A Framework for E-VPN Performance Monitoring

draft-zheng-l2vpn-evpn-pm-framework-00

Vero Zheng (vero.zheng@huawei.com)
Robin Li (lizhenbin@huawei.com)

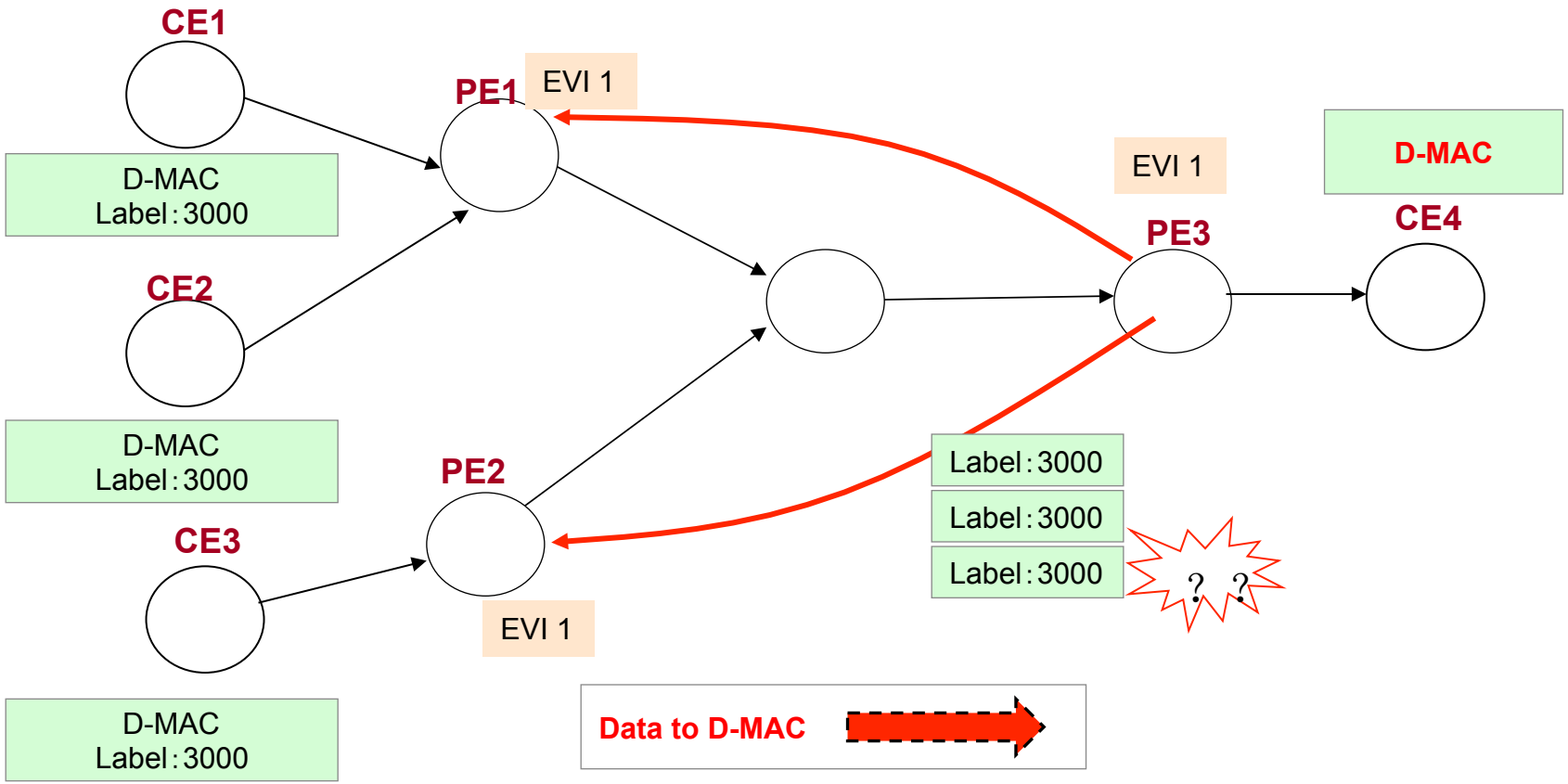
L2VPN WG, IETF 87, Berlin, 29 July 2013

Background

- **Virtual Private LAN Service (VPLS) is a proven and widely deployed Ethernet L2VPN solution with limitations. Also, new applications are driving several new requirements for other L2VPN services**
- **Ethernet VPN (E-VPN) solution has been proposed to meet the requirements**
- **Performance Monitoring (PM) in E-VPN is desired**
- **Challenges for performance monitoring in E-VPN**
  - Identifying the source EVI of received packets
- **This document introduces the framework for E-VPN PM**

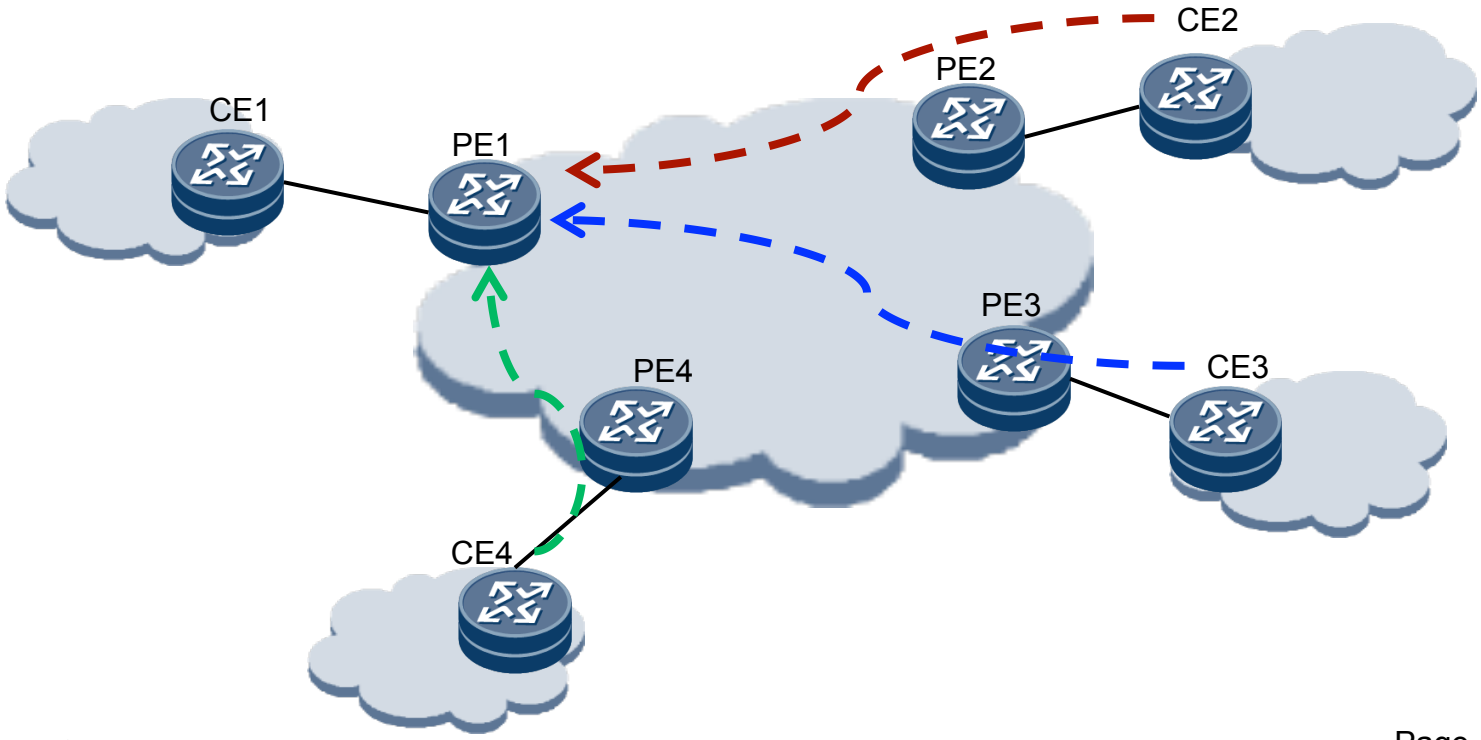
Challenge for E-VPN Performance Monitoring

- Network Model: Multipoint-to-Point or Multipoint-to-Multipoint
  - Existing mechanisms for MPLS networks are for P2P or P2MP.



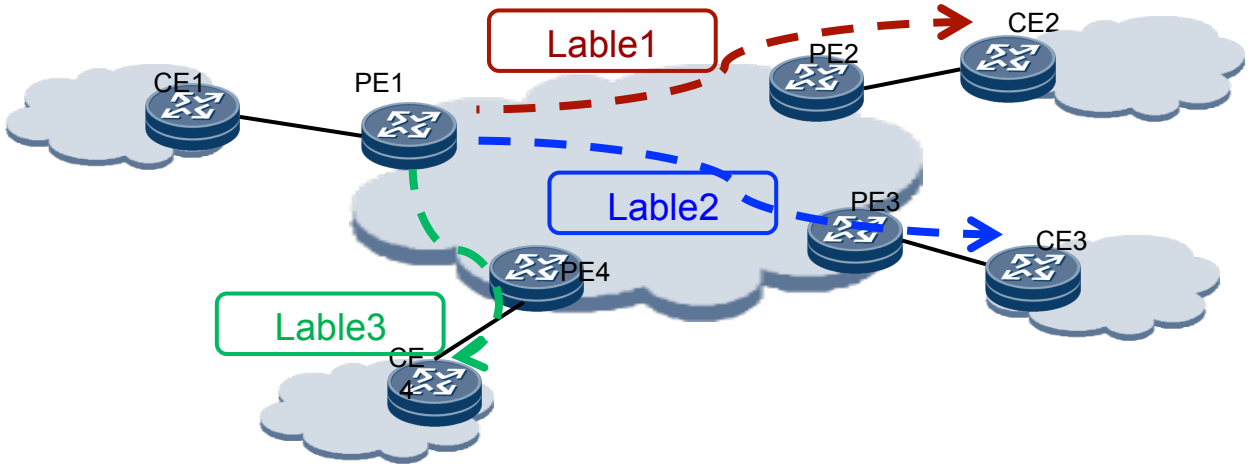
New Concept for E-VPN PM

- **EVI-to-EVI Tunnel (ET)**
  - Point-to-point connection between two EVIs in a E-VPN
  - ET is used by the egress PE to identify the ingress EVI



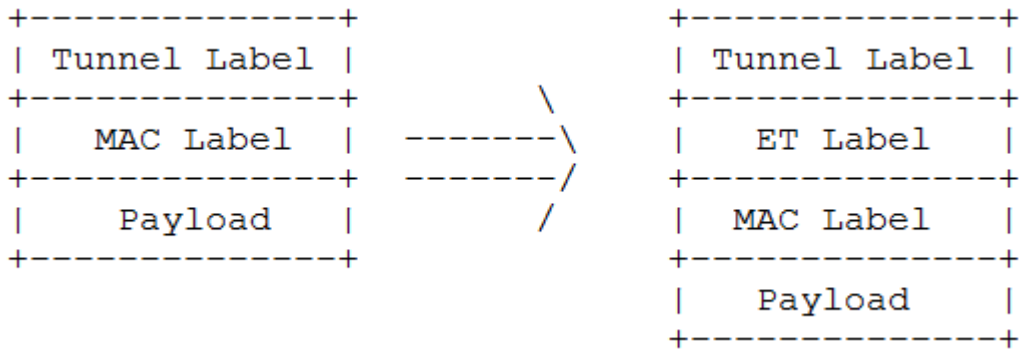
Control Plane Mechanisms

- **Step1: VPN membership auto-discovery**
  - Could be achieved by the Ethernet A-D route per EVI defined in draft-ietf-l2vpn-evpn
- **Step2: EVI-to-EVI Tunnel Label Allocation – ET Label**
  - For each local EVI, the egress PE SHOULD allocate different ET labels for each remote EVI in PEs belonging to the same E-VPN

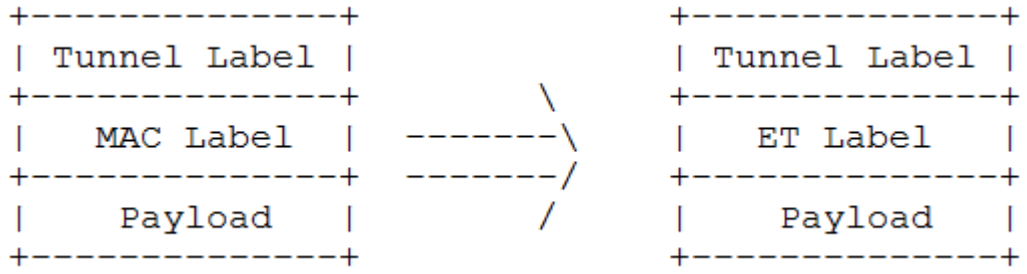


Packet Encapsulation with ET label

- **Approach 1: additional ET label for Ingress EVI identification**



- **Approach 2: replace MAC label with ET label**



E-VPN Performance Monitoring

- **PM mechanisms in RFC 6374 can be used for E-VPN**
  - Loss & Delay measurement
  - Address format for E-VPN:
    - Source addresses for E-VPN: (RD + PE address) of source EVI
    - Destination addresses for E-VPN: (RD + PE address) of destination EVI

Next Steps

- **Solicit comments & feedbacks**
- **Revise the draft**

Thank you