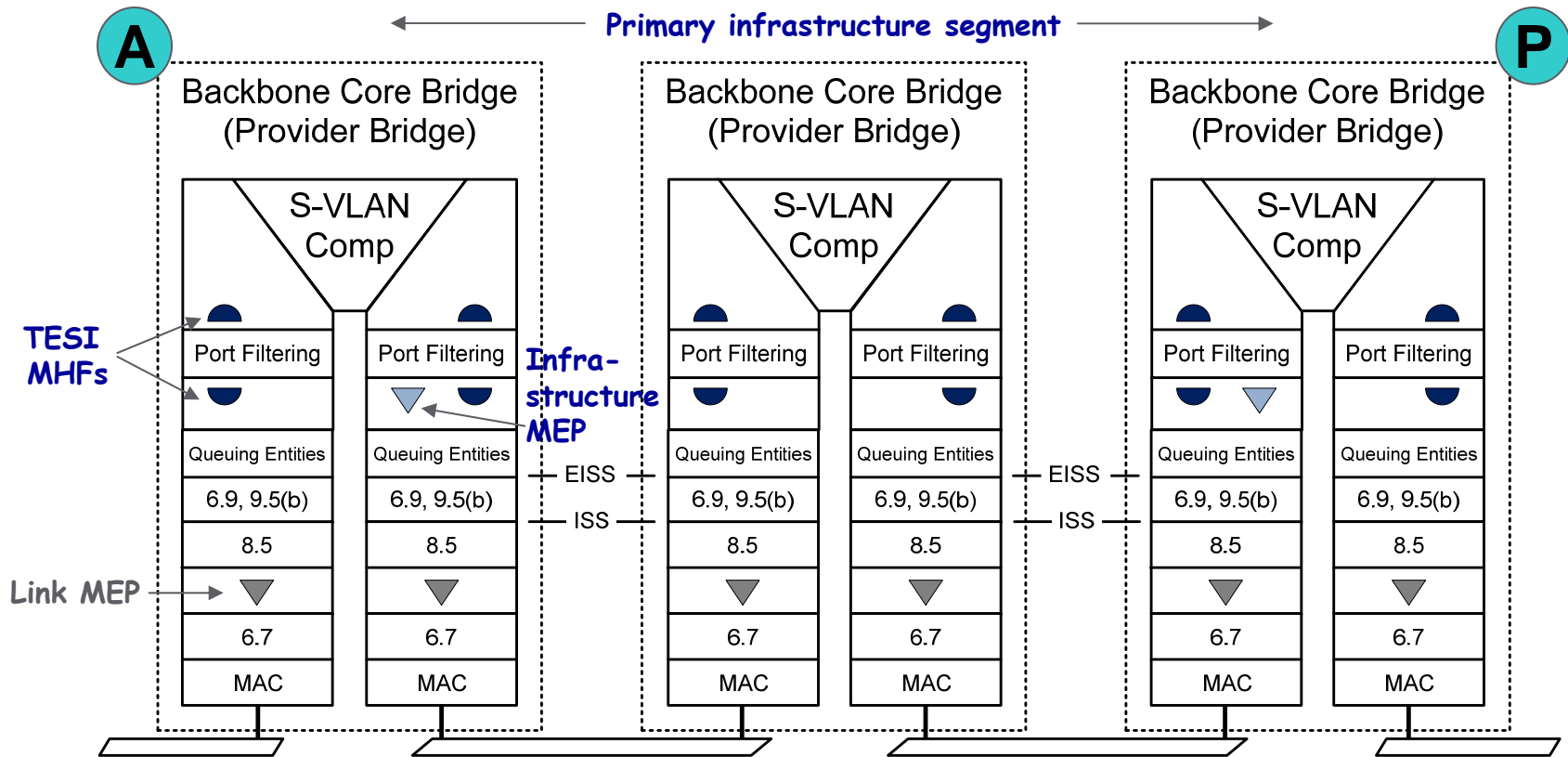
6.9 : Support of the EISS
9.5(b) : TPID for S-TAG
8.5 : Bridge Port Transmit and Receive
6.7 : Support of the ISS by specific MAC Procedures

6.17 (VID), 6.18 (I-SID), 6.19 (TESI) mux/demux not shown

➢ **Introduce MEPs (with individual MAC addresses) on PNPs of nodes A and P to monitor infrastructure segment integrity (using a B-VID from the range allocated for PBB-TE)**
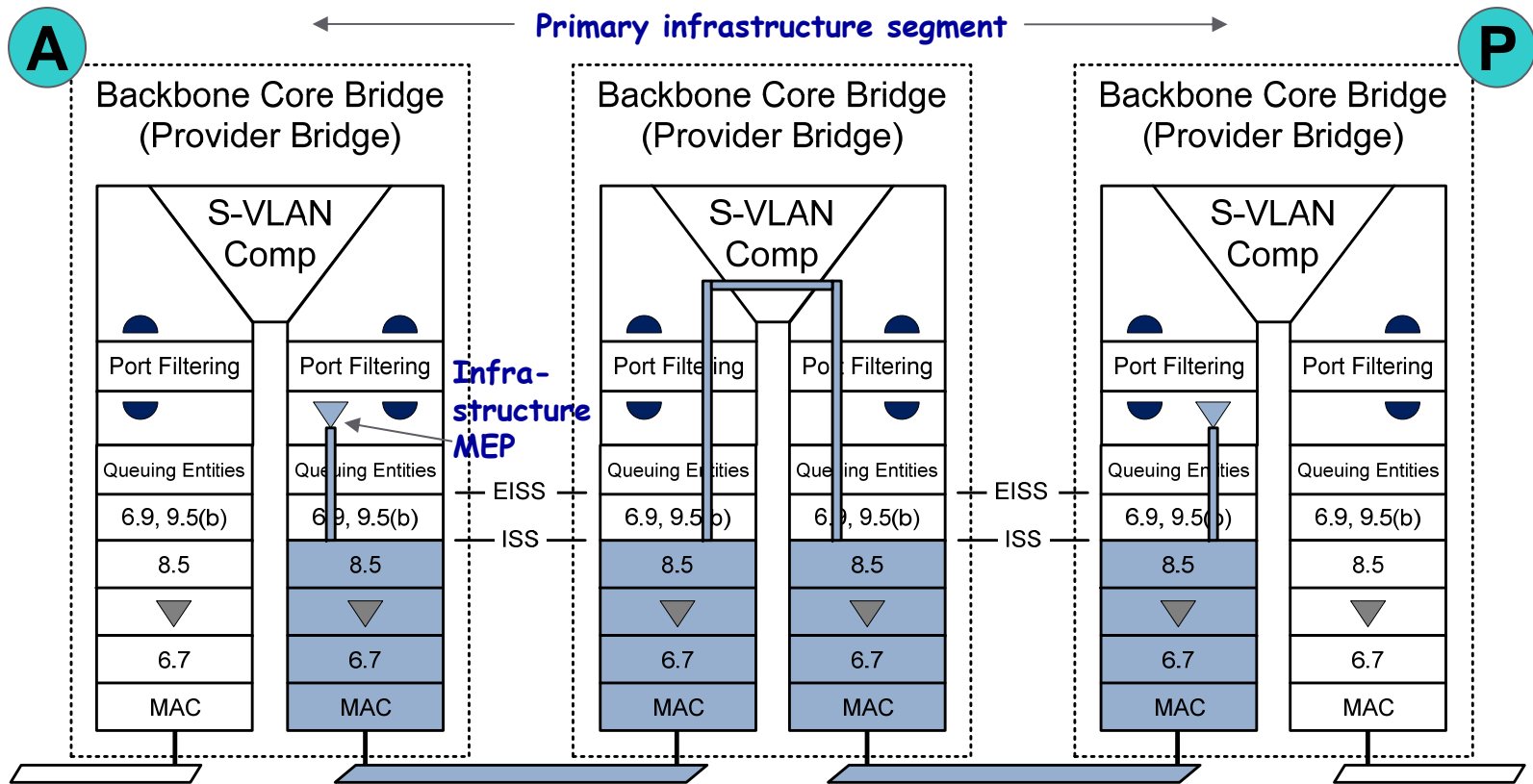
PBB-TE Infrastructure Segment Integrity

6.9 : Support of the EISS
9.5(b) : TPID for S-TAG
8.5 : Bridge Port Transmit and Receive
6.7 : Support of the ISS by specific MAC Procedures

6.17 (VID), 6.18 (I-SID), 6.19 (TESI) mux/demux not shown

➢ **CCMs between the PNP MEPs monitor that individual datapath, which includes the common shaded areas, and all links**

PBB-TE Infrastructure Segment Integrity
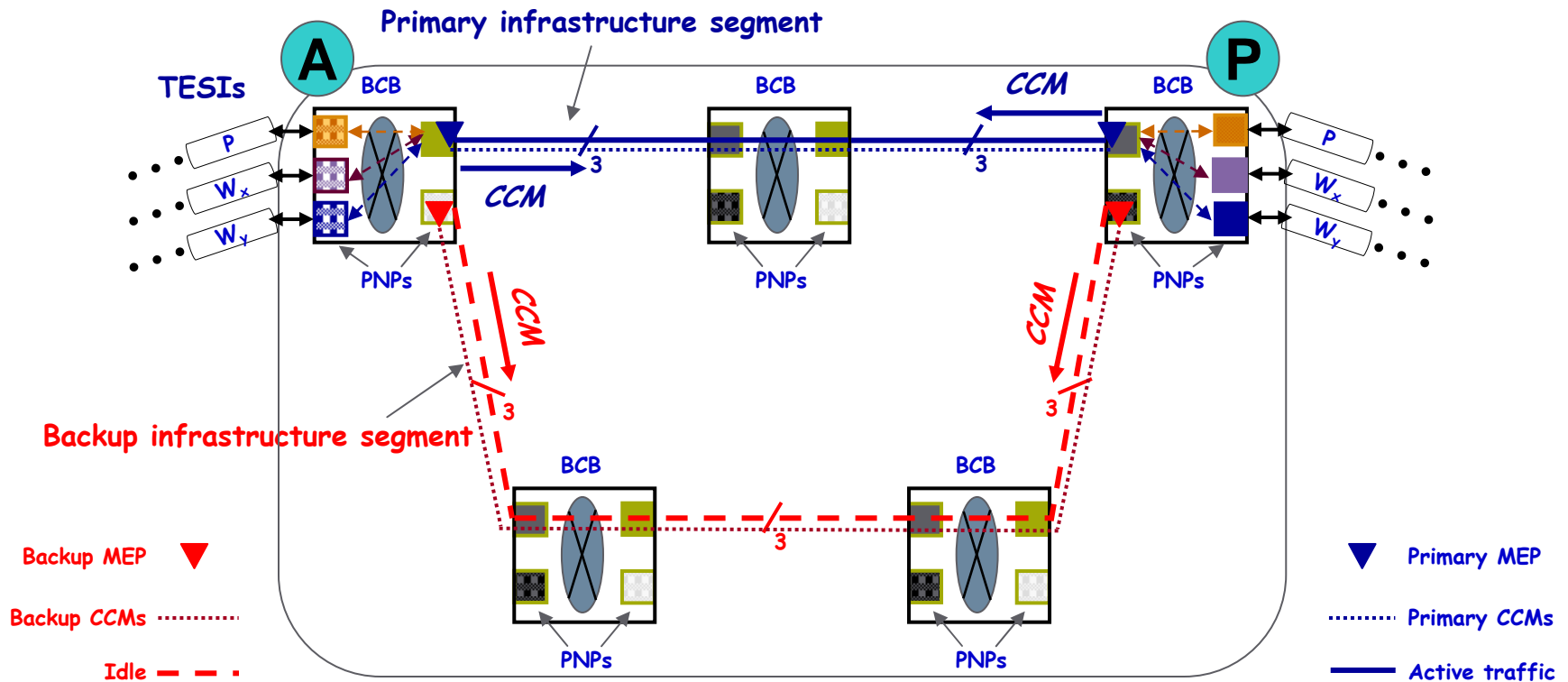
- CCMs between nodes A and P on the primary and backup infrastructure segments cannot use the same addressing as the e2e ESPs

$$\langle P, A, ESP\text{-}VID \rangle \neq \langle ESP\text{-}DA, ESP\text{-}SA, ESP\text{-}VID \rangle$$

- Therefore the infrastructure segment integrity coverage does not entirely monitor the constituent TESI segments

TESI Segment Integrity and e2e Protection
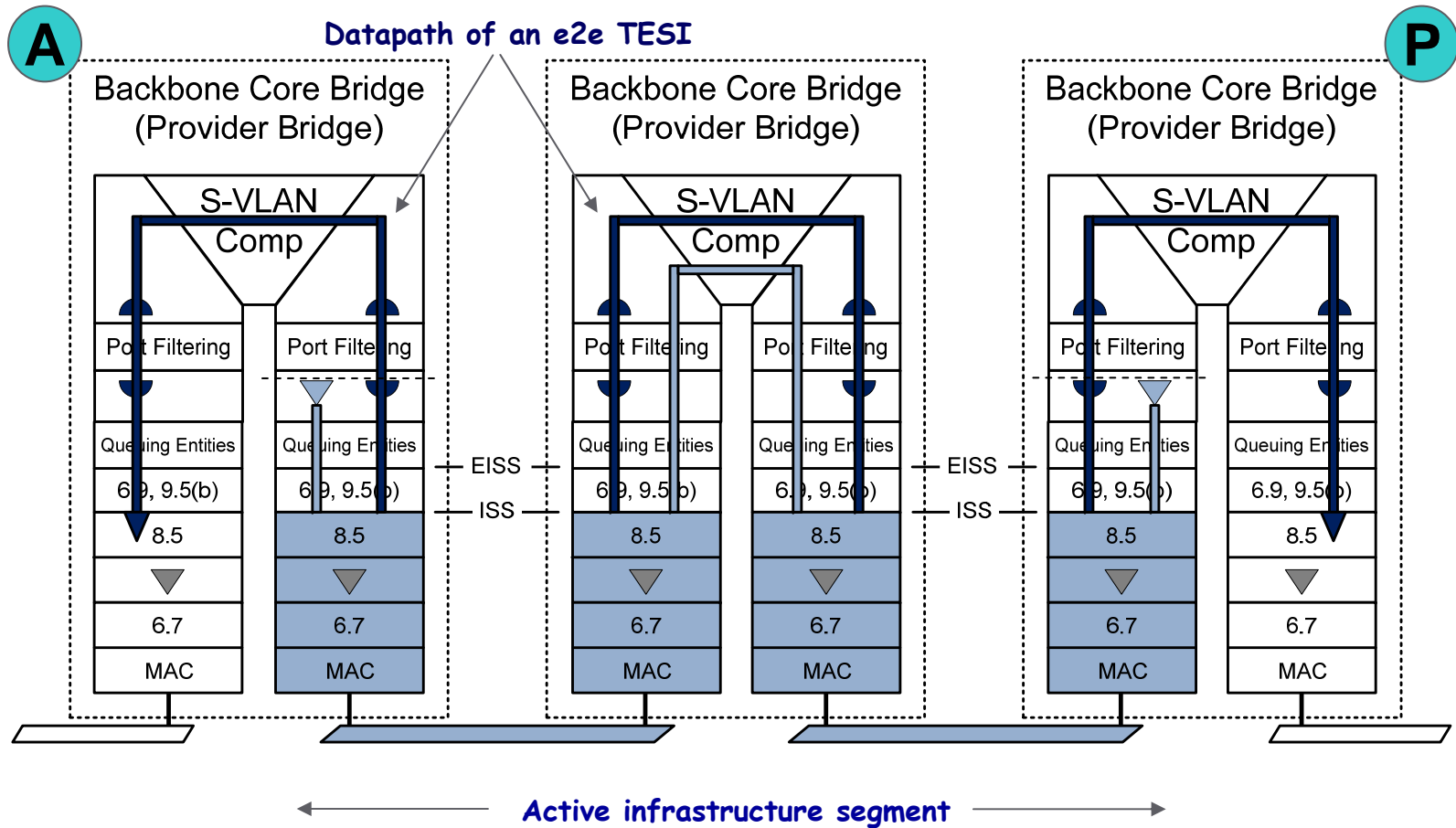
➢ **A fault on the dark blue datapath, specific to a TESI, would be protected by e2e P802.1Qay TESI protection**

PBB-TE Infrastructure Segment Switch
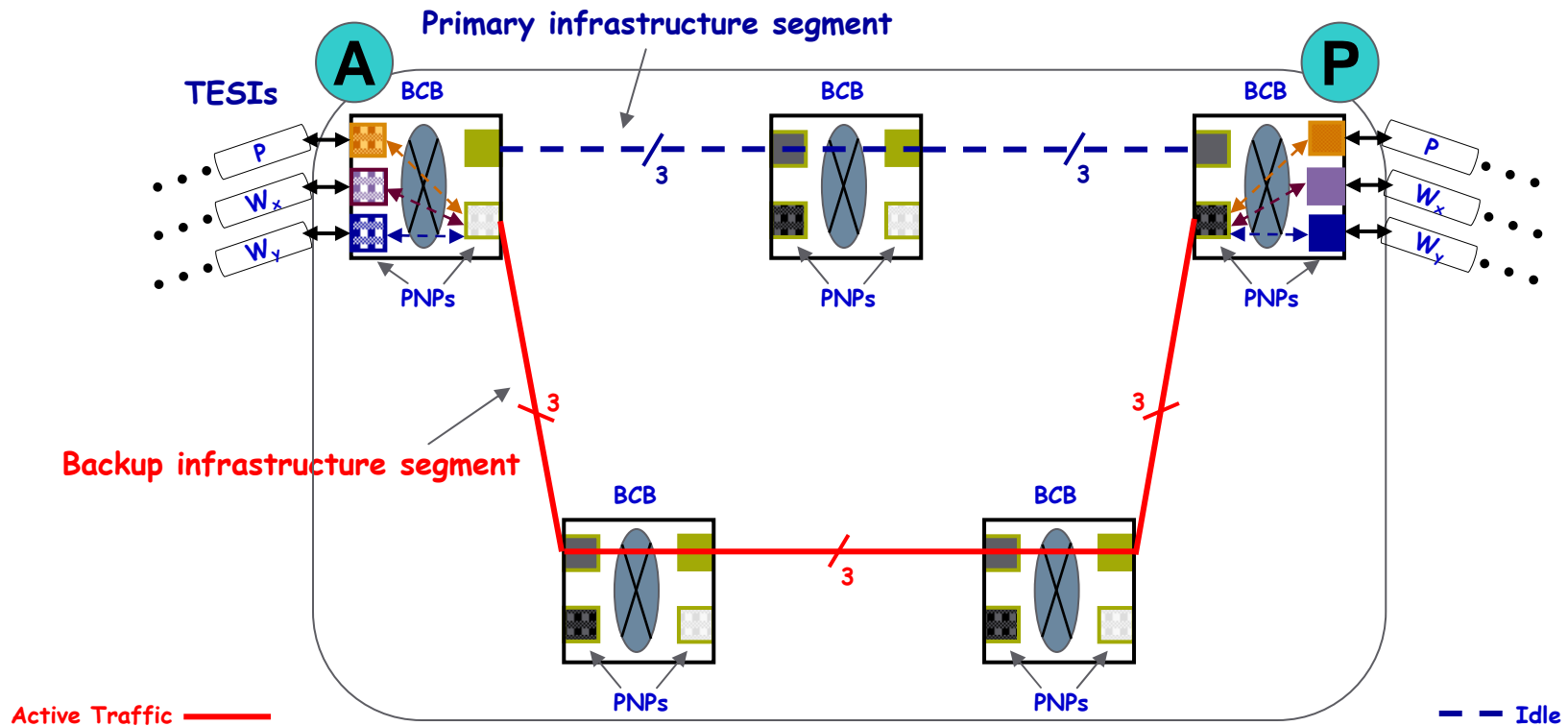
- ➤ **The switching trigger is either loss of infrastructure CCMs or an operator request**
- ➤ **FDBs on nodes A and P are updated with the Port entries for the PNPs on the backup infrastructure segment**

Infrastructure Segment Switch Limitation

➢ **The portion of a TESI datapath through an *active segment* that is not monitored by the infrastructure segment CCMs is monitored by the e2e CCMs from P802.1Qay, and a fault there would be protected by e2e P802.1Qay TESI protection**

➢ **However, the corresponding portion of a TESI datapath through the *inactive segment* cannot be monitored by the e2e CCMs since they are not forwarded on that path**

➢ **Performing a protection switch to a path of unverified integrity is called "blind switching"**

Infrastructure Segment Switch Limitation

➢ **The potential impact of blind switching is:**
  - **For a fault initiated switch to the inactive infrastructure segment (with a latent TESI datapath fault), the e2e P802.1Qay protection mechanism for the affected TESI would eventually execute following its hold-off timer and if protection resources are available → prolonged traffic loss**
  - **For a manual switch to the inactive infrastructure segment (with a latent TESI datapath fault), there would be traffic loss on the TESI until the e2e P802.1Qay protection mechanism executed → unnecessary traffic loss**

➢ **The first scenario can be argued as acceptable since there are two faults**

➢ **But would a manual switch resulting in traffic loss (albeit brief, say ~150ms) for this latent datapath fault scenario be considered Carrier Grade?**

Protection Functionality Checklist

➢ **Basic elements of 1:1 infrastructure segment protection scheme:**

    ☑ **Triggers / Protected Domain**

        – **MEPs at infrastructure segment endpoints monitor CCMs**

    ☑ **Bridge mechanism**

        – **Selective 1:1 bridge via FDB egress Port entry update**

    ☑ **Selector mechanism**

        – **Merging selector via PNP B-VID membership**

    ☑ **Protection phases**

        – **Single phase protocol**

    ☑ **Signalling channel / information**

        – **CCM RDI flag for bridge request under fault conditions**

        – **Dual-ended management plane requests for operator commands**

1:1 Infrastructure Segment Protection Recap

➢ **Complements the current e2e P802.1Qay TESI protection by providing independent protection for infrastructure segment faults**

➢ **Could also provide maintenance domain independence if operator requests are supported**

➢ **A TESI segment datapath fault, not covered by the infrastructure integrity check, on the *active segment* would be protected by the e2e PBB-TE protection**

➢ **A TESI segment datapath fault, not covered by the infrastructure integrity check, on the *inactive segment* can lead to brief, unnecessary traffic loss until protected by the e2e PBB-TE protection**

1:1 Segment Server Protection Switching

1:1 Segment Server Protection

➢ **Rather than attempt to provide a protection mechanism at the same layer, consider a hierarchal approach**

➢ **Fully encapsulate all e2e PBB-TE traffic, along either the working or protection entity, into a new PBB-TE protected domain for the extent of the segment**

➢ **Provides full integrity coverage**

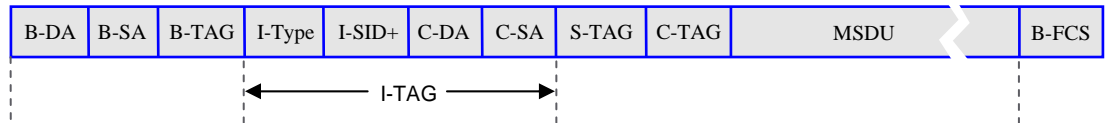➢ **Avoids defining a new protection mechanism**

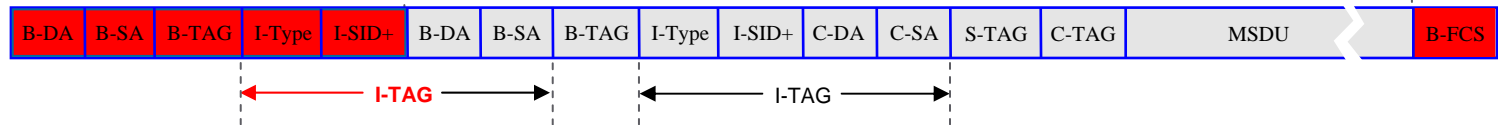# PBB-TE 1:1 Segment Server Protection
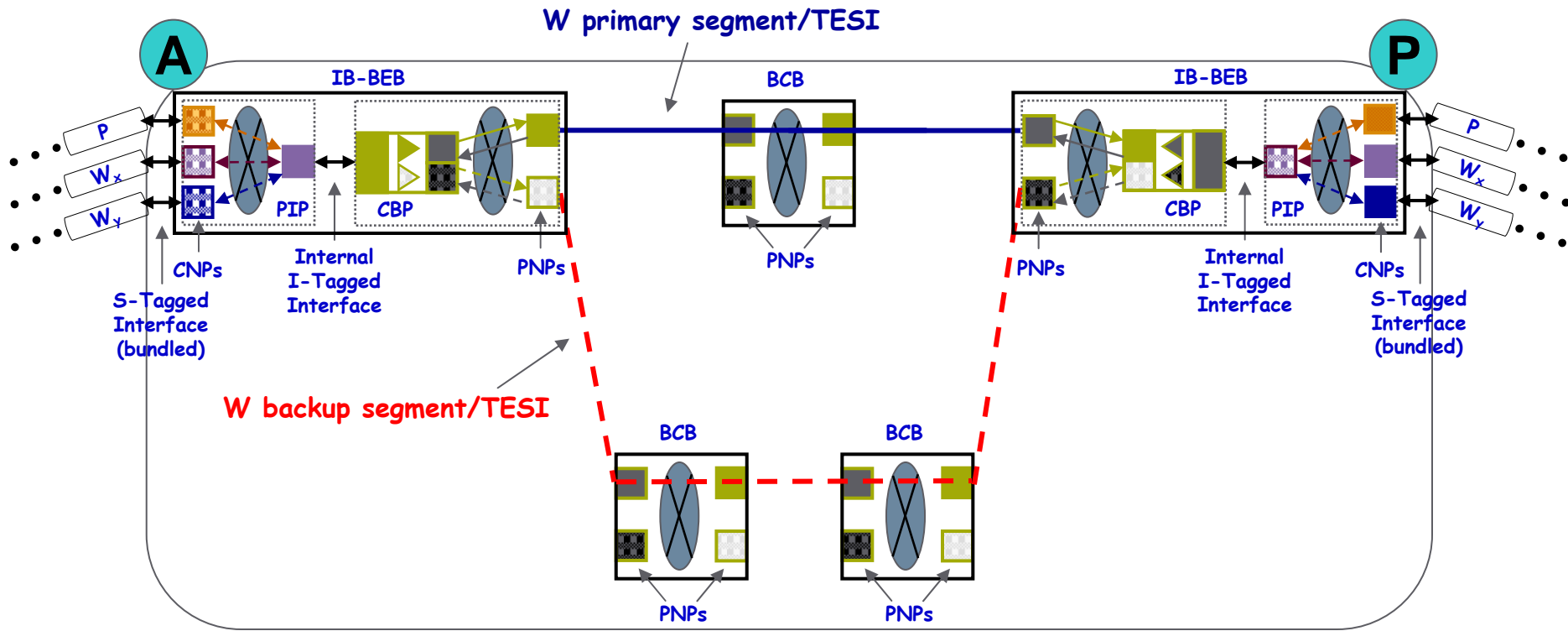
- ➤ **Upgrade the BCBs at the edges of the segment to IB-BEBs and provide a PBB hierarchal (802.1ah 26.6.1) S-tagged interface (802.1ah 25.4)**
- ➤ **Each segment is now a new (server layer) TESI in a regular PBB-TE 1:1 TESI PG, with the corresponding TESI CCM integrity coverage**

PBB-TE 1:1 Segment Server Protection

Frame at segment ingress/egress:

B-DA	B-SA	B-TAG	I-Type	I-SID+	C-DA	C-SA	S-TAG	C-TAG	MSDU	B-FCS

I-TAG (spanning I-Type to C-SA)

Frame within segment:

B-DA	B-SA	B-TAG	I-Type	I-SID+	B-DA	B-SA	B-TAG	I-Type	I-SID+	C-DA	C-SA	S-TAG	C-TAG	MSDU	B-FCS

I-TAG (spanning I-Type to I-SID+ in red section)   I-TAG (spanning I-Type to C-SA)

- ➢ **Segment B-MACs are the server IB-BEBs (nodes A and P) CBPs' MACs**
- ➢ **Segment B-VID corresponds to either primary or backup segment**
- ➢ **Segment I-SID would be specific to that protected domain**
- ➢ **Note the original ESP B-TAG is retained according to the bundled S-tagged interface definition**
- ➢ **A fresh FCS would be calculated and appended over the segment**
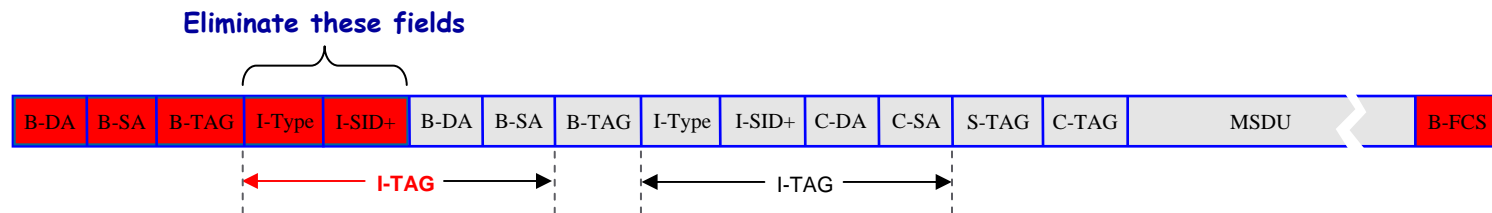
1:1 Segment Server Protection Summary

➢ **Segment integrity coverage is complete since the server layer provides the necessary CCMs over both primary and backup segments (i.e., the server P802.1Qay working and protection TESIs)**

➢ **Protection within the segment is exactly as defined by P802.1Qay**

➢ **No new work for 802.1**

➢ **The price tag is the additional PBB encap**

Note that the P802.1Qay PAR scope statement "This project will not take account of multi-domain networks" is referring to peered networks, not hierarchal networks such as discussed here

Segment Server Protection Variations

Segment Server Protection Variation I

➢ **Recall:** *The price tag is the additional PBB encap*

➢ **There are a couple of perspectives on this:**

   • **The extra equipment involved (i.e., IB-BEB vs BCB)**

   • **The extra bandwidth consumed due to the encap**

➢ **It has been suggested that the I-TAG is not really required within a PBB-TE segment**

➢ **The I-component PIP and B-component CBP of the IB-BEB could be simplified to not utilize a full I-TAG (i.e., leave just the e2e B-MACs)**

➢ **The additional PBB encap would be the minimum achievable 16B (rather than 22B) – still much larger than a 4B MPLS label used for FRR**
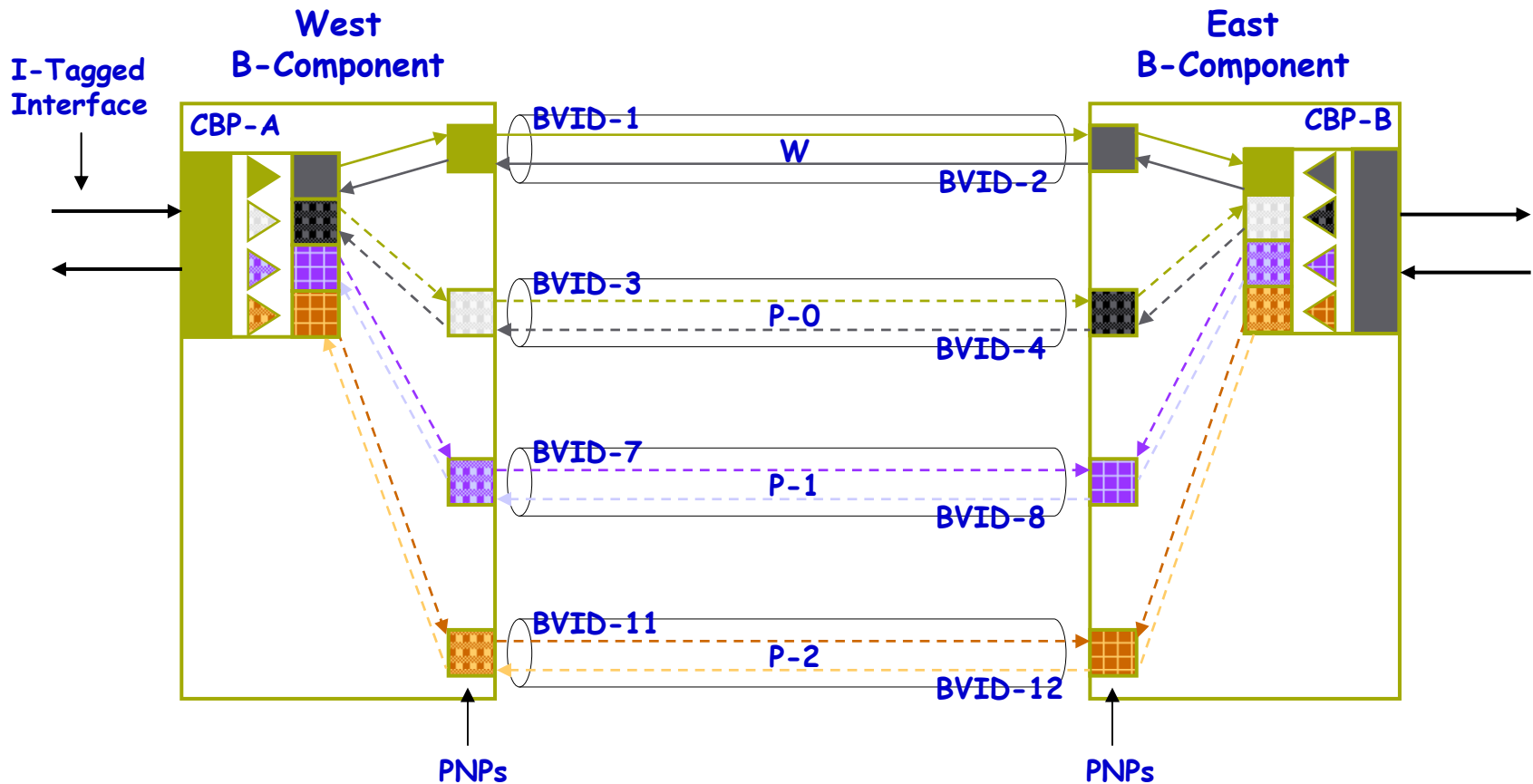
Eliminate these fields

| B-DA | B-SA | B-TAG | I-Type | I-SID+ | B-DA | B-SA | B-TAG | I-Type | I-SID+ | C-DA | C-SA | S-TAG | C-TAG | MSDU | B-FCS |

← I-TAG → ← I-TAG →

Segment Server Protection Variation II

➢ **Recall that the requirements outlined in:**

   new-Protection-Vinod-Case-for-Segment-Protection-0908-v1.pps

   included support for M:1 protection on the segment

➢ **An M:1 mode could be a relatively straightforward enhancement of the existing P802.1Qay PBB-TE 1:1 TESI protection**

➢ **M:1 provides very high availability by switching to whichever protection entity is available, by automatically escalating through a pre-established prioritized sequence**

Note that the same M:1 mode could be used for the e2e protection scheme, if M+1 diverse paths are available e2e.

Example 3:1 PBB-TE Protection Group

West B-Component

East B-Component

I-Tagged Interface

CBP-A

CBP-B

BVID-1

W

BVID-2

BVID-3

P-0

BVID-4

BVID-7

P-1

BVID-8

BVID-11

P-2

BVID-12

PNPs

PNPs

Transmit CBP traffic is sent over a given TESI by altering the B-VID accordingly
Received CBP traffic is the merge of traffic from all TESIs

Segment Server Protection Variation III

➢ **Recall that existing P802.1Qay PBB-TE 1:1 TESI protection can optionally operate in a load-sharing mode, where groups of BSIs are individually 1:1 protected across a set of multiple TESIs**

➢ **So M+1 TESIs within a segment could be used in P802.1Qay load-sharing mode, thereby not requiring a new specification**

➢ **Two disadvantages compared to the previous M:1 TESI protection are:**
  - **If both the W and P TESIs fail for a given PG then its traffic is lost**
  - **More operationally complex as traffic is spread across multiple TESIs within a segment**

Conclusions

- ➢ **1:1 Infrastructure Segment Protection**
  - **Relies on having e2e P802.1Qay TESI protection for handling certain TESI segment datapath faults**
  - **That corner case integrity exposure can lead to brief, unnecessary traffic loss for a manual switch**
- ➢ **1:1 Segment Server Protection**
  - **Provides full integrity coverage**
  - **No new work for 802.1**
  - **Requires additional PBB encap**
  - **Possible variants:**
    - **without full I-TAG**
    - **M:1 mode**
    - **load-sharing mode**