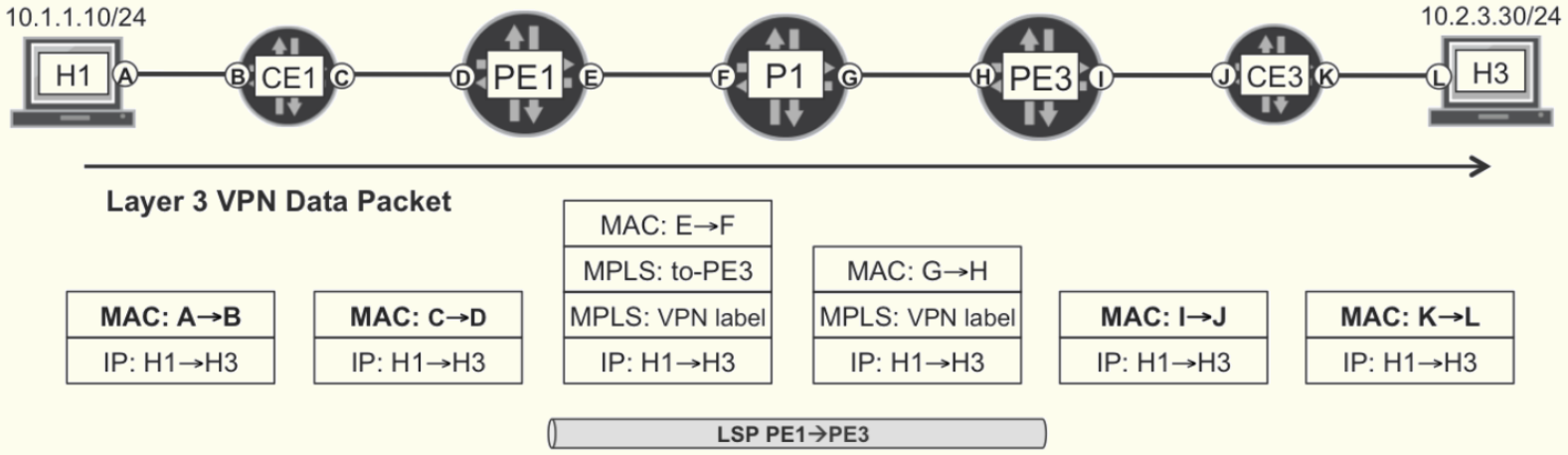
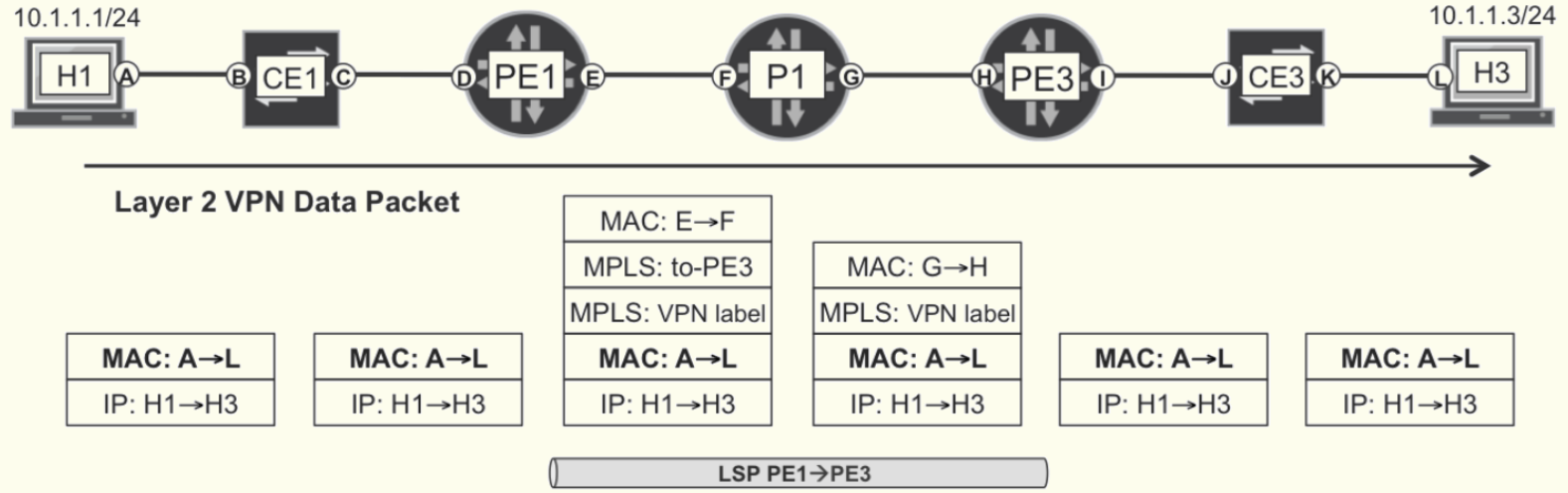
# Virtual Private Networks

## Layer 2 VPNs

Enzo Mingozzi
Professor @ University of Pisa
enzo.mingozzi@unipi.it

# L3VPN vs. L2VPN



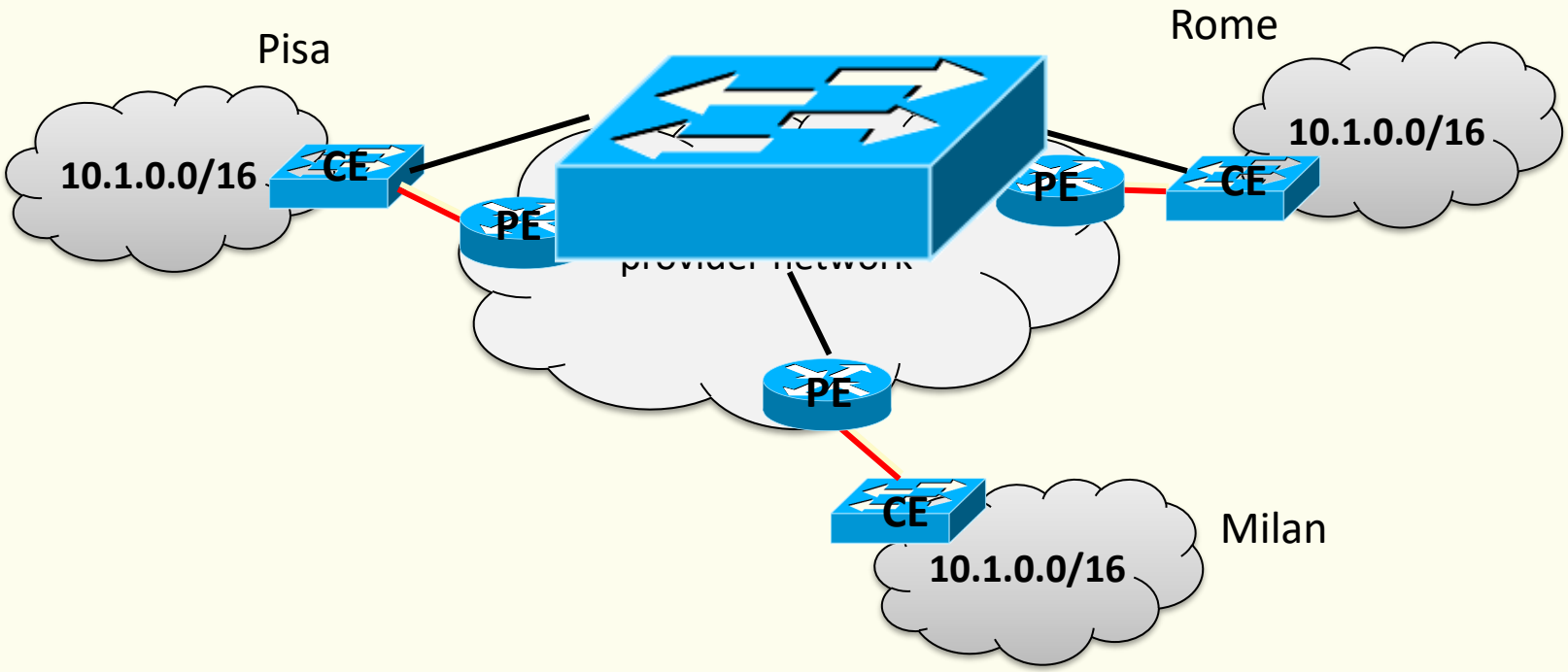



# L2VPN use cases

- L2VPN is a *bidirectional* service that provides an **overlay** to transport Layer 2 frames (Ethernet)
  - The actual underlay is composed of unidirectional transport LSPs
- Who is interested in such service?
  - **Corporate WAN**
  - **Data centers**
  - **SPs themselves for backhauling**

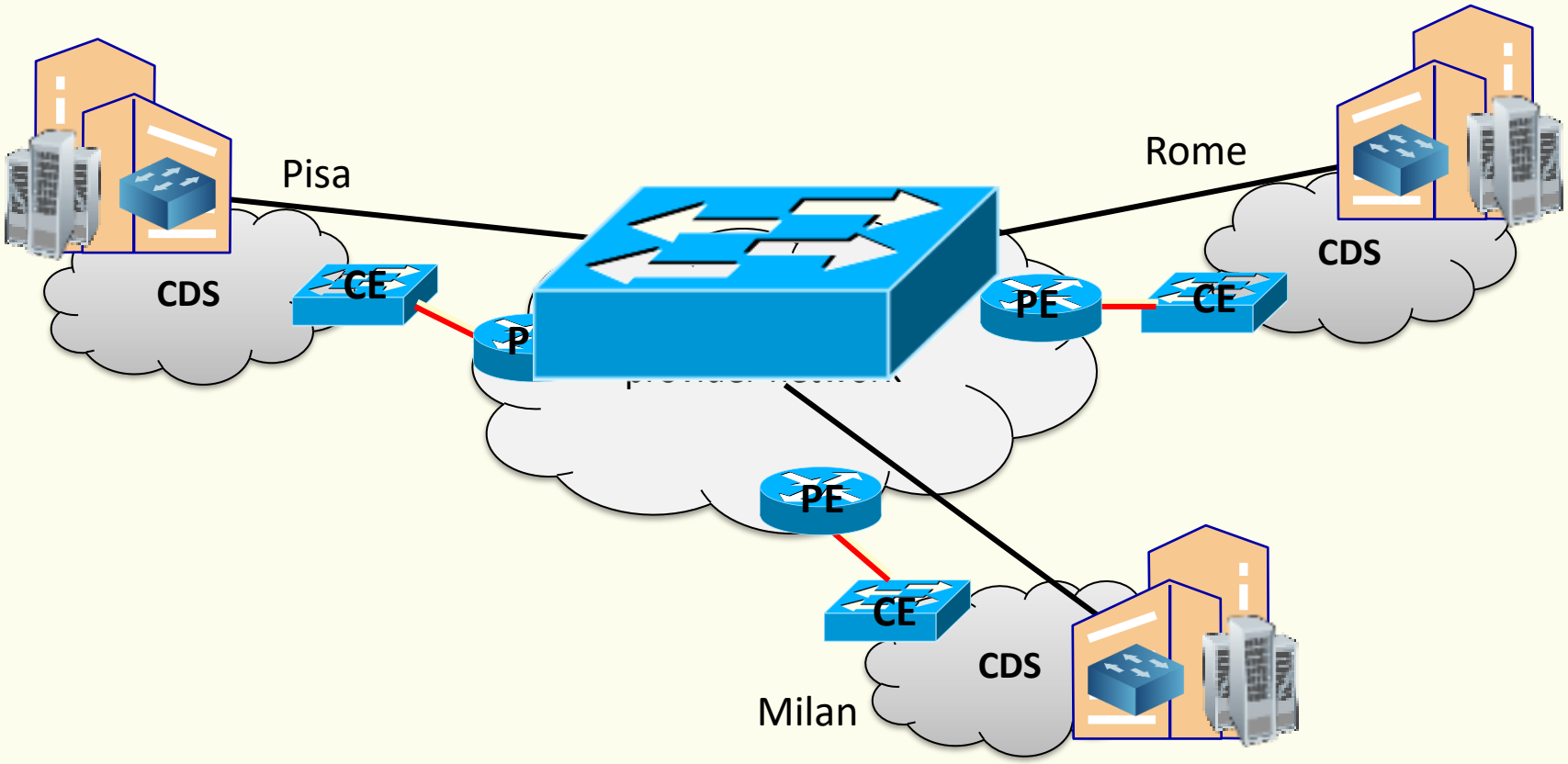
# WAN emulation

- WAN L2 links
  - E.g., to build its own MPLS core

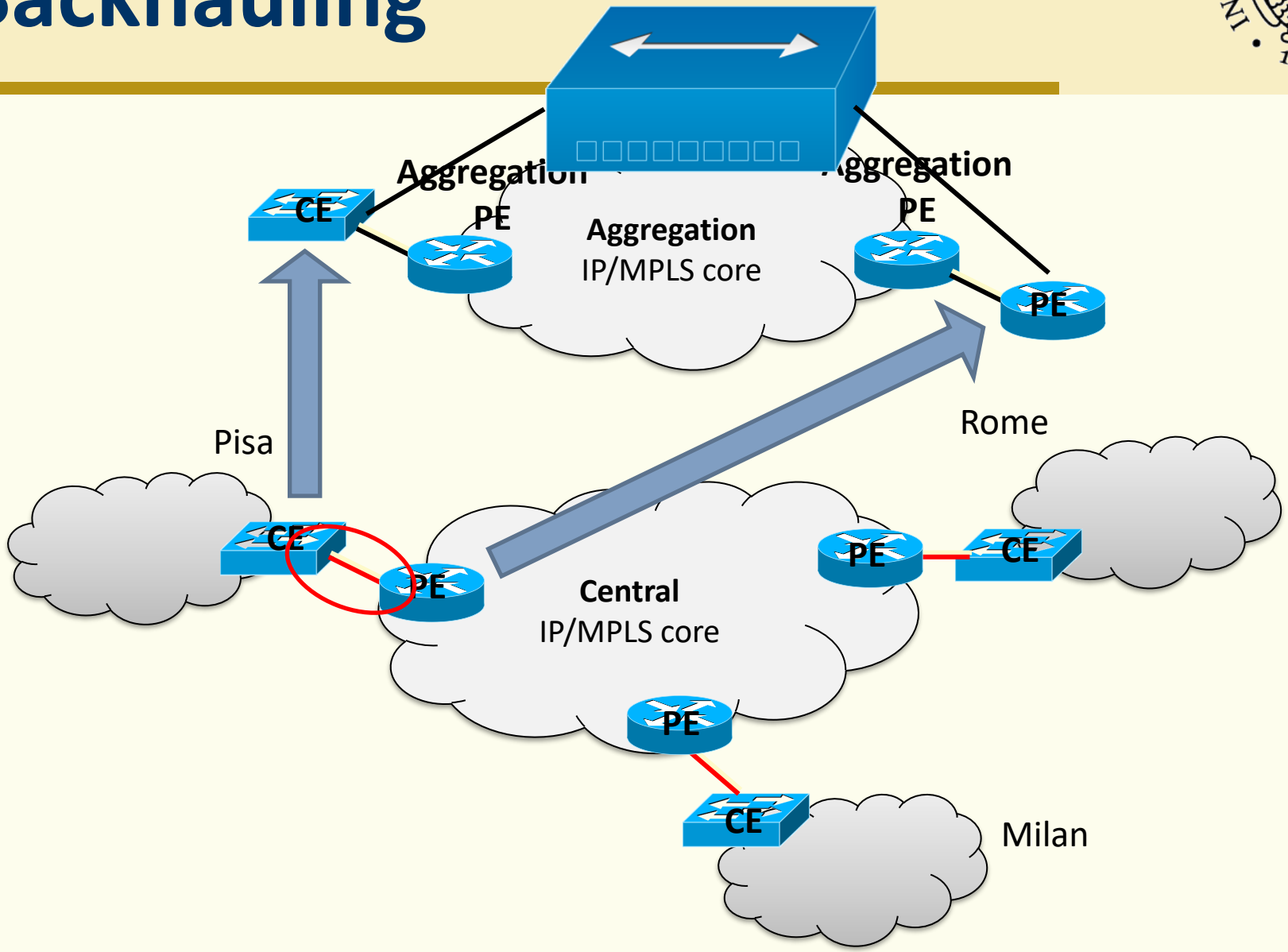


# Data Center Interconnect (DCI)

- Tenant L2 overlays across a set of geographically distributed Data Centers



# Backhauling

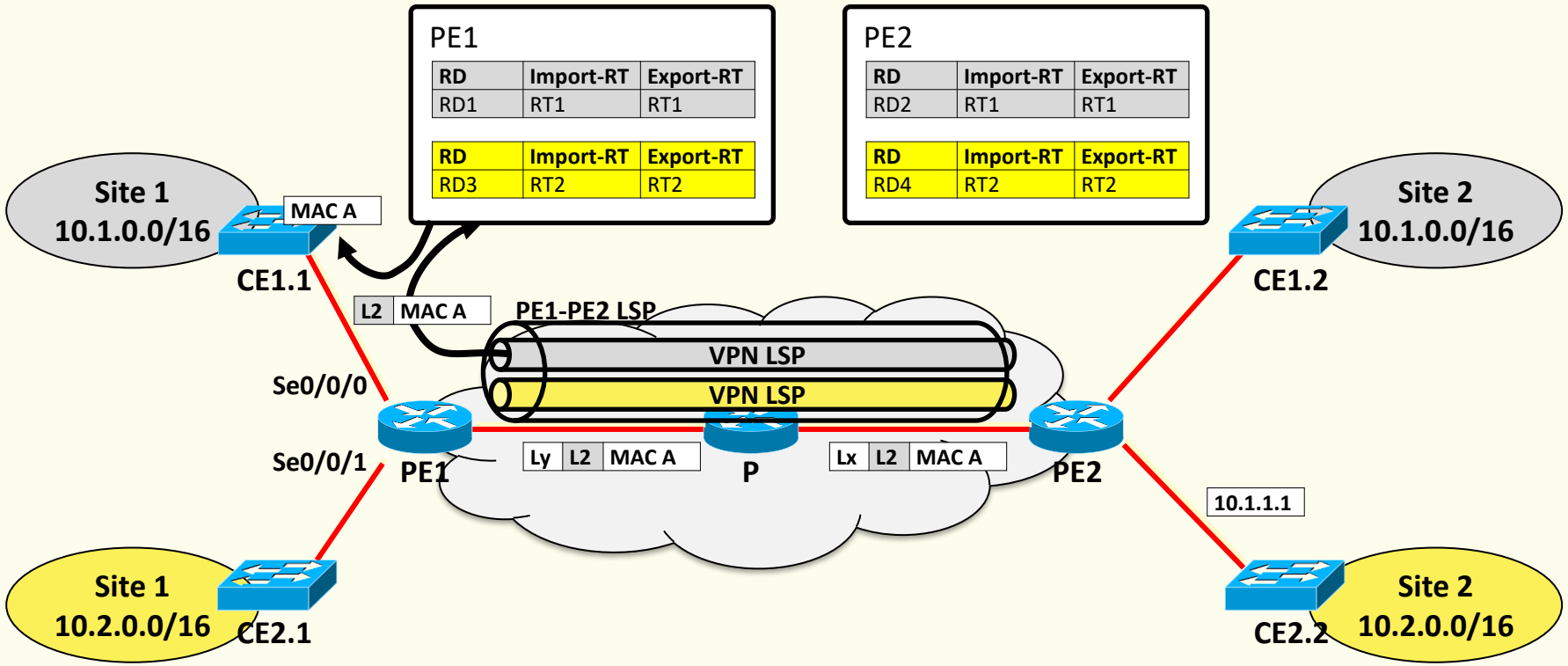


# L2VPN topologies

- L2VPNs can be **Point-to-Point** (P2P) or **Multipoint-to-Multipoint** (MP2MP)
- This definition is **service-centric**, not transport-centric: **it refers to the number of sites** that a given L2VPN can have
- **P2P** L2VPNs have 2 sites only
  - Virtual Private Wire Service (**VPWS**) or **VLL**
- **MP2MP** L2VPNs have ≥2 sites
  - Virtual Private LAN Service (**VPLS**)

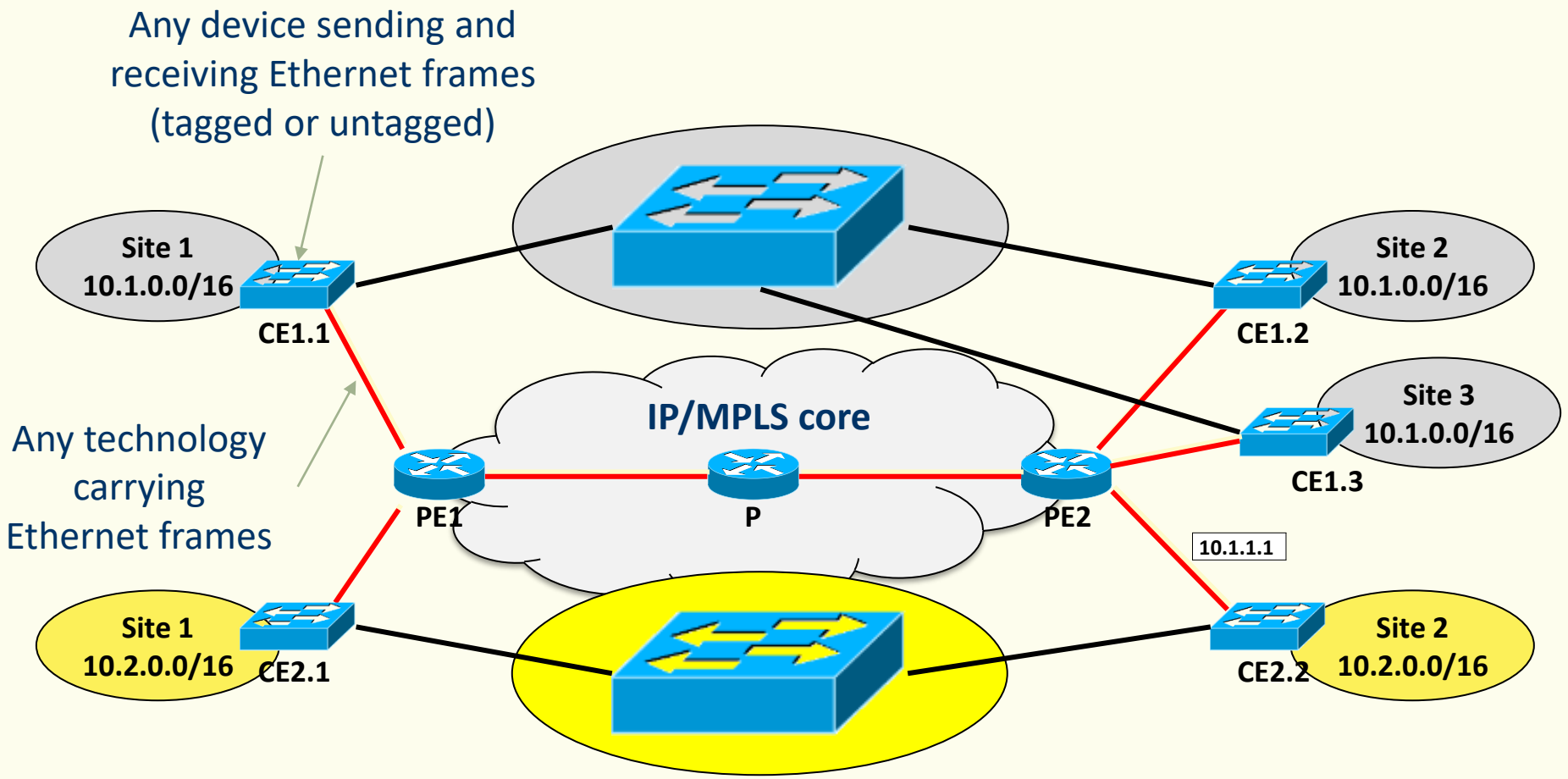
# P2P - VPWS

- Also called ***pseudowire* (PW)**
- No MAC learning between PEs

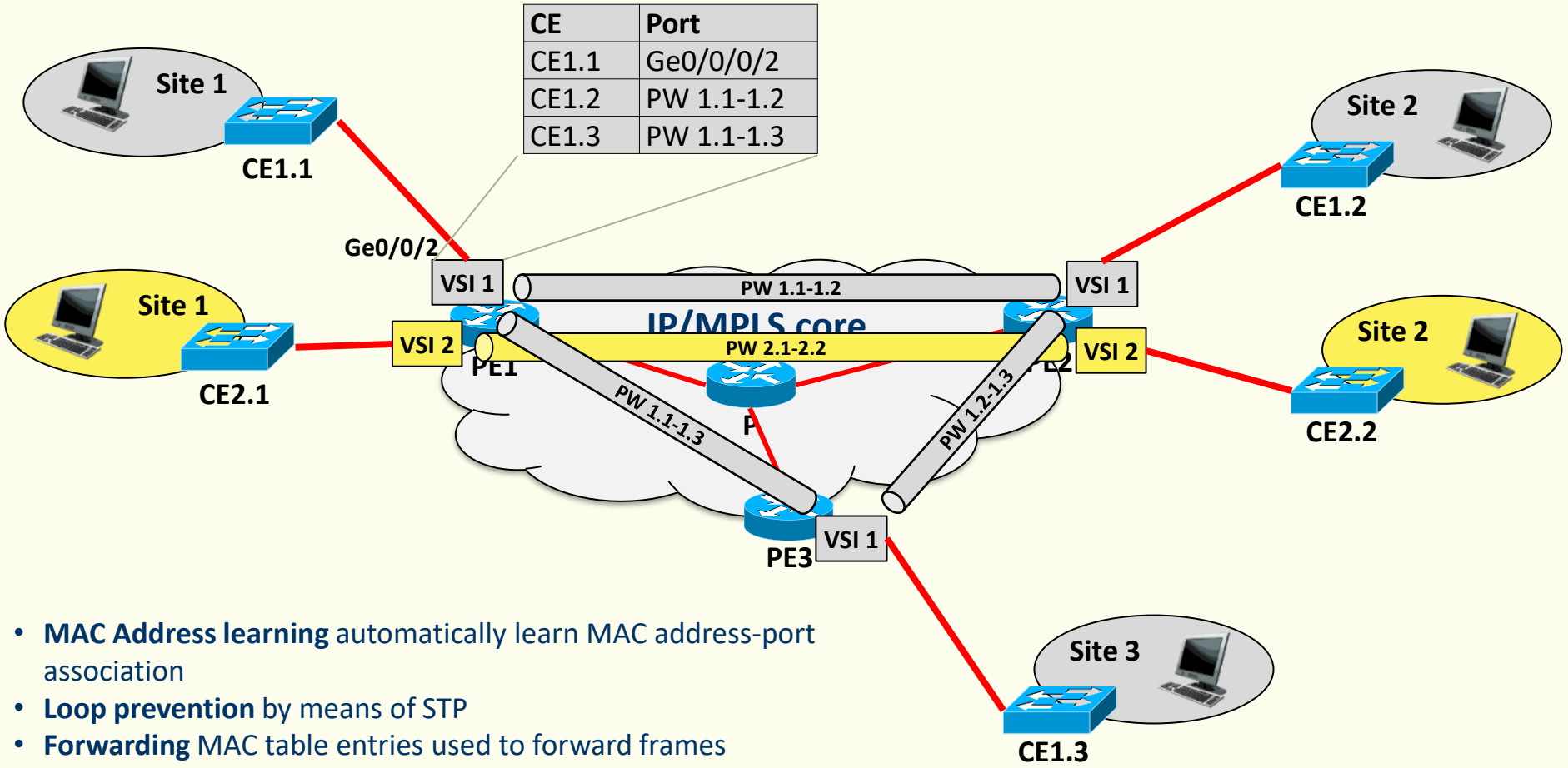


# Virtual Private LAN Service

- Emulate an Ethernet switch

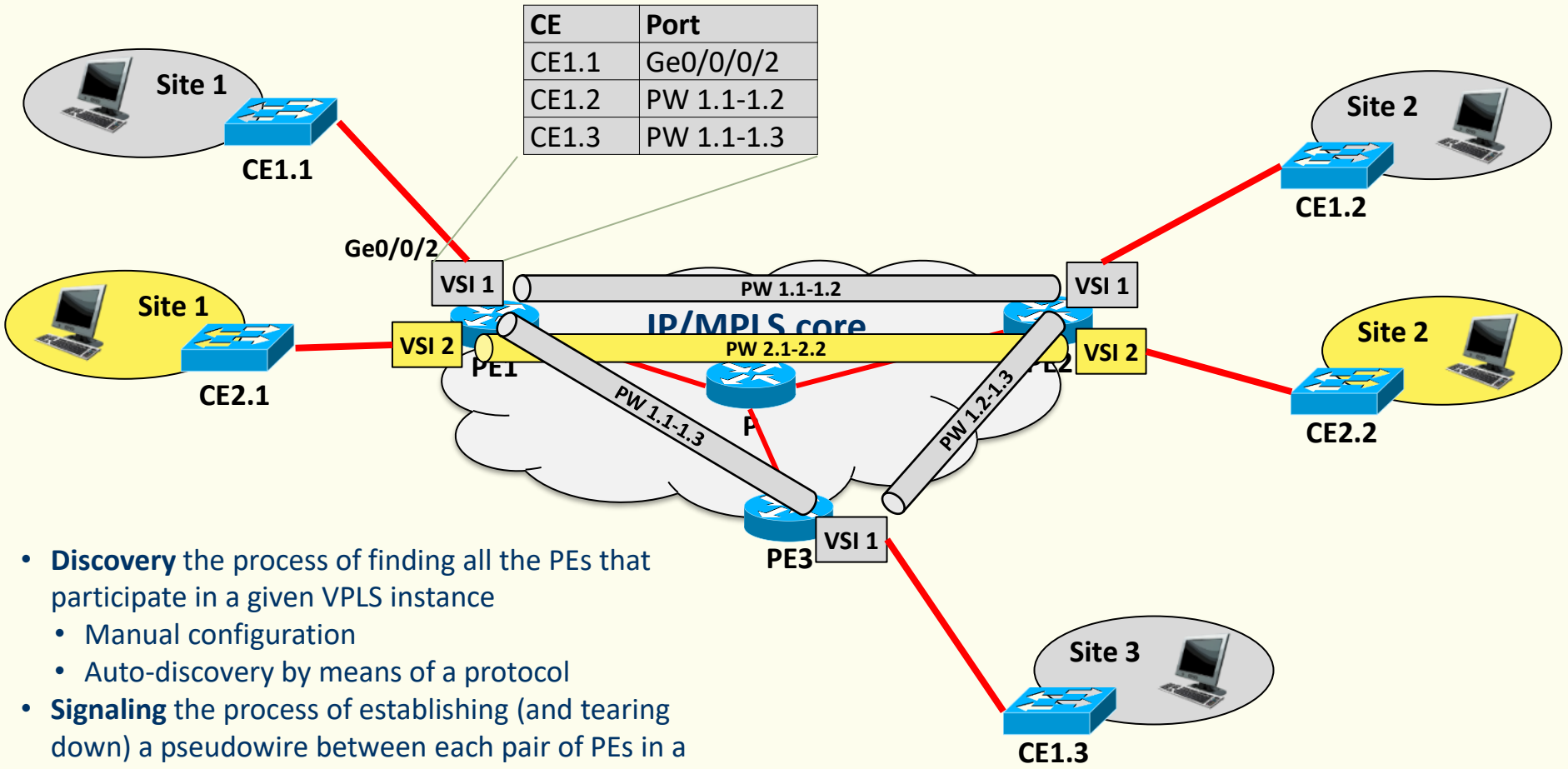


# VPLS – operational model




- **MAC Address learning** automatically learn MAC address-port association
- **Loop prevention** by means of STP
- **Forwarding** MAC table entries used to forward frames
- **Flooding** send unknown BUM (*Broadcast-Unknown-Multicast*) traffic to all other VPLS's VSIs

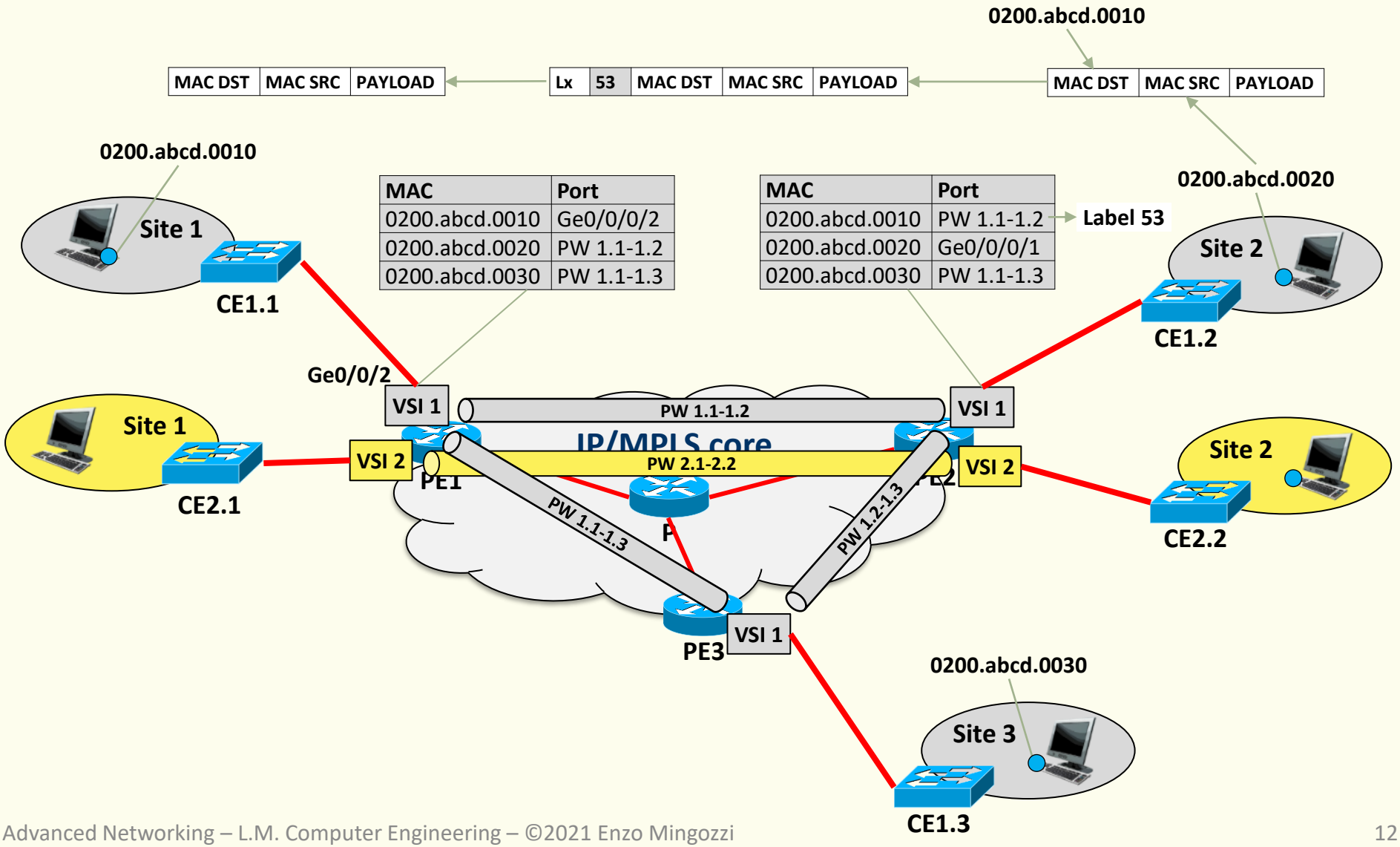
# VPLS – management plane



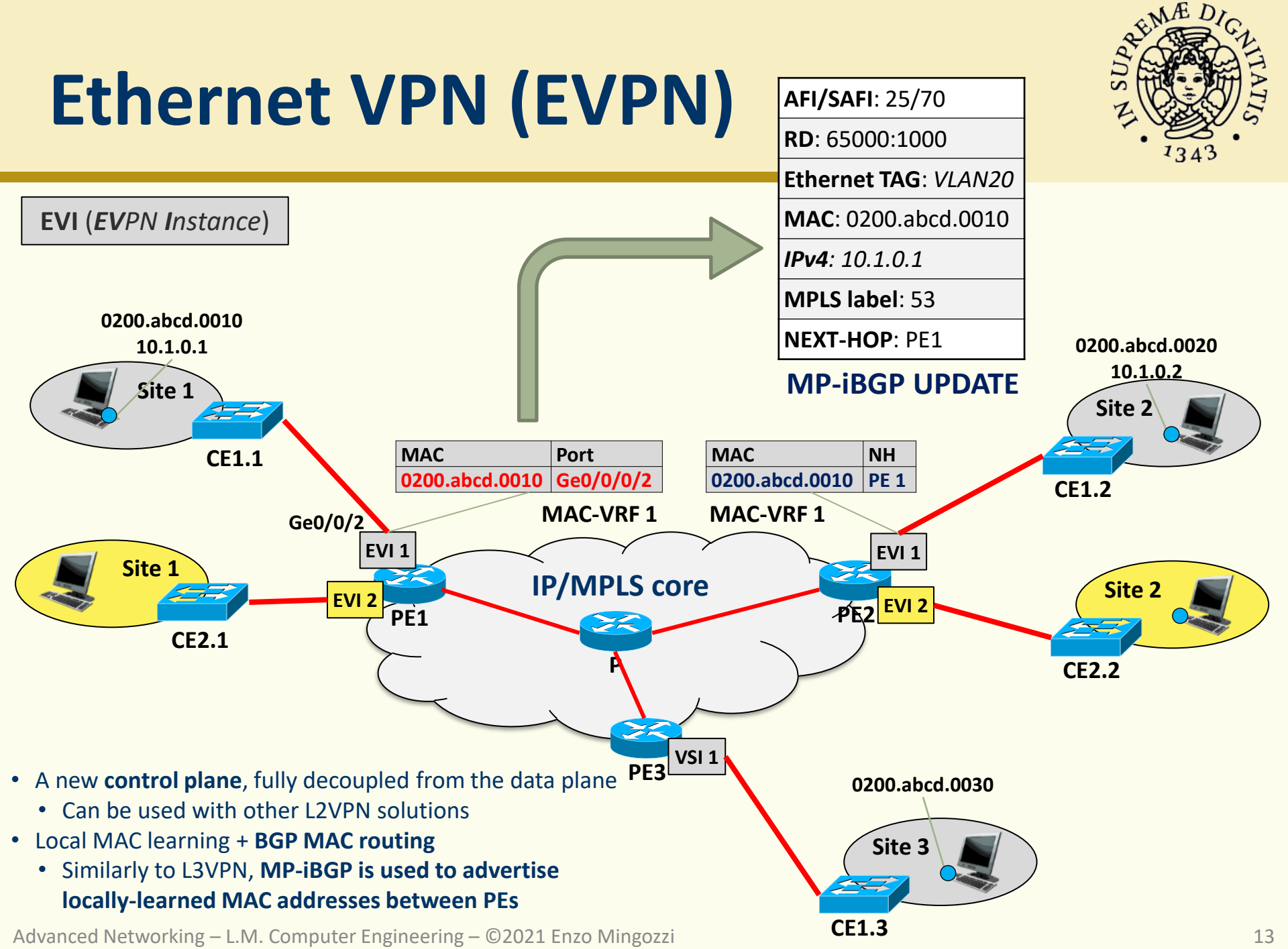

- **Discovery** the process of finding all the PEs that participate in a given VPLS instance
  - Manual configuration
  - Auto-discovery by means of a protocol
- **Signaling** the process of establishing (and tearing down) a pseudowire between each pair of PEs in a VPLS
  - Exchange MPLS labels for demultiplexing over the same PE-PE LSP

**RFC 4761** - ***Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling***

# VPLS – data plane



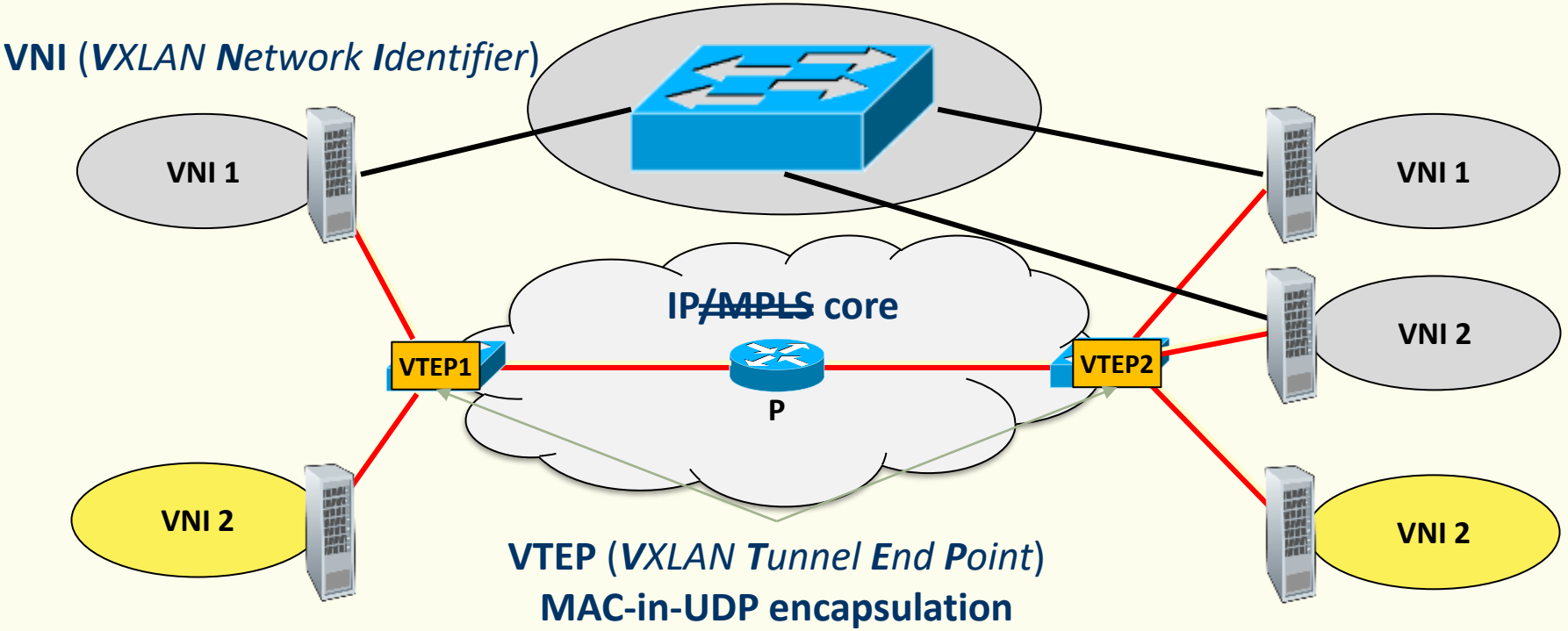
# Ethernet VPN (EVPN)




- A new **control plane**, fully decoupled from the data plane
  - Can be used with other L2VPN solutions
- Local MAC learning + **BGP MAC routing**
  - Similarly to L3VPN, **MP-iBGP is used to advertise locally-learned MAC addresses between PEs**

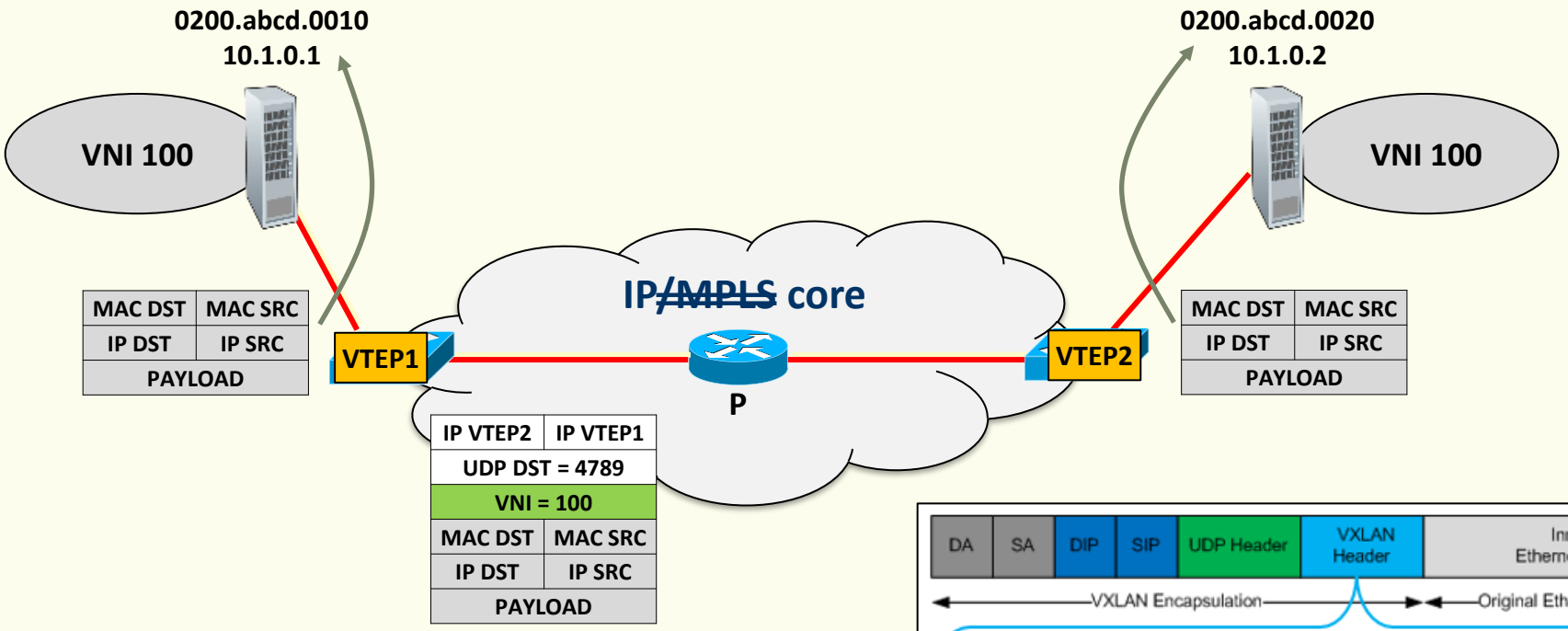
# VXLAN - operation

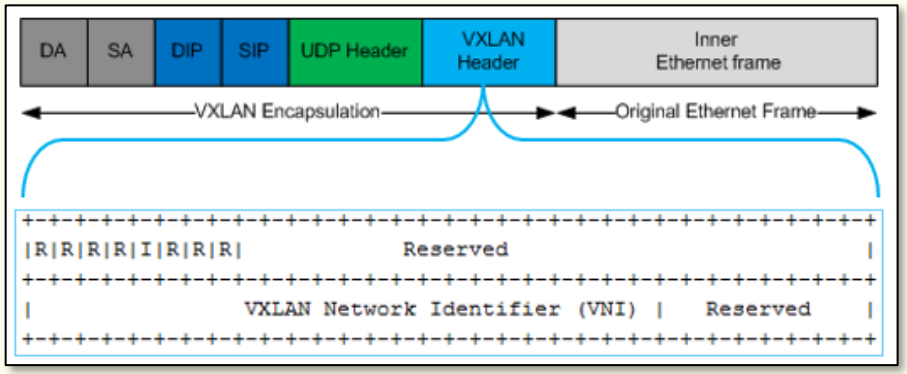
- Transport is realized by an IP network (underlay) *instead of a switched Ethernet*
  - *No need for STP, load balancing over multiple paths*



# VXLAN – data plane

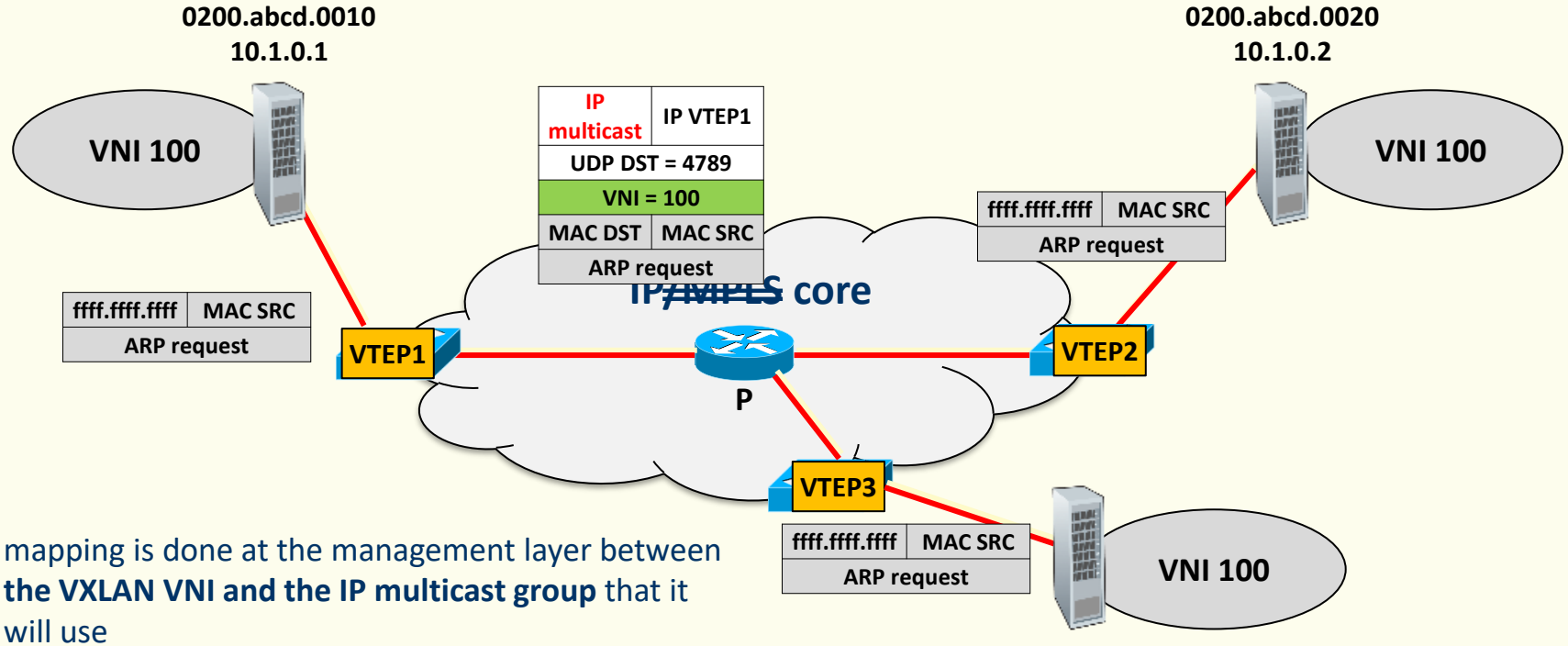
- Frame unicast, MAC-to-VTEP association known



# VXLAN – data plane

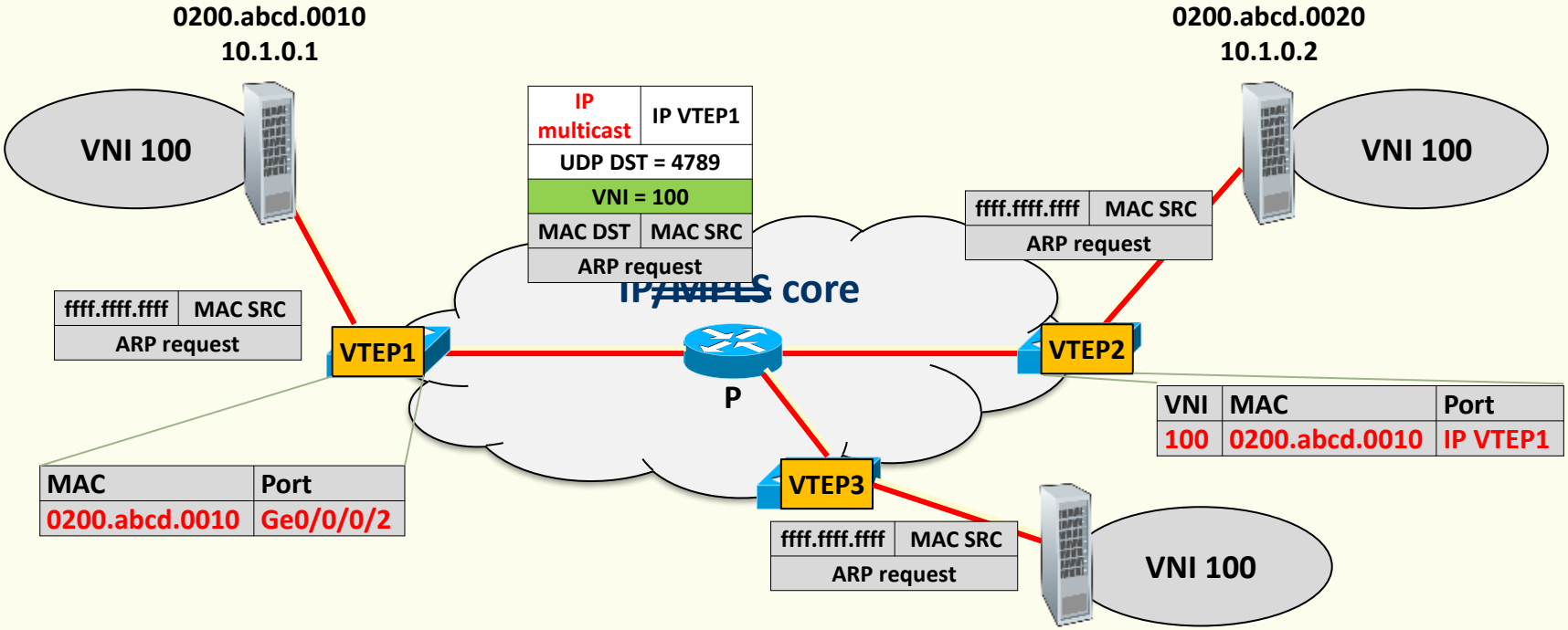
- Frame BUM




1. mapping is done at the management layer between **the VXLAN VNI and the IP multicast group** that it will use
2. use of **multicast routing protocols** like Protocol Independent Multicast - Sparse Mode (PIM-SM see [RFC4601]) to provide efficient multicast trees within the Layer 3 network.

# VXLAN – data plane

- MAC learning




1. Local MAC learning
2. Remote MAC learning

# References

- RFC **4761** –Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
- RFC **7209** – Requirements for Ethernet VPN (EVPN)
- RFC **7348** – Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks
- RFC **7432** – BGP MPLS-Based Ethernet VPN
- RFC **8365** – A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)