

# Virtual Private Networks

---

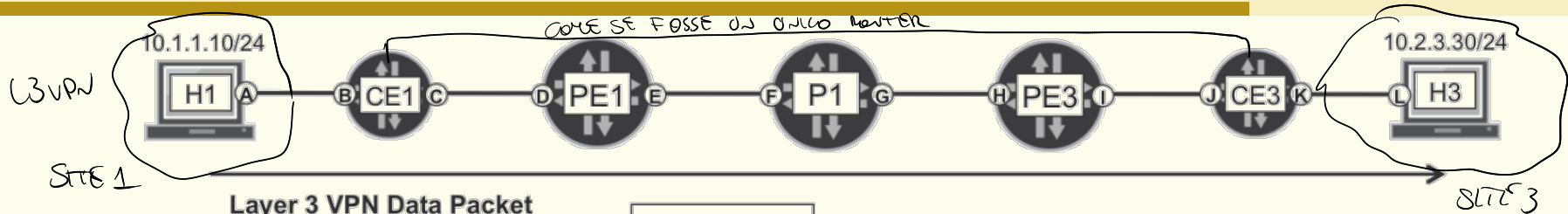
Layer 2 VPNs

Enzo Mingozzi

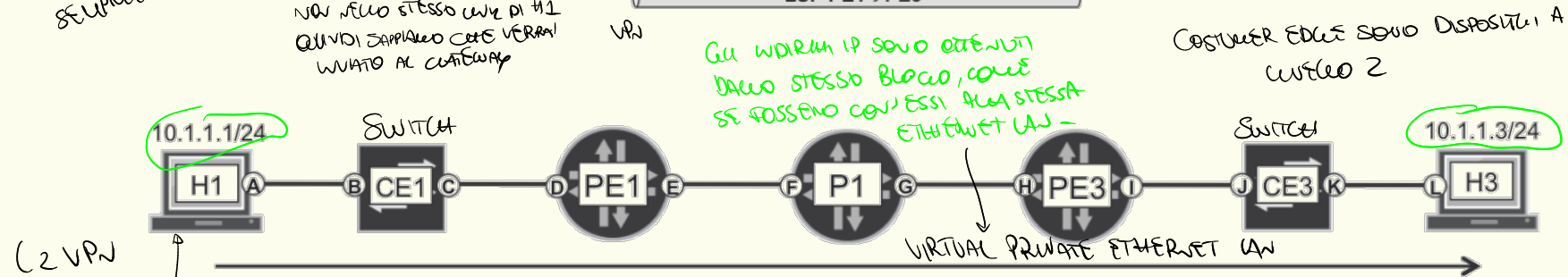
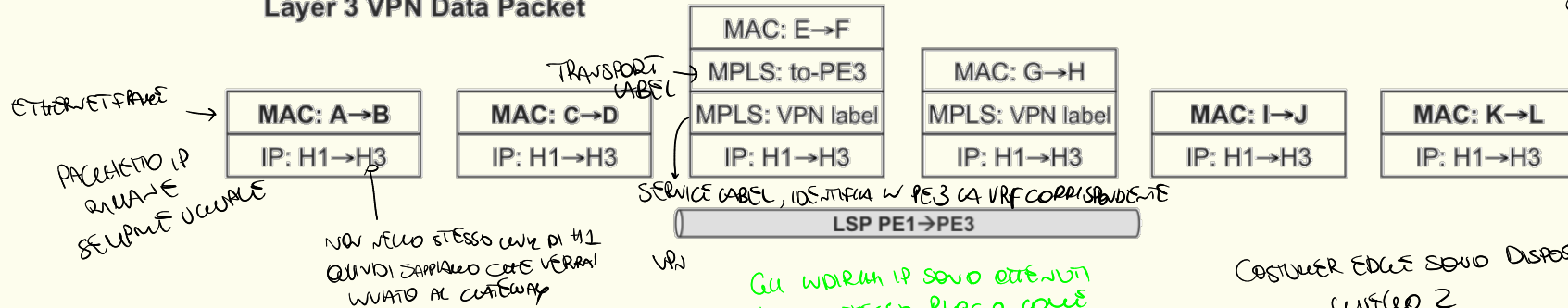
Professor @ University of Pisa

[enzo.mingozzi@unipi.it](mailto:enzo.mingozzi@unipi.it)

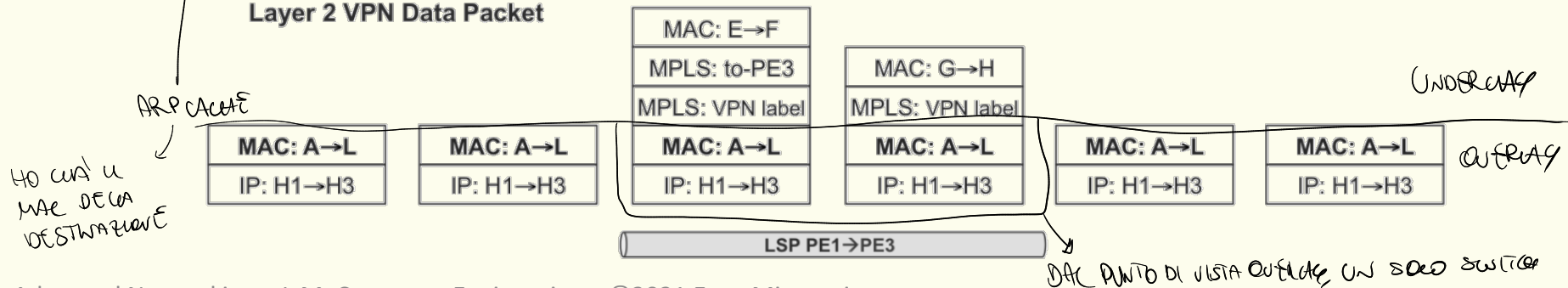
# L3VPN vs. L2VPN



Layer 3 VPN Data Packet



Layer 2 VPN Data Packet

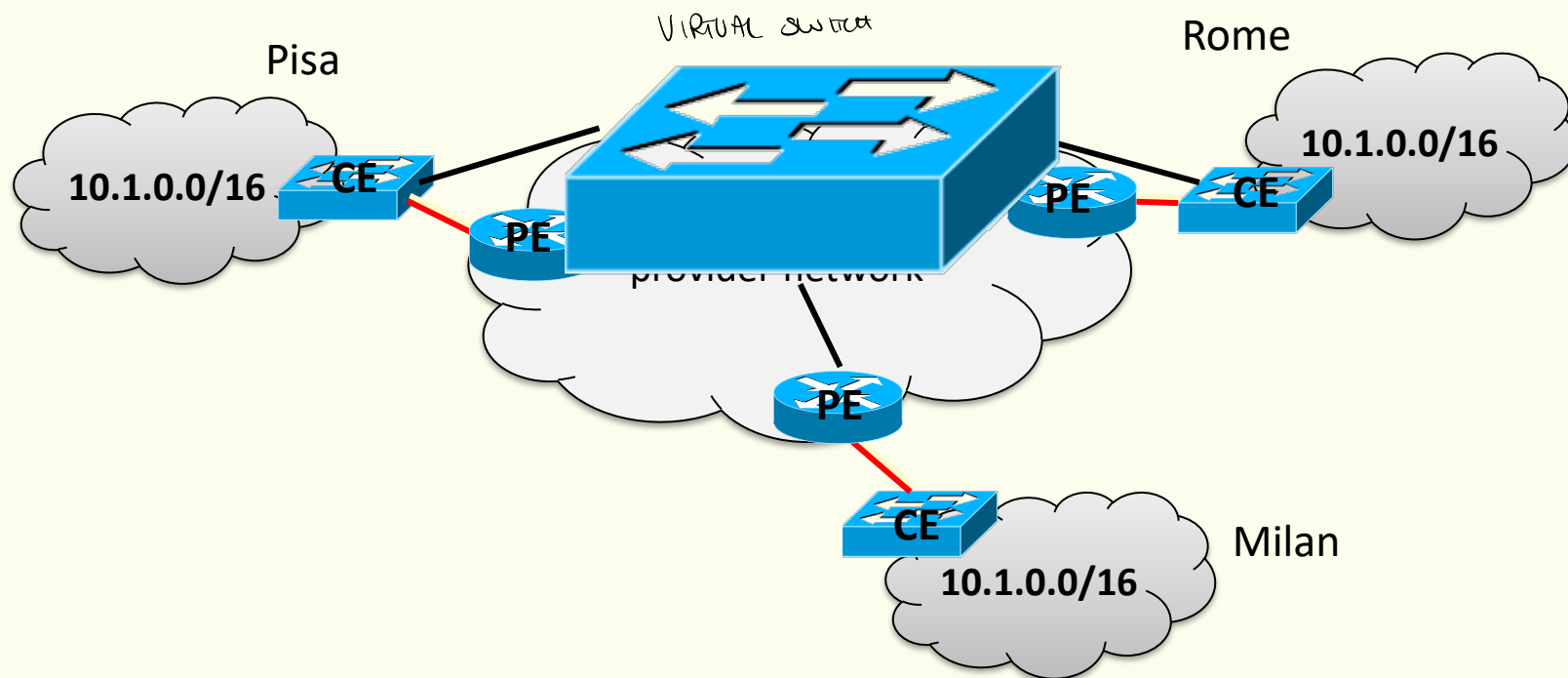


# L2VPN use cases

- 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**

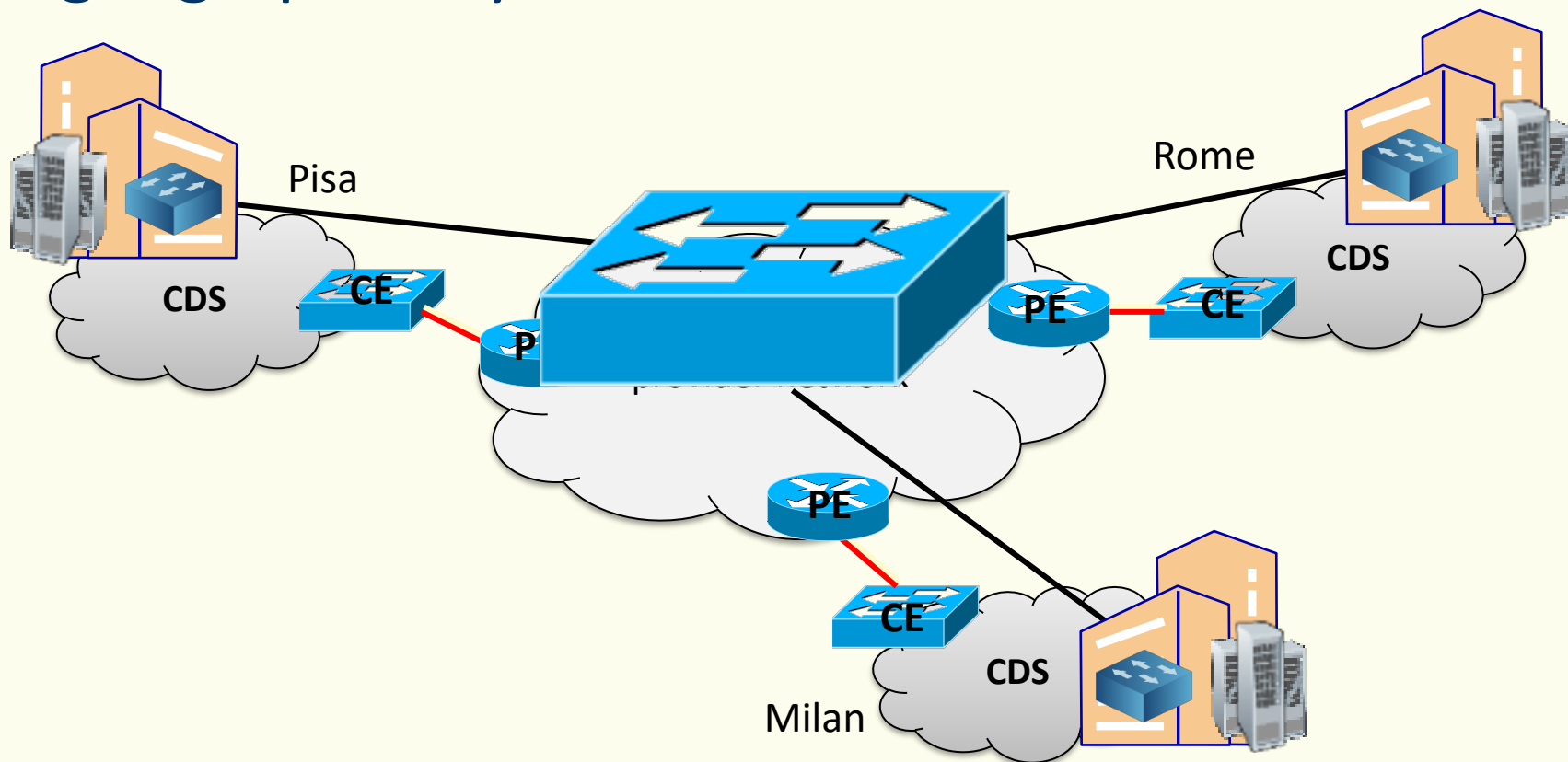
# WAN emulation

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

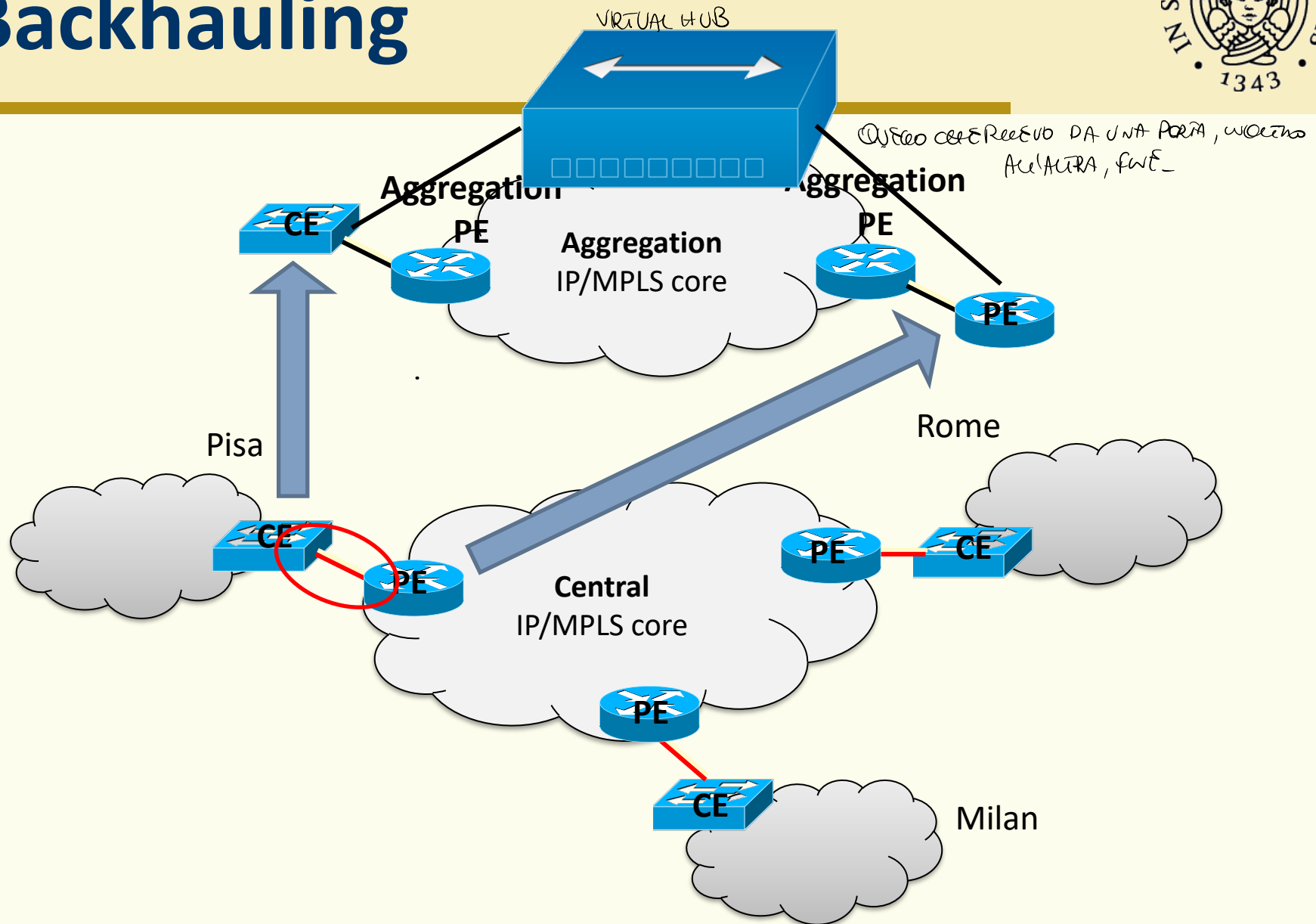


# Data Center Interconnect (DCI)

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



# Backhauling

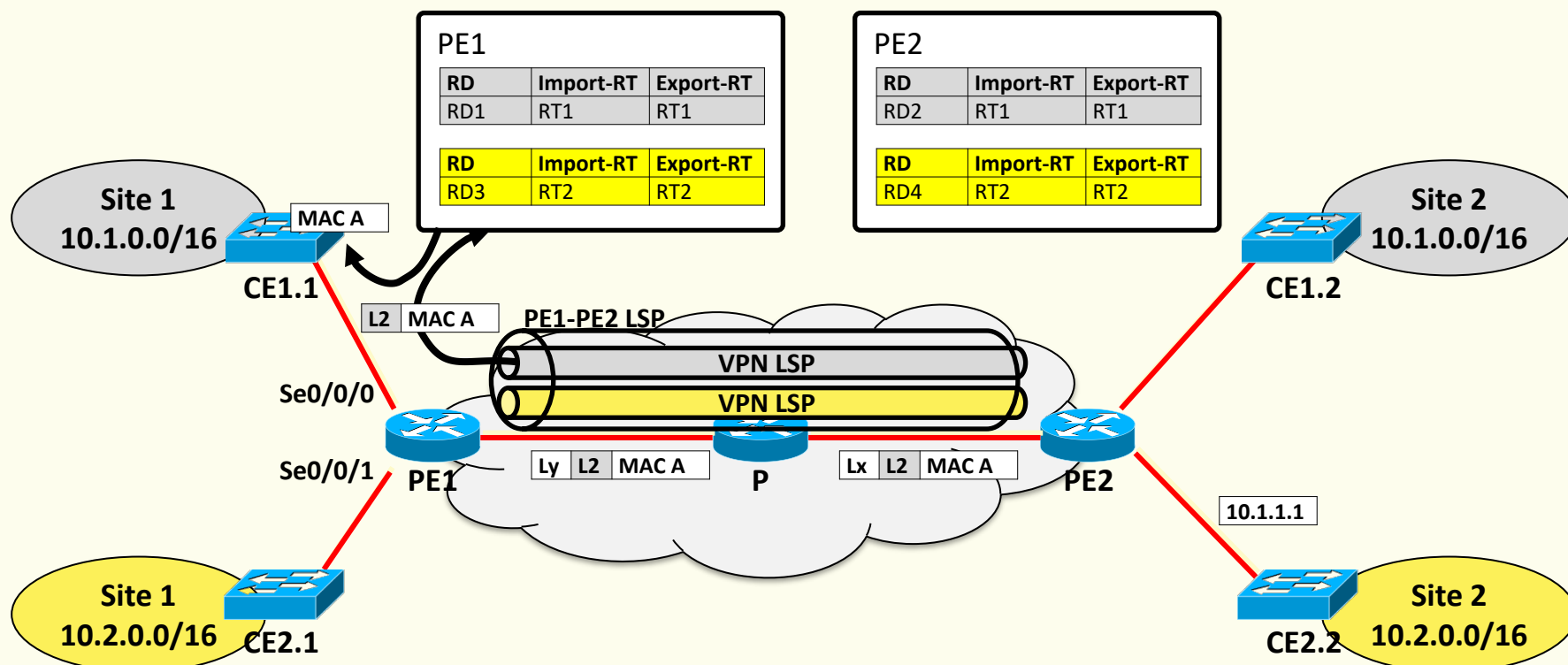


# L2VPN topologies

- 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  $\geq 2$  sites
  - Virtual Private LAN Service (**VPLS**)

# P2P - VPWS

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



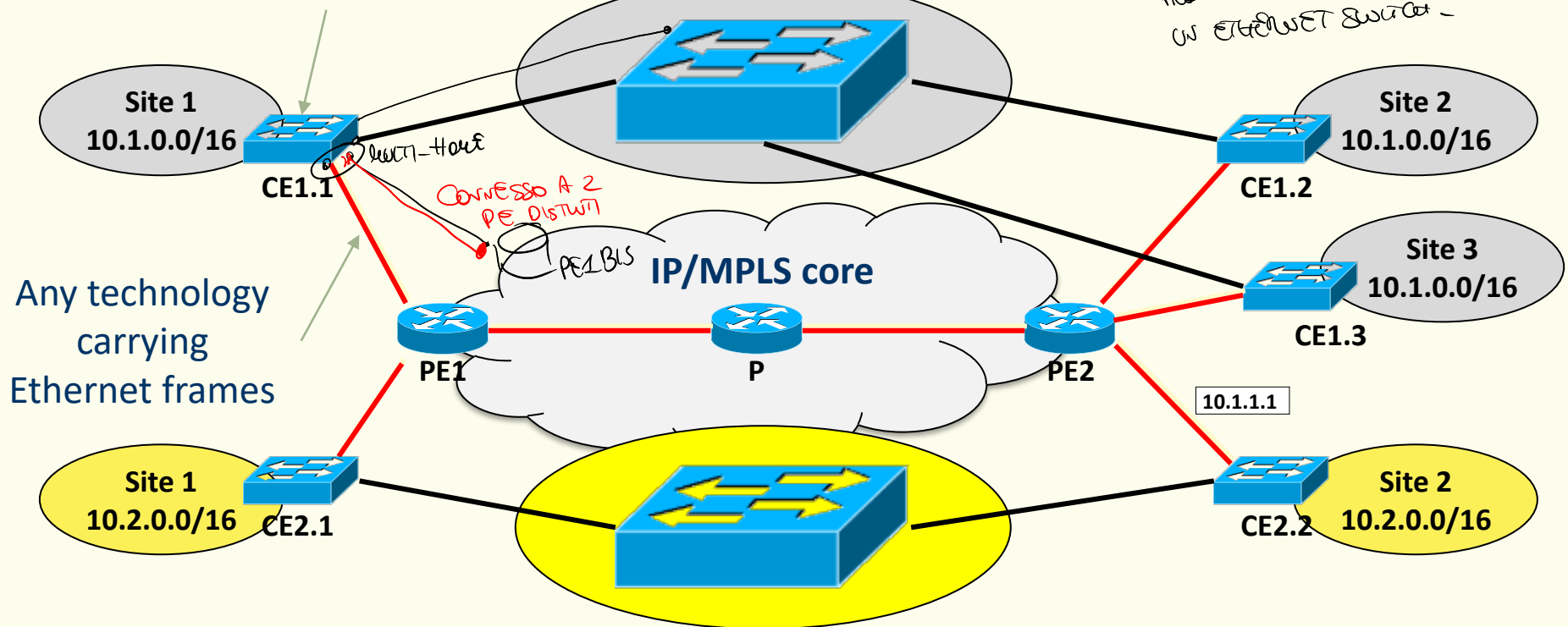


# Virtual Private LAN Service



- Emulate an Ethernet switch

Any device sending and receiving Ethernet frames (tagged or untagged)



WOLFFSTA PERCHÉ  
MANCA UNA ID  
WOLFFSTA PERCHÉ  
C'È WOLFFSTADT DEL C.E.

→ PAR+ALLENTE  
W COMPTA  
E W COMSTA

## VIRTUAL SWITCH INTERFACE

VFT

CE	Port
CE1.1	Ge0/0/0/2
CE1.2	PW 1.1-1.2
CE1.3	PW 1.1-1.3

VIRTUAL FORWARDING INSTANCES ~ MAC TABLE

↳ UNA PER OVA VST

BRIDGE - DOWN

## Site 2



**CE1.2**

NOU C'É U MAC DECA PORTA  
NECA UFI TROVO U MAE DEU

Ge0/0/2

1. 1st 2

→ ① SECO STESSO PT O  
PT STESSO W UN Aera

→ ~~POWT-TO-POWT LEAK CASE~~  
EL UNA VLAUDI

no 2 SPECIALE,  
con solo 2 nodi.

## Site 2



## CE2.2

Puo' ESSERE (E DI  
SOLO E) CONSTATO  
A PU' PE

PERCHÉ DEVE ESSERE W  
CERCAO DI ESSERE W  
STP? NON HO COO W  
PROVEREN NETWORK PERCHÉ FUN MISTO

QwI VSI E' CONNESSA AD QwI ALTRA  
VSI NEI BRUCIE DONATI ATTRAVERSO  
UNO PSEUDOWIRE -

## LIABILITY

- **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

CE = VPS

PERSONAL CUSTOMER SERVICE  
CARE & SUPPORT  
THE US COOP! QUALITY  
SERVICE

### Site 3

**CE1.3**

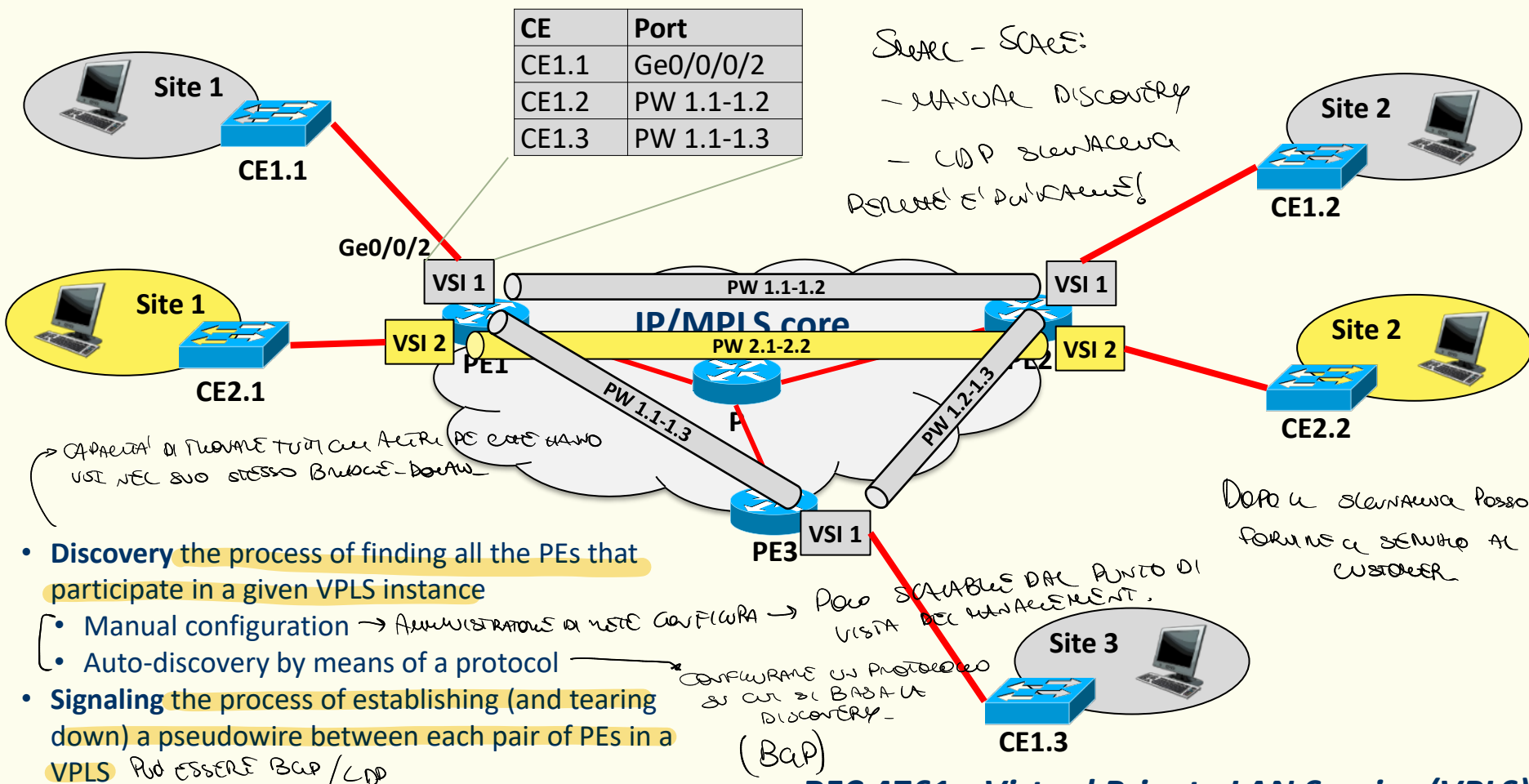
Product - Home Customer  
New Pool Osborne  
1 unit  
Shower - Active

↳ Per questo ho bisogno di fare mesh

→ Quando Recebo o Budget vouo a TIRE e FAZME USE  
TRAVE QUELA DA CRI SEI E! ARRENTIA -

CE USI COTTE CO  
RILASCIANO, NON LE UNGUANO  
DI NUOVO - 10

# VPLS – management plane



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

Wordetto di A  $\rightarrow$  0200.abcd.0010



# Ethernet VPN (EVPN)



## EVI (EVPN Instance)

NON USO IL TRADIZIONALE MAC  
LEARNING DI UN  
ETHERNET  
SWITCH MA  
USO UN  
PROTOCOLLO DI  
CUI SOLO  
SUPERMARE.

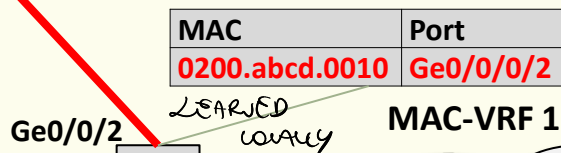
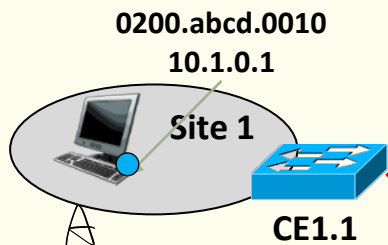
A COSA SERVE?

OTTIMIZZAZIONE DI SPACIO  
SE A VOI VE W/AVE UN  
MESSAGGIO A B CONVOSE  
IL SUO IP, ANZI DI DEVE  
USARE PER PER NECESSARIE MAE

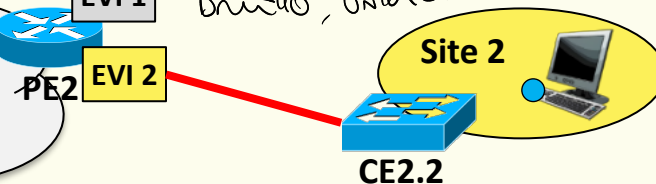
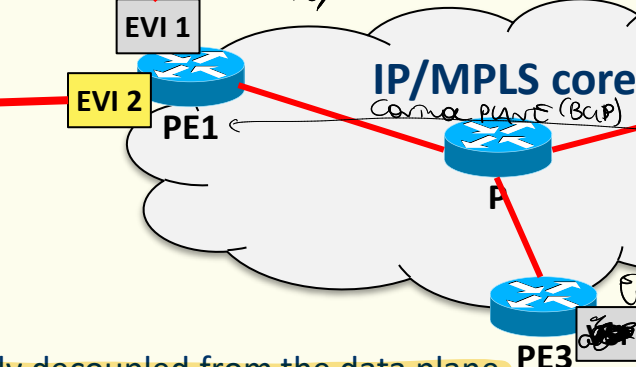
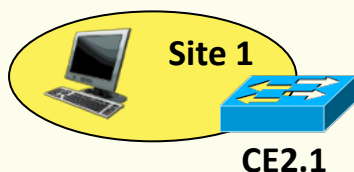
## MP-iBGP UPDATE

AFI/SAFI: 25/70	TRANSPORTANDO W FORMAZIONE EVPN
RD: 65000:1000	
Ethernet TAG: VLAN20	
MAC: 0200.abcd.0010	MAC ADDRESS W/VE DI W/VE UN IP
IPv4: 10.1.0.1	
MPLS label: 53	SERVICE LABEL
NEXT-HOP: PE1	

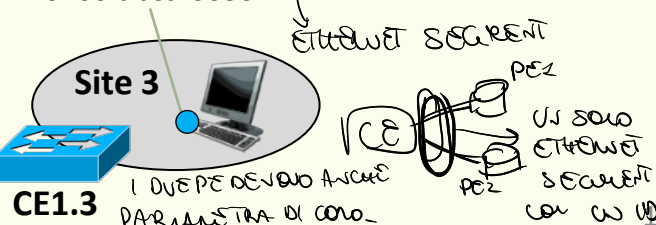
MAC ADDRESS sono  
FCAT  
0200.abcd.0020



MESSAGGIO  
AND E  
RISPONDE,  
PE2 NON DEVE FARE BRODCAST  
PERCHÉ SA CHE A CEN È  
DISTRIBUITO, UNICAST.



LEVEL1 - HARD CUSTODI STAGE DEVEI  
POSSO SECCARE SE USARE SWAPS - ACTIVE  
OPPURE FARE COB BALANCE  
0200.abcd.0030



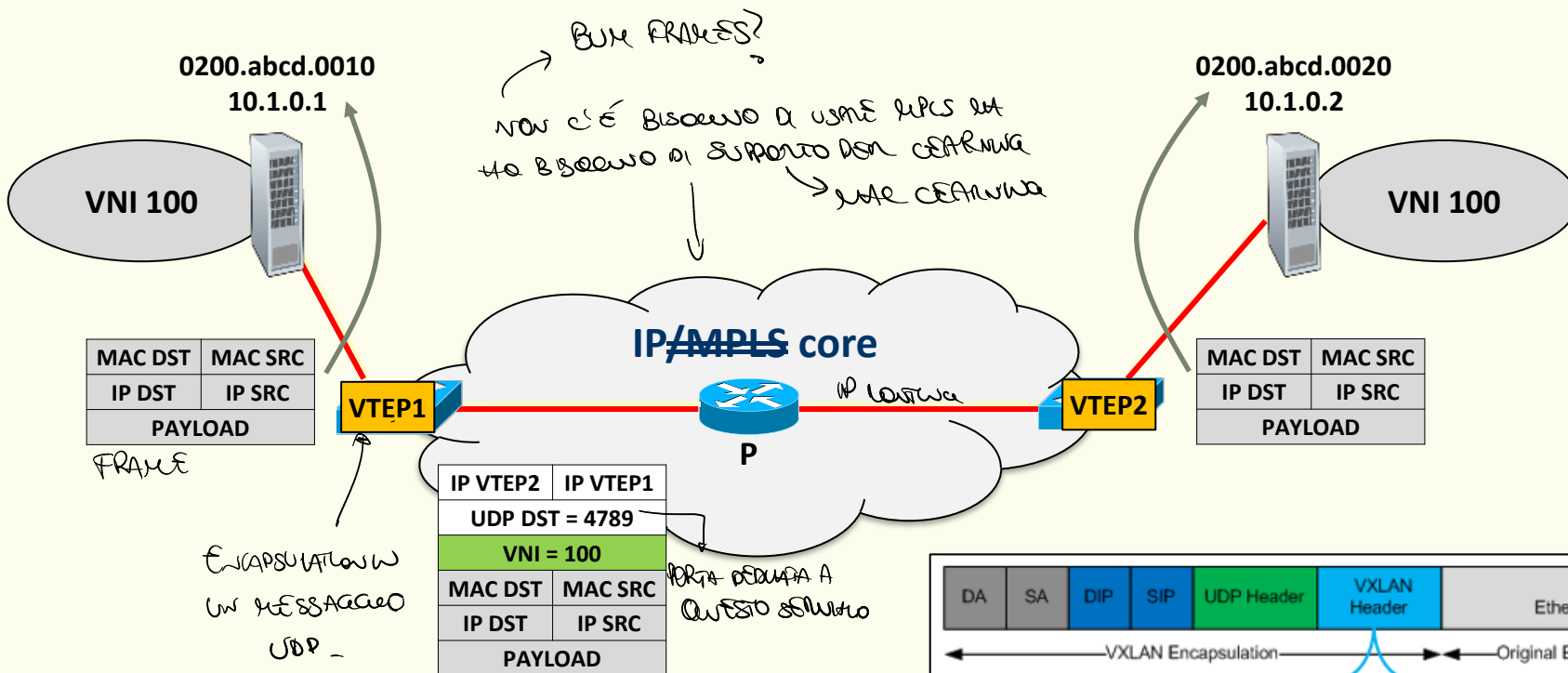
- A new **control plane**, fully decoupled from the data plane
  - Can be used with other L2VPN solutions
- Local MAC learning + **BGP MAC routing**
  - Similarly to L3VPN, **MP-iBGP is used to advertise locally-learned MAC addresses between PEs**



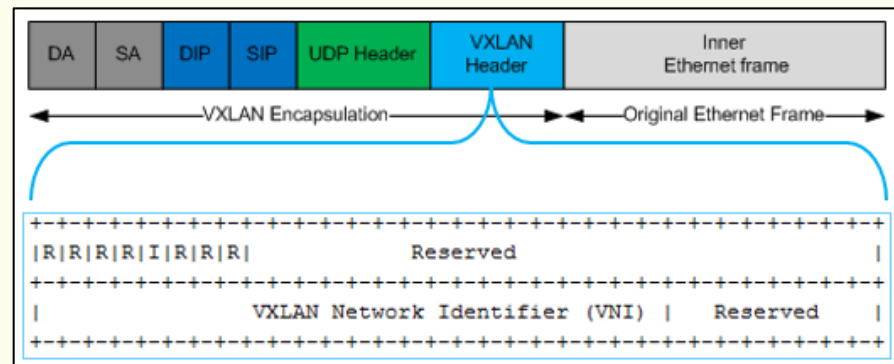


# VXLAN – data plane

- Frame unicast, MAC-to-VTEP association known

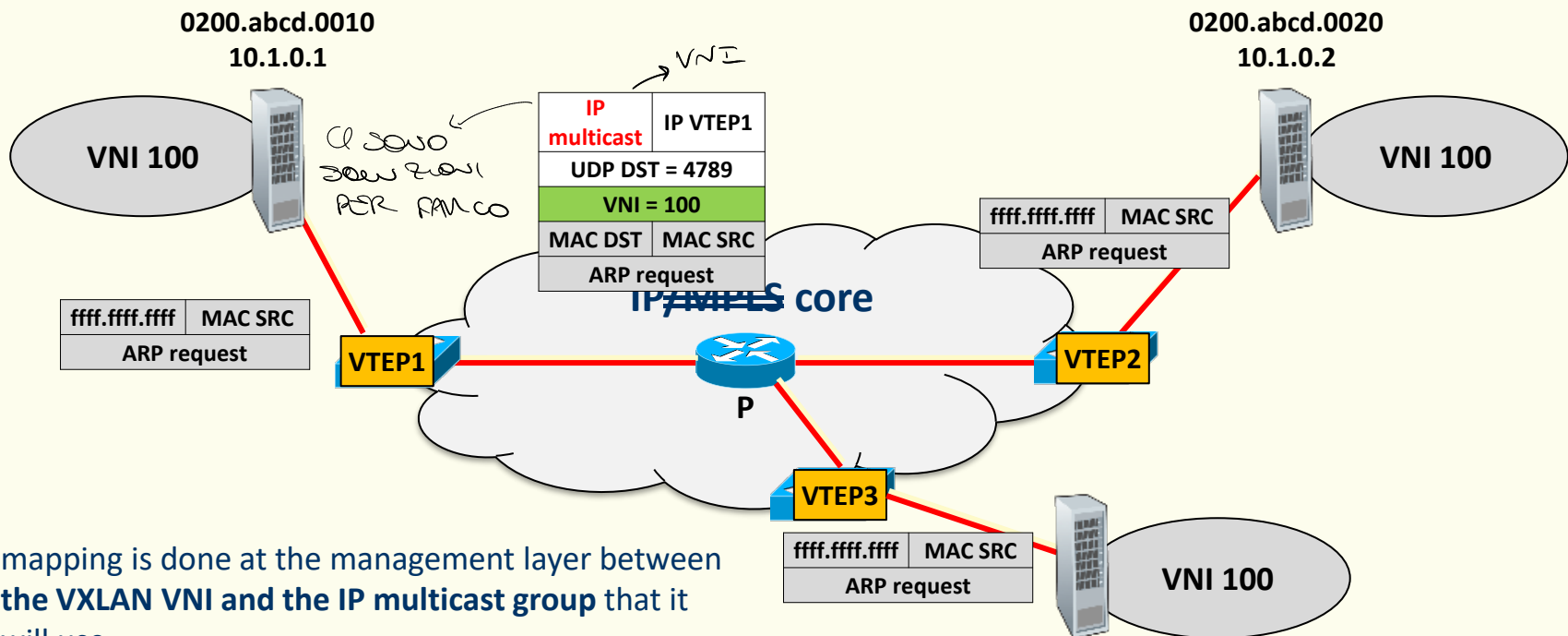


VLAN ID sono codificati in 12 bit che non sono abbastanza per  
questo VNI sono su 24 bit.



# VXLAN – data plane

- **Frame BUM** → Ho bisogno di supporto ad IP multicast nella underlay network.

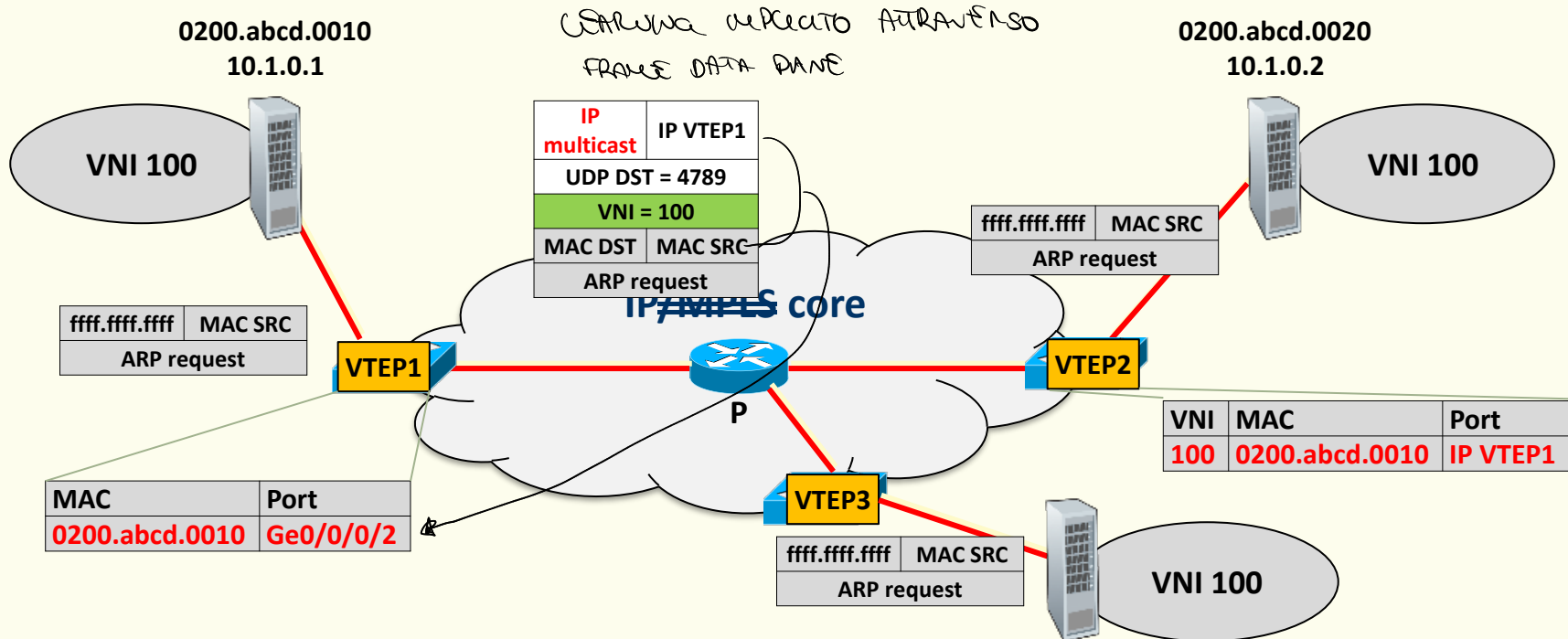


1. mapping is done at the management layer between the **VXLAN VNI** and the **IP multicast group** that it will use
2. use of **multicast routing protocols** like Protocol Independent Multicast - Sparse Mode (PIM-SM see [RFC4601]) to provide efficient multicast trees within the Layer 3 network.



# VXLAN – data plane

- MAC learning → ESAGHERATE QUELLO ASPETTANDO SENZA PROTOCOLLO DI SUPPORTO



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)