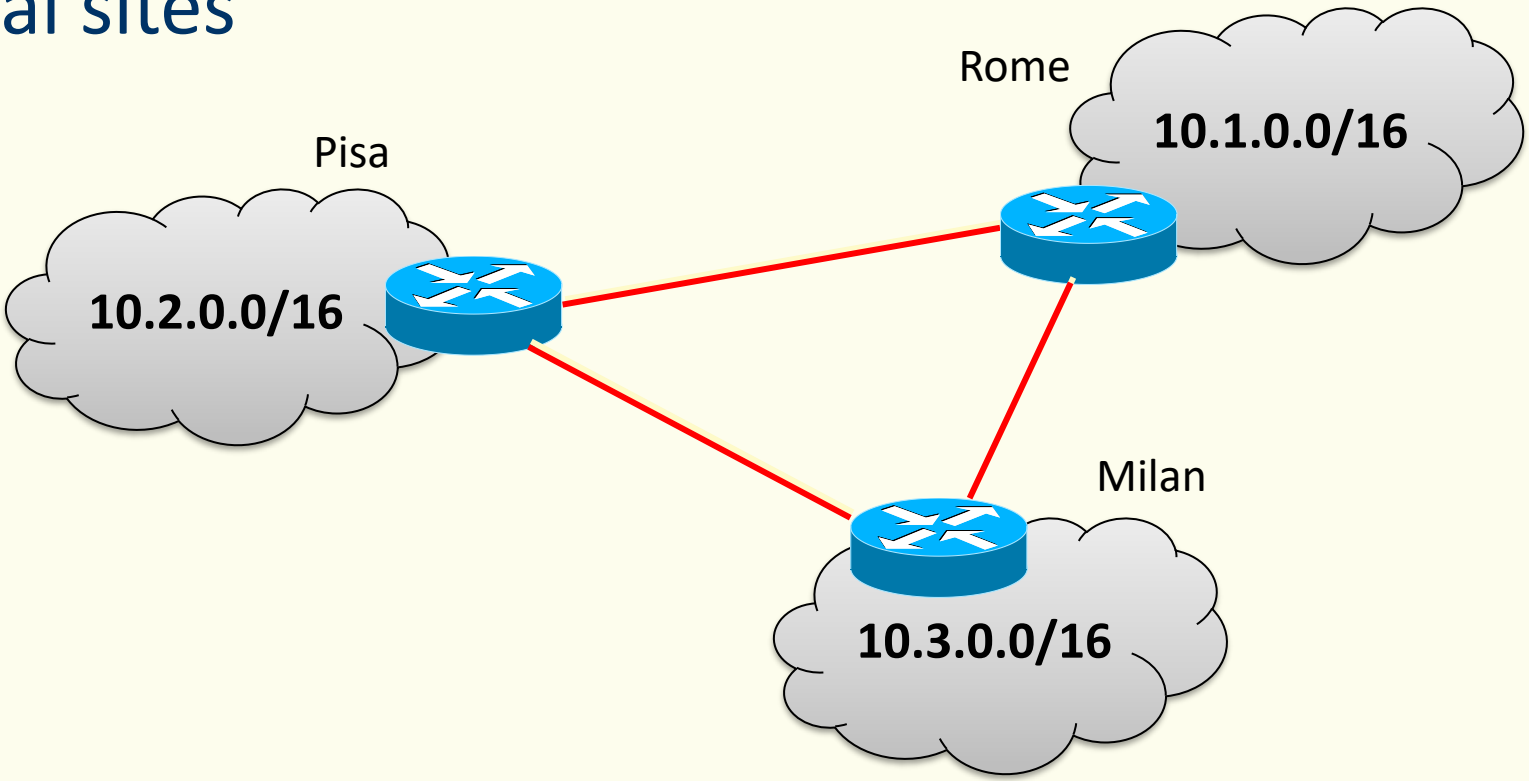
Virtual Private Networks

BGP/MPLS IP VPNs

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

Corporate WANs

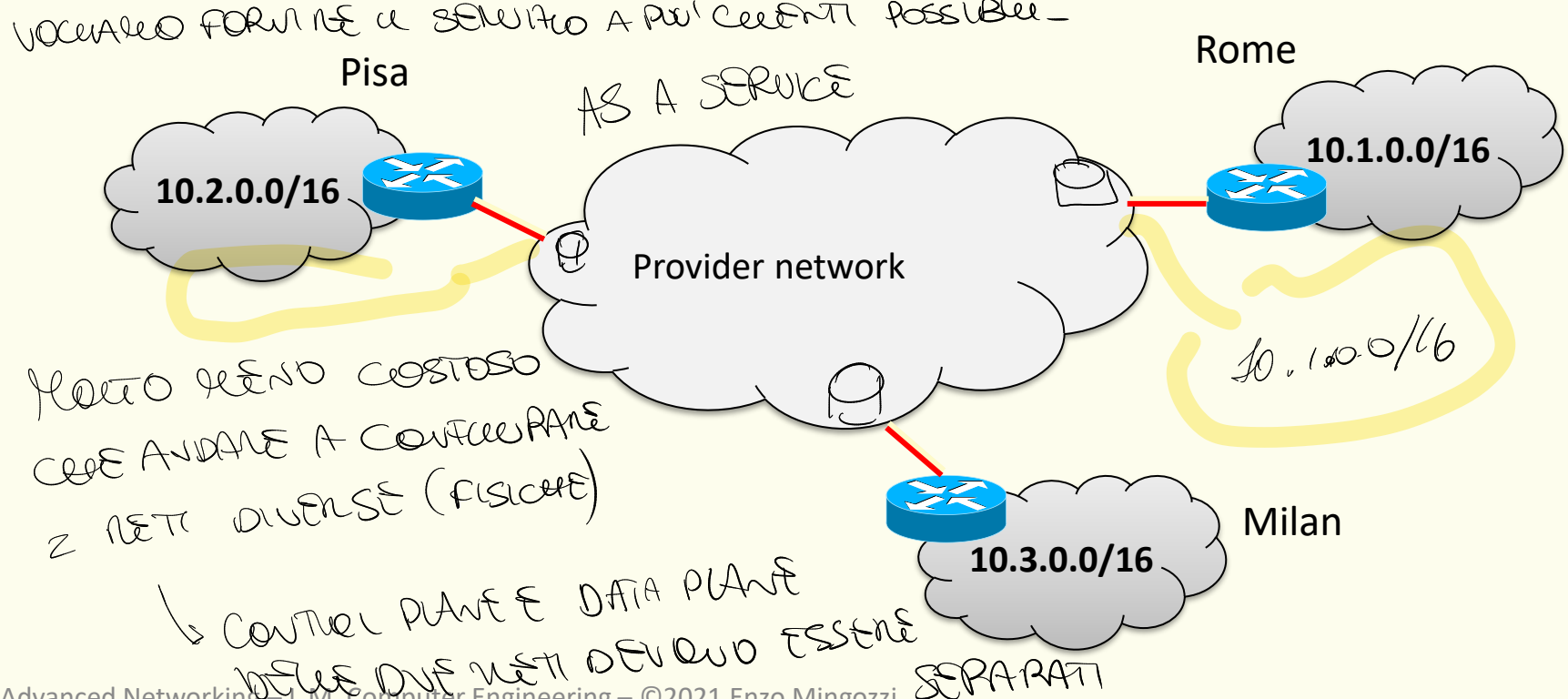
- The Wide Area Network (WAN) infrastructure is the set of links interconnecting border routers at local sites



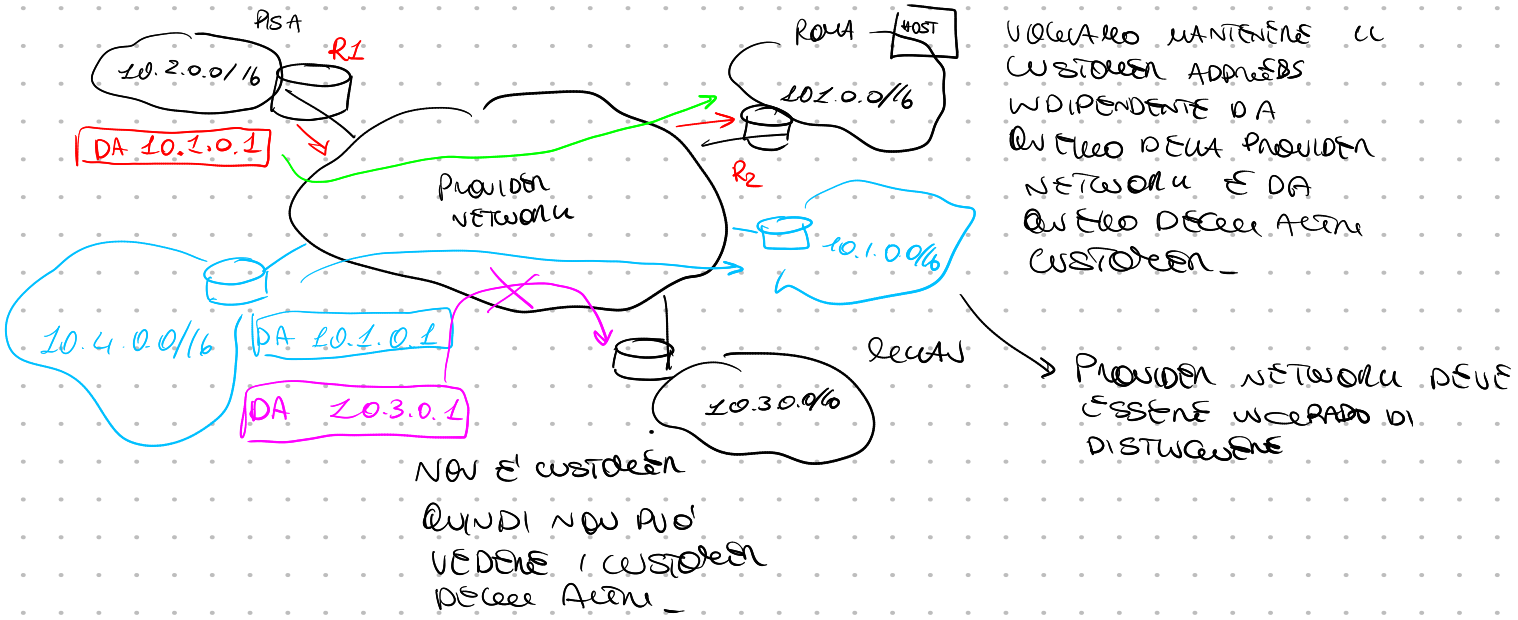
Virtual Private Networks

VPN SERVICE A BUSINESS CONSUMER

- **Private**: exclusive use, independent addressing and routing (COME UNA RETE FISICA)
- **Virtual**: the actual infrastructure is shared



HO RETI GEOGRAFICAMENTE SEPARATE, COME SERVIZIO STO OFFRENDO?



VOGLIAMO MANTENERE LE CUSTOMER ADDRESS INDIPENDENTE DA QUELLO DELLA PROVIDER NETWORK E DA QUELLO DELLE ALTRE CUSTOMER.

RICAN → PROVIDER NETWORK DEVE ESSERE INCARICATO DI DISTINGUERE

NON È CUSTOMER QUINDI NON PUÒ VEDERE I CUSTOMER DELLE ALTRE.

POSSIAMO ACCOPPIARE QUALCOSA AL PROTOCOLLO IP PERCHÉ ABBIAMO ADDRESS OVERLAPPING E PERCHÉ POSSIAMO METTERE DEI VINCOLI AL TRAFFICO

↓

INDIRIZZI USATI DUE VOLTE

R1

10.20.0.0/16	50

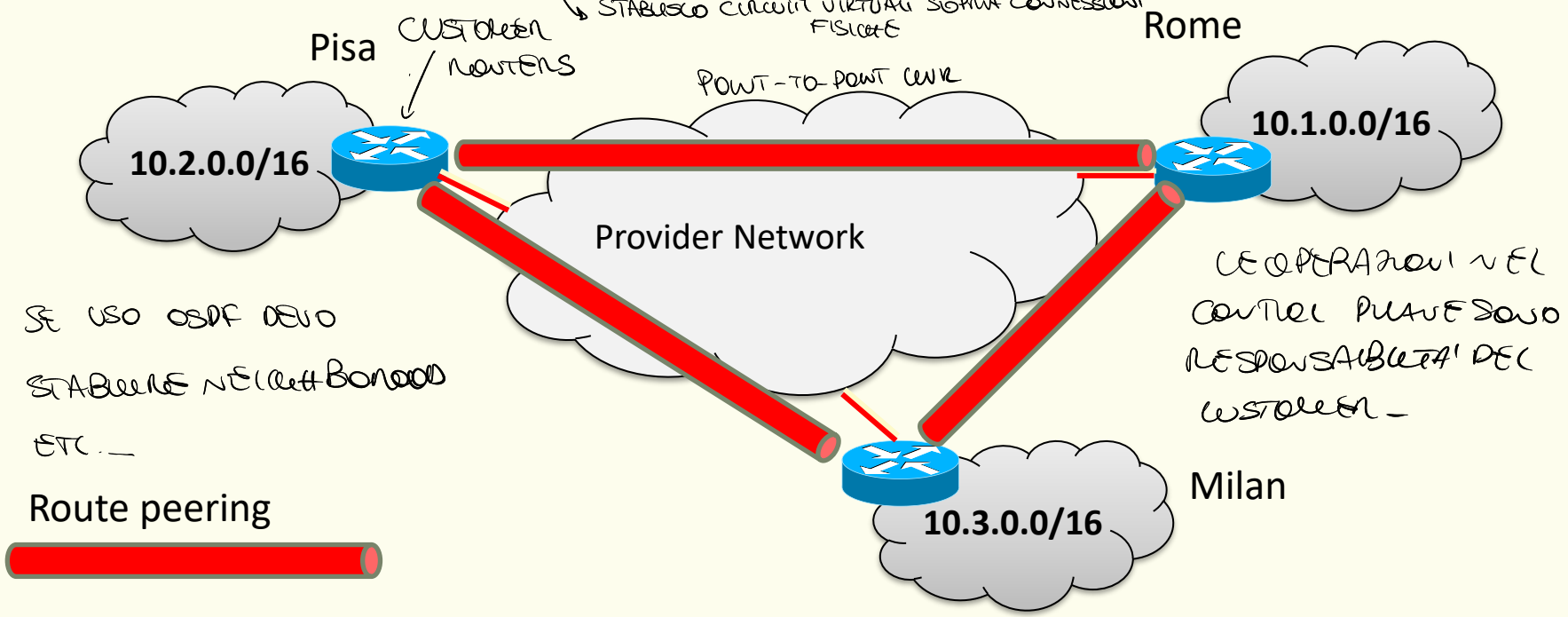
ROUTING TABLE

COME FANNO I ROUTER AI BORDI DELLE RETI CUSTOMER A CONOSCERE LE ALTRE RETI?

- DEFAULT ROUTE?
  PRO: NON HO BISOGNO DI DYNAMIC LEARNING
  CONTRO: COSTOSO AD OGNUNO TRAFFICO AGGIUNTO SE MANCANO PUBLIC

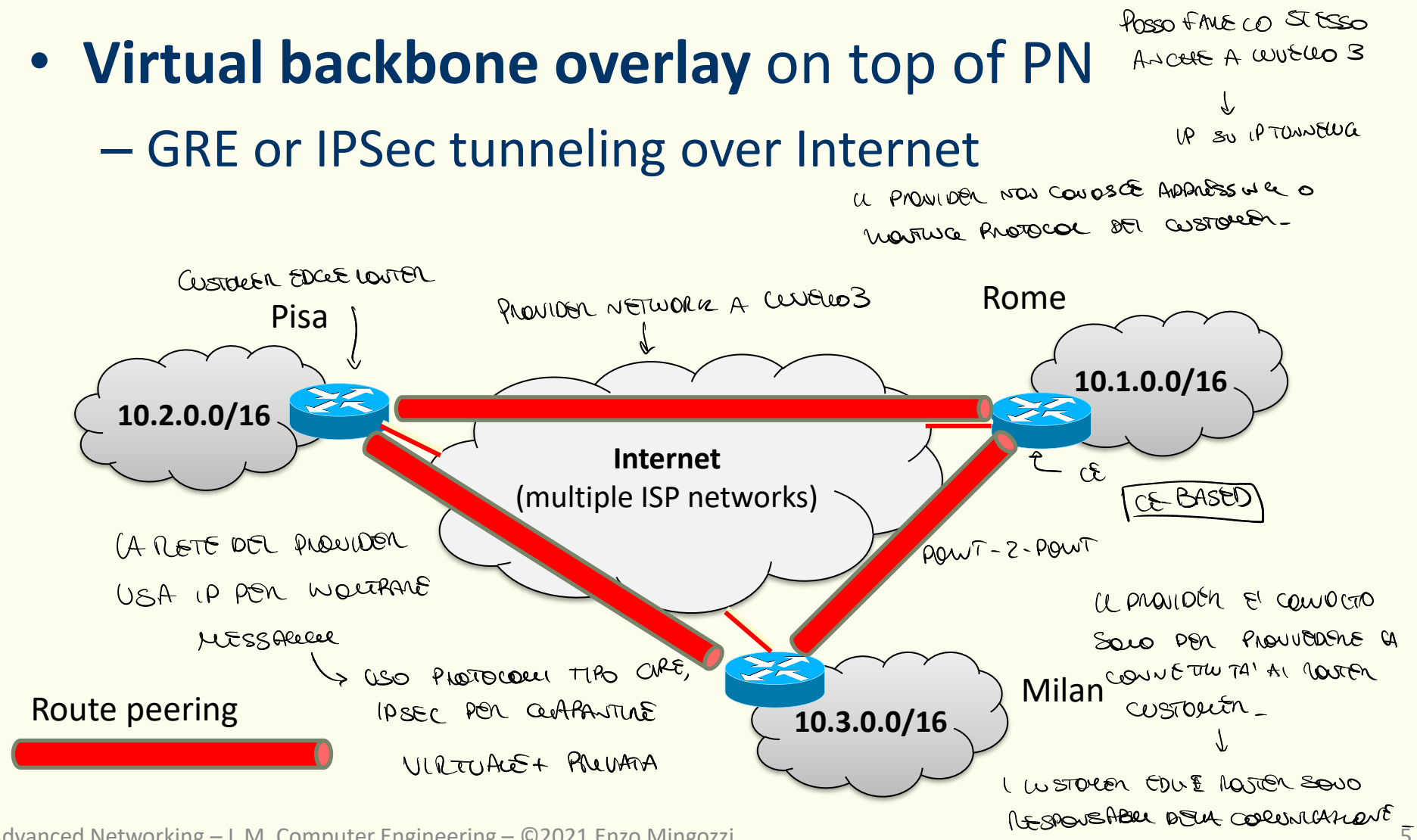
Virtual CE-CE links

- **Virtual backbone overlay** on top of PN
  - Leased lines (L1, dedicated circuit)
  - Frame Relay (L2, pachet switched) (ATM)



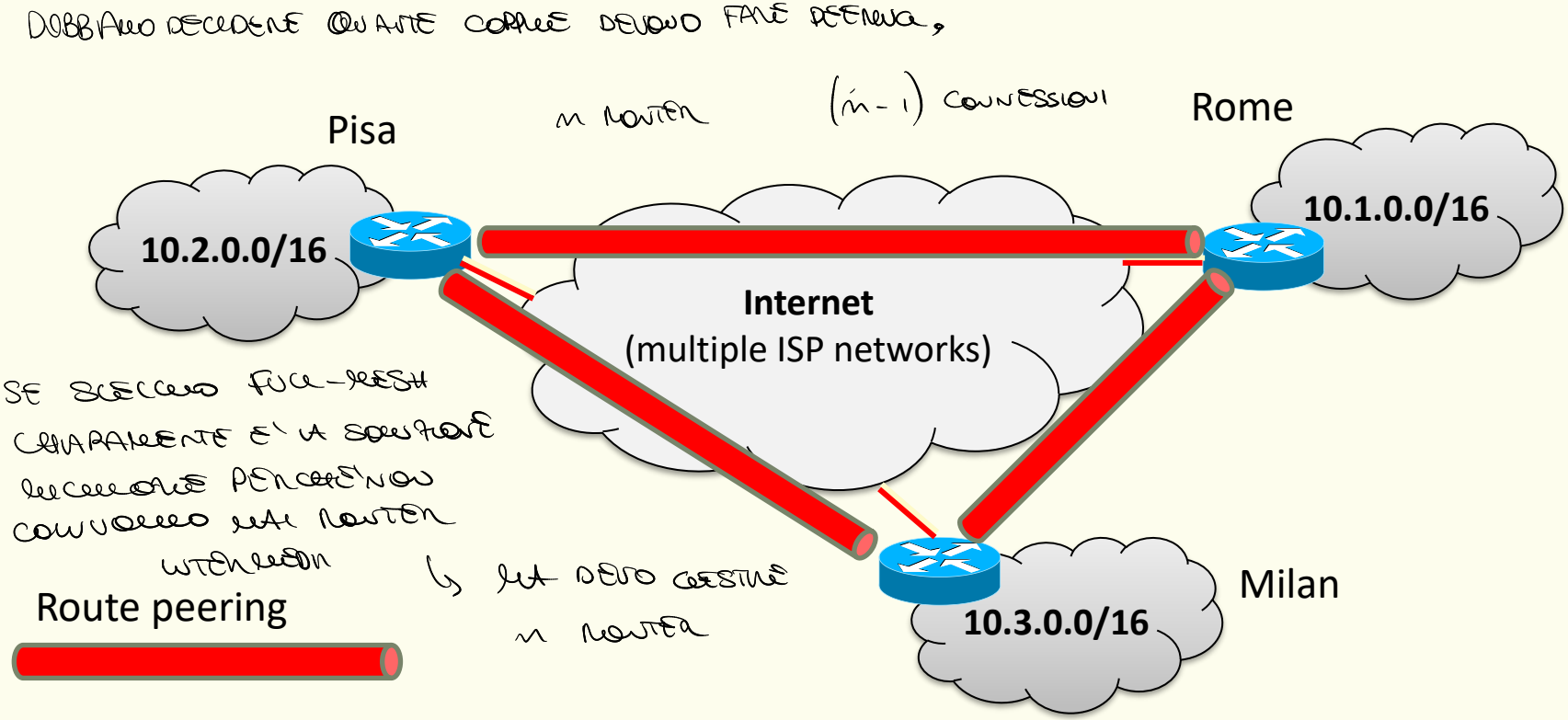
Virtual CE-CE links

- **Virtual backbone overlay** on top of PN
  - GRE or IPSec tunneling over Internet



Virtual CE-CE links

- CE routers at different sites **peer with each other**
- The overlay is ***visible*** to the VPN's **routing algorithm**



Virtual CE-CE links

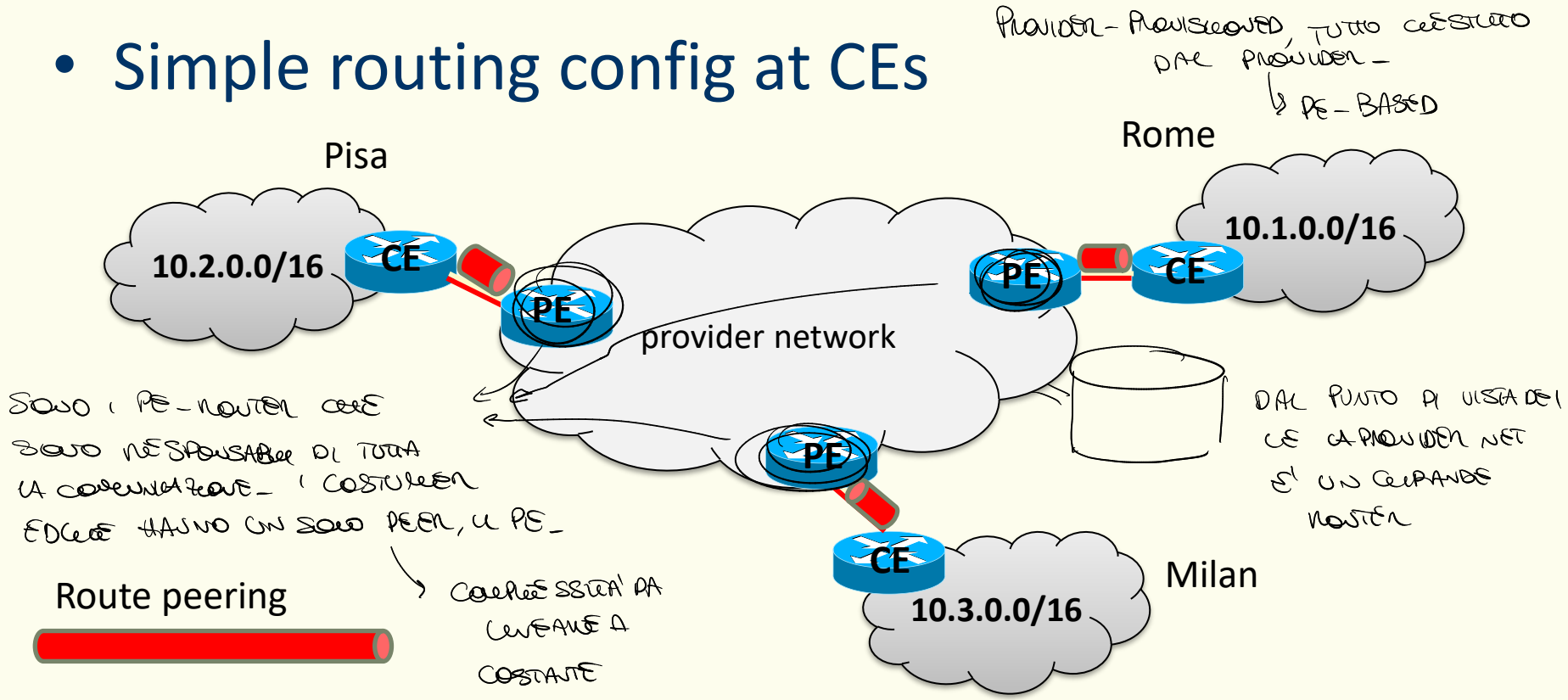
- **Pros**
  - Achieves the fundamental goals of a VPN
    - Connectivity, private addressing, privacy of traffic
- **Cons**
  - VPN is implemented by Customer Edge (CE) routers
    - Requires network management expertise
  - IGP scaling routing limitations (mesh of CE peers)
  - Amount of configuration required for adding a new site
  - If provider managed
    - Scaling of management limitations with multiple customers

DAL PUNTO DI VISTA DEL PROVIDER QUESTA SOLUZIONE NON È OTTIMALE PERCHÉ NON È FACILE CONTROLLARE MOLTI CE-

DATI I PUNTI 3 CONTRO: DAL PUNTO DI VISTA DEL CUSTOMER HO IL SERVIZIO DA PERSONE TROPPO DI MIA COMPETENZA. IL PROVIDER PUÒ FARSI CARICO DI AL CUNE RESPONSABILITÀ. IL PROVIDER PUÒ GESTIRE IL CUSTOMER-EDGE.

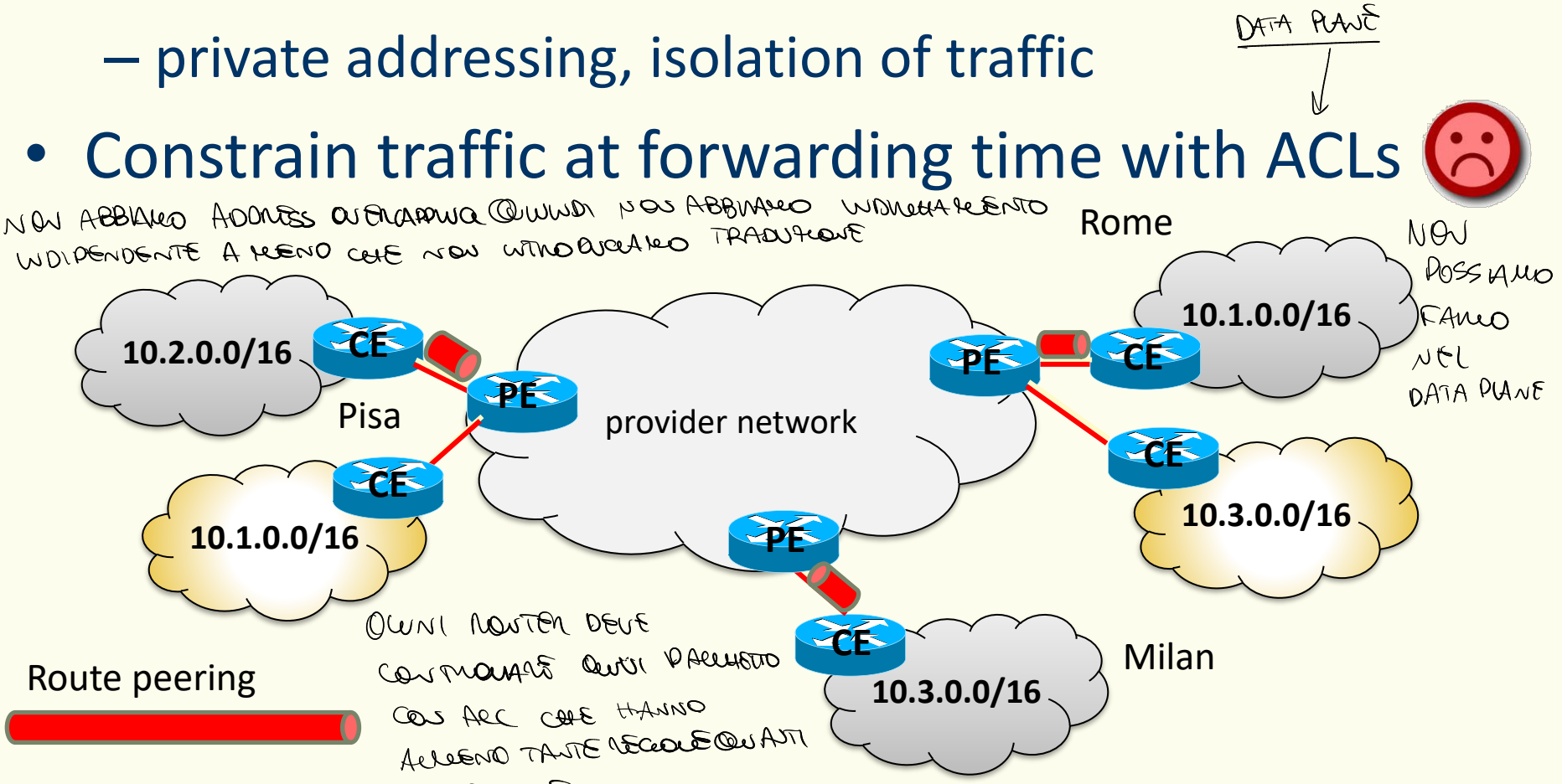
CE-PE peering approach

- **PE-based VPN**
  - scales with the number of customers
- Simple routing config at CEs



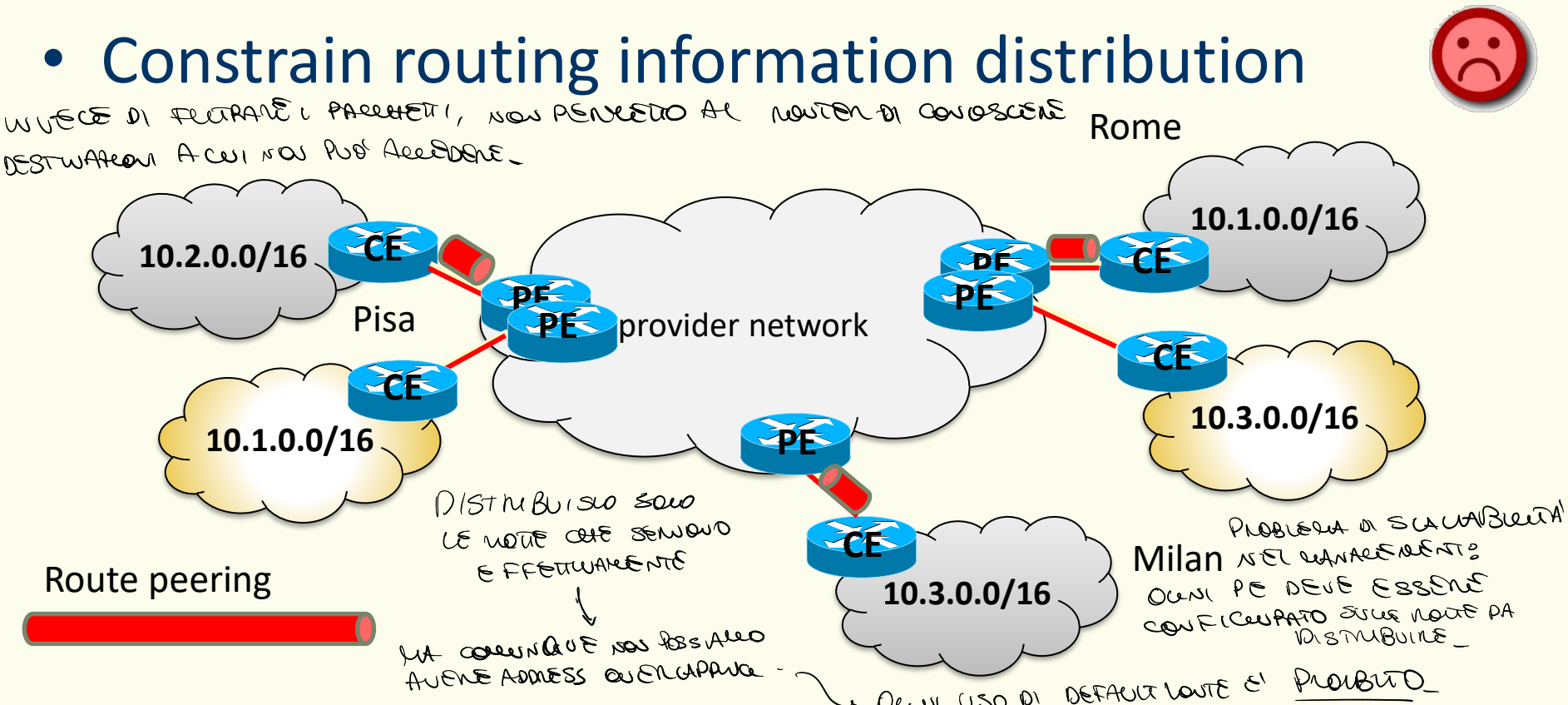
CE-PE peering approach

- How to achieve VPN goals?
  - private addressing, isolation of traffic
- Constrain traffic at forwarding time with ACLs



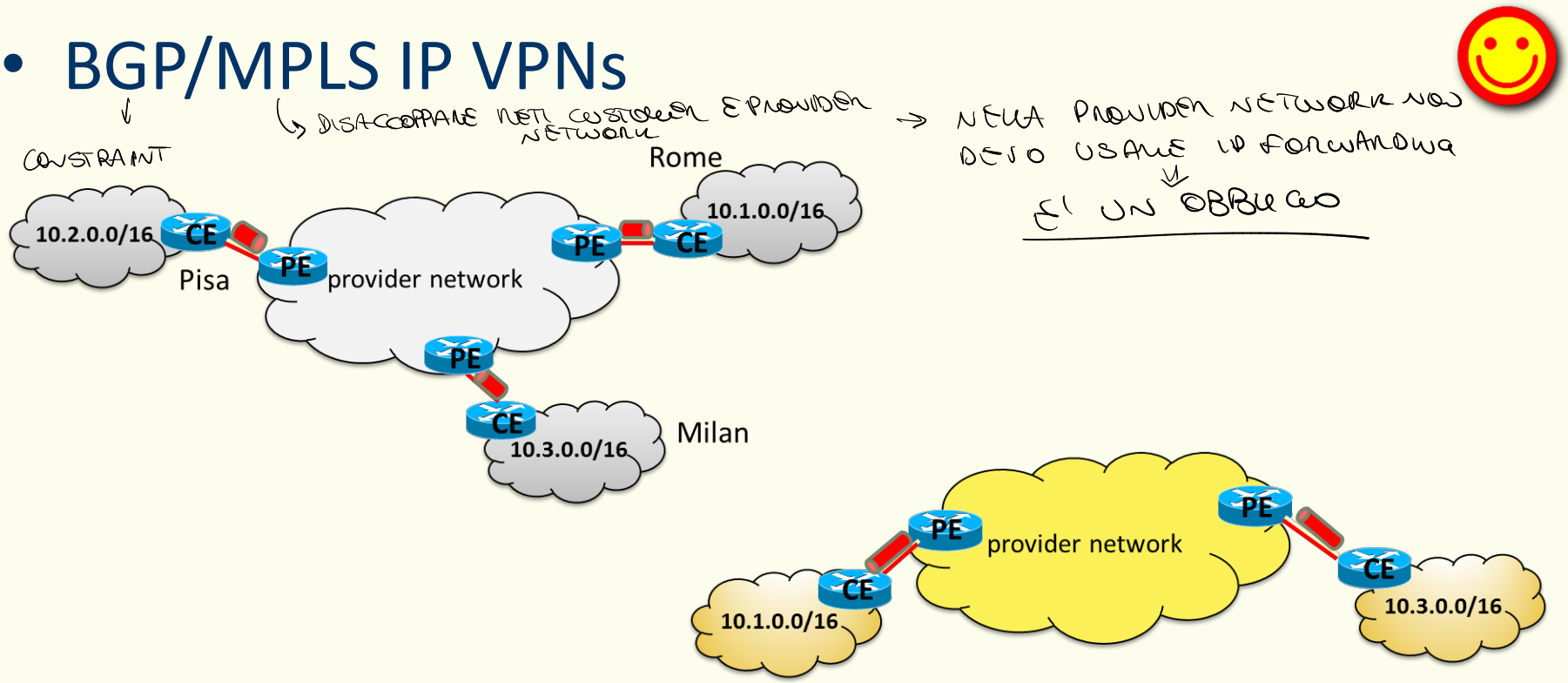
CE-PE peering approach

- How to achieve VPN goals?
  - private addressing, isolation of traffic
- Constrain routing information distribution



CE-PE peering approach

- How to achieve VPN goals?
  - private addressing, isolation of traffic
- BGP/MPLS IP VPNs

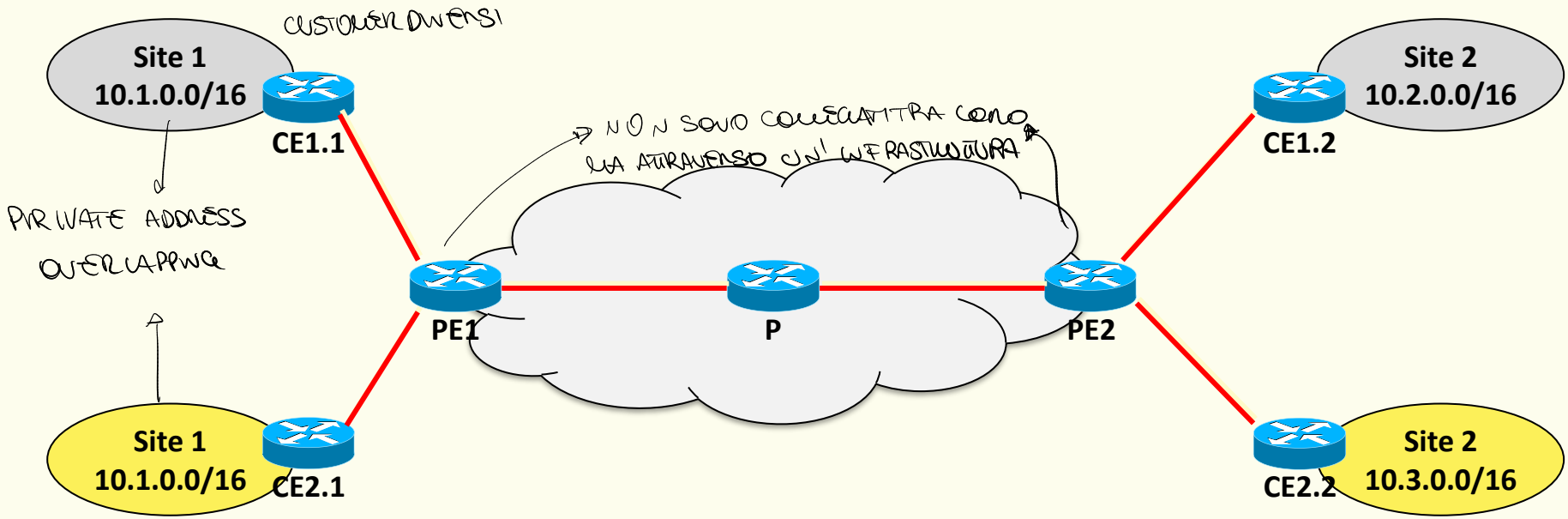


BGP/MPLS IP VPNs

- Originally developed as a Cisco solution for provider-provisioned VPNs
- Following its success, standardized afterwards as RFC 4364
- Also known as **L3VPNs** ~ CI SARANNO ANCHE L2 VPN

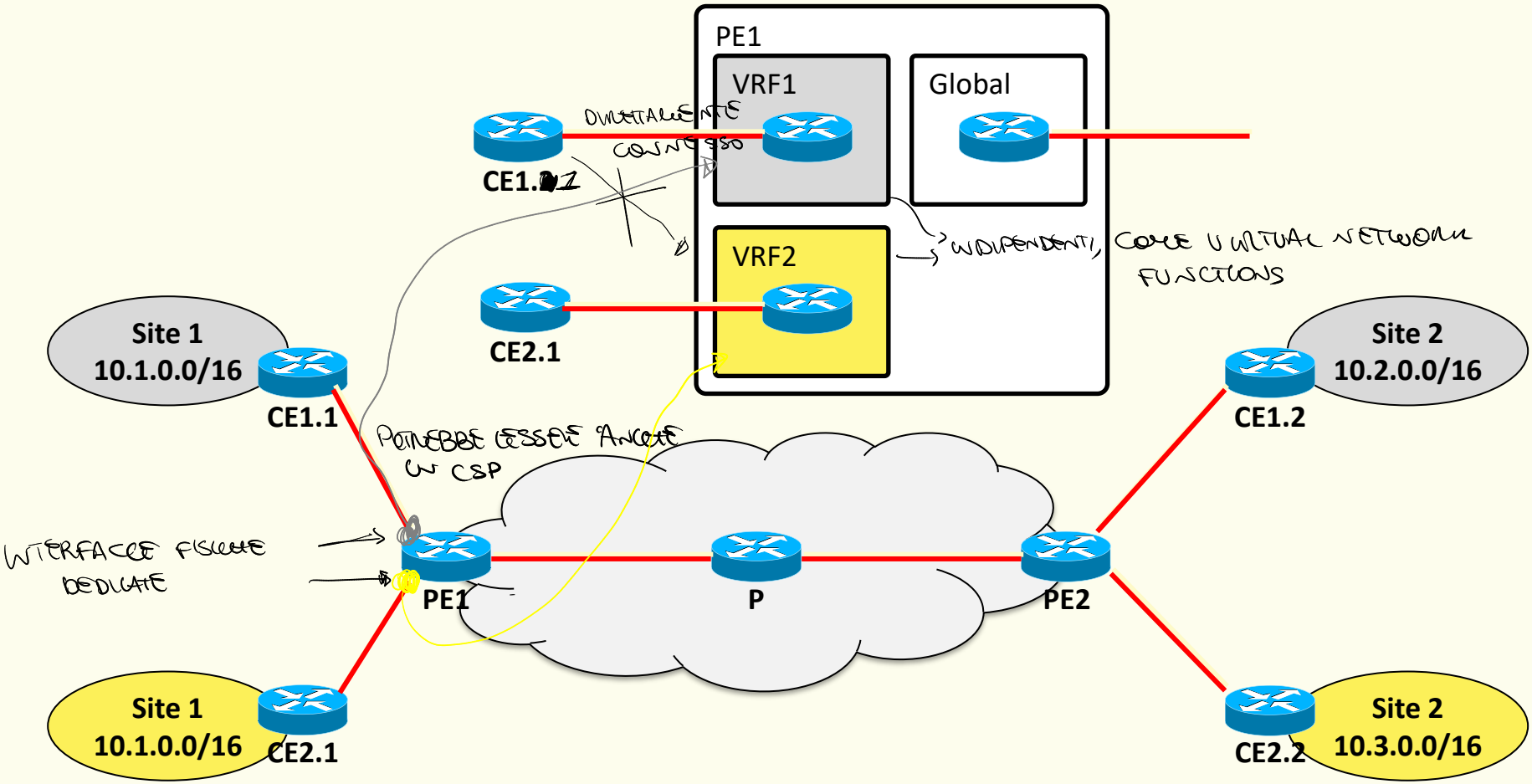
Example network

- Customer sites
  - Multiple sites may be attached to the same PE
  - One CE may be attached to multiple PEs
  - Multiple networks within each site



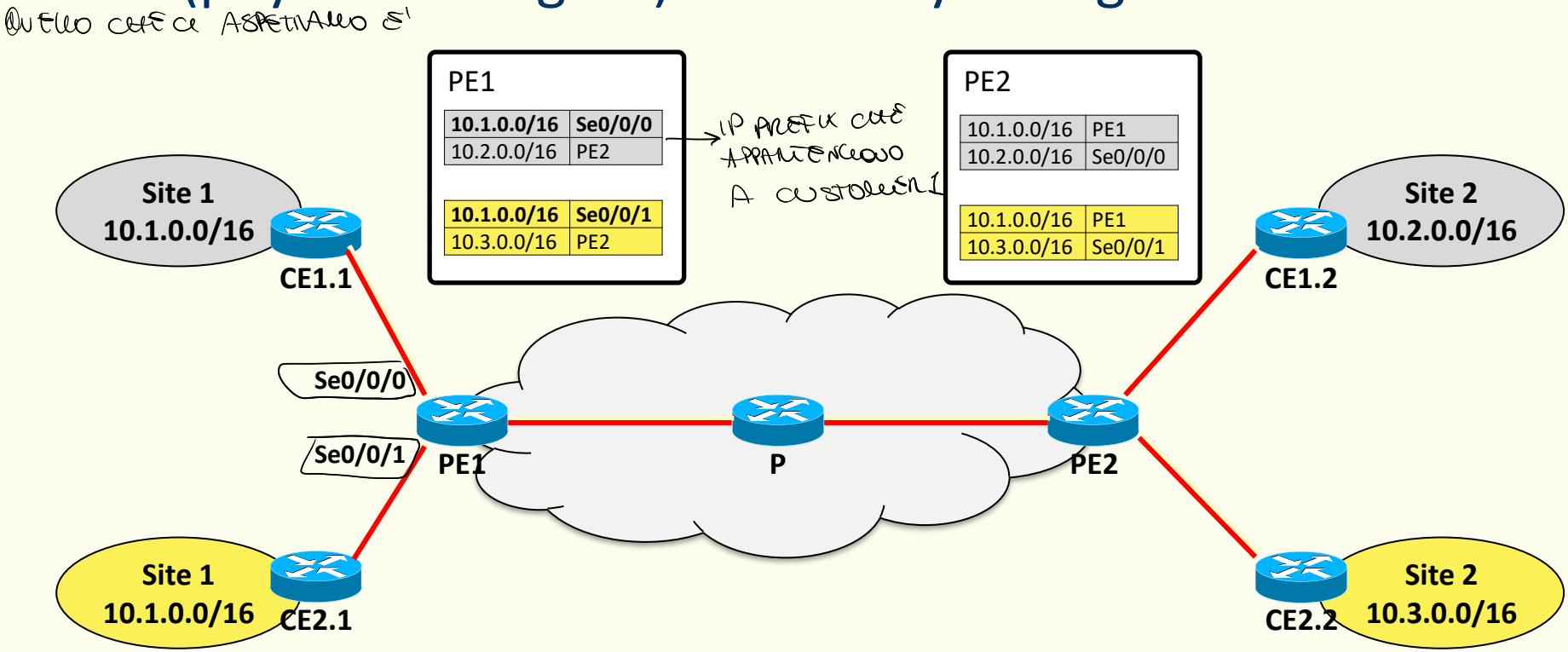
Isolation of traffic

- Per-VPN routing and forwarding tables (VRF)



Isolation of traffic

- Per-VPN routing and forwarding tables (VRF)
  - VRF look-up based on associating interfaces to CE (physical or logical) to VRFs by configuration

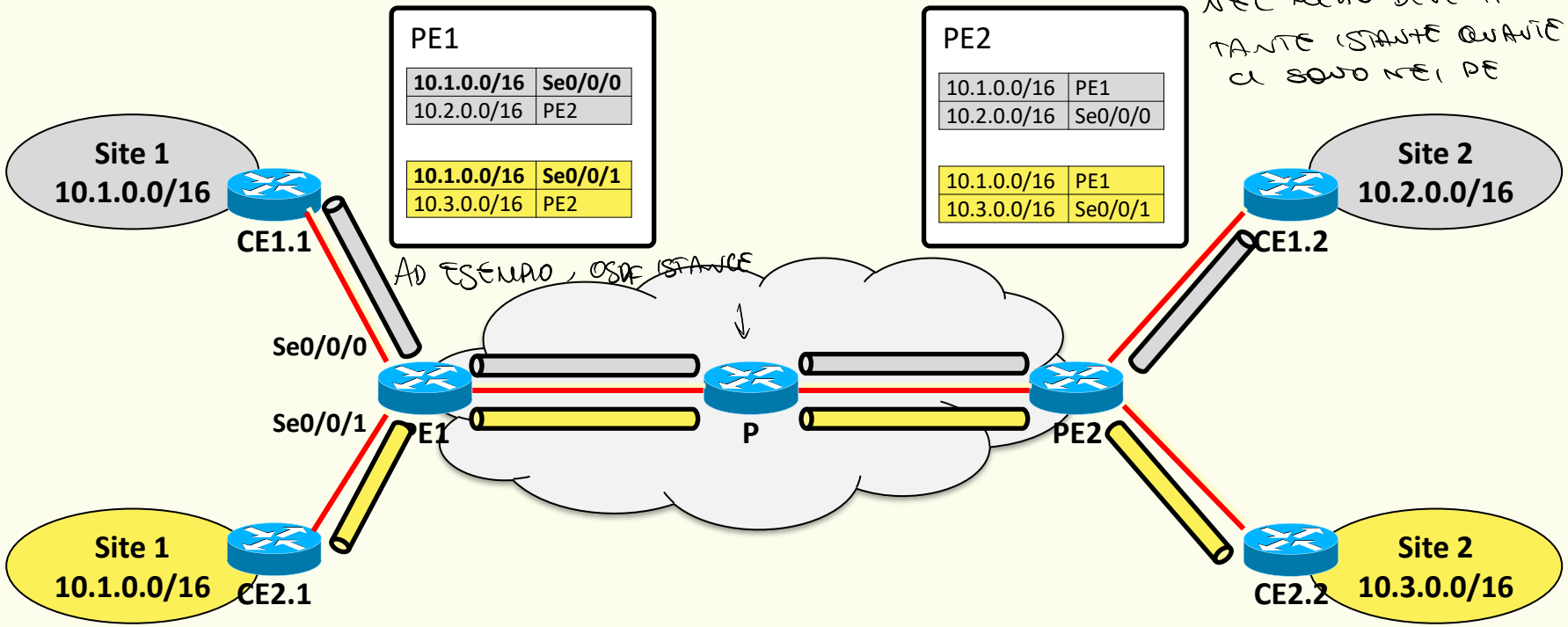


Constrained route distribution

- Run one routing protocol instance per VPN

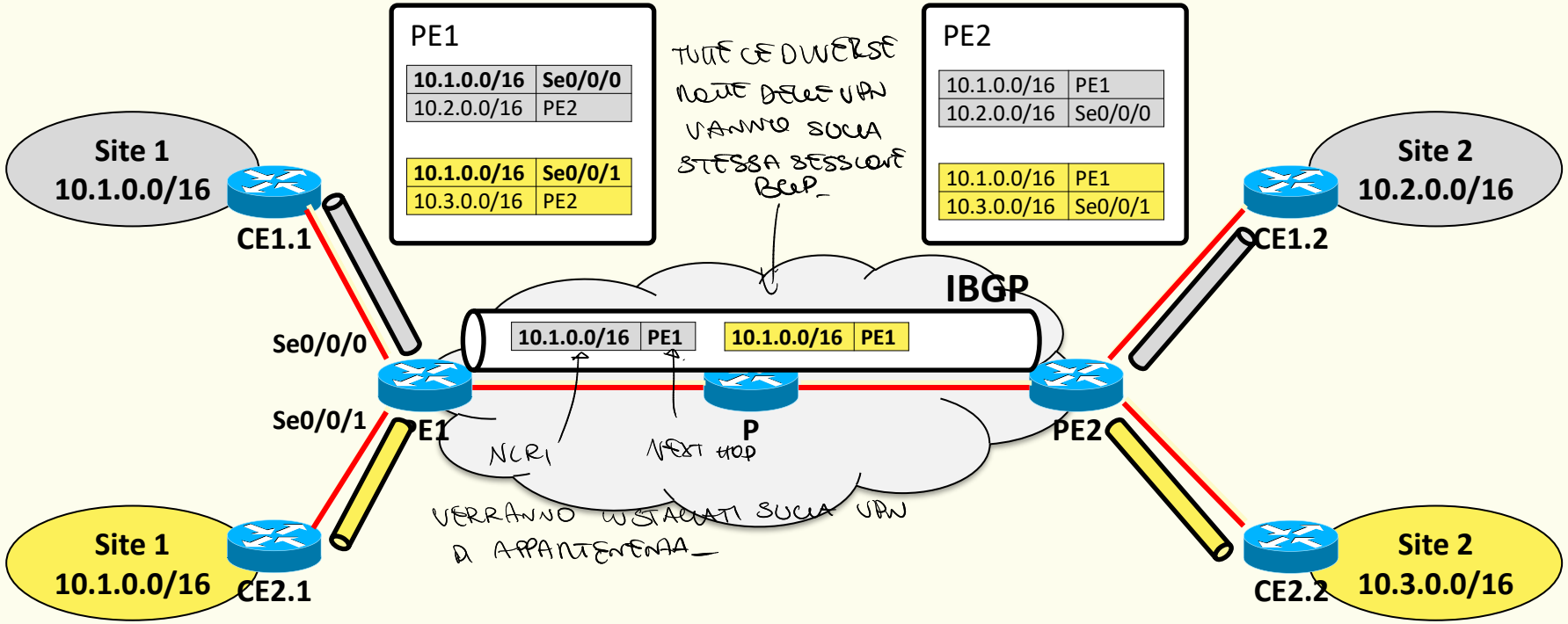
COME FACCIO A DECIDERE QUALE VRF USARE?

PIÙ ISTANZE VRF PIÙ ISTANZE DEL PROTOCOLLO DI ROUTING → ① SOLUZIONE PER CUI IL PE DEVE CONFIGURARLE OGNI CUSTOM.
② PE1 NON PUÒ ESSERE NEIGHBOR DI PE2 SE NON SONO DIRETTAMENTE COLLEGATI E OGNI ROUTER CHE SIA NEL MEZZO DEVE AVERE TANTE ISTANZE QUANTE CI SONO NEI PE



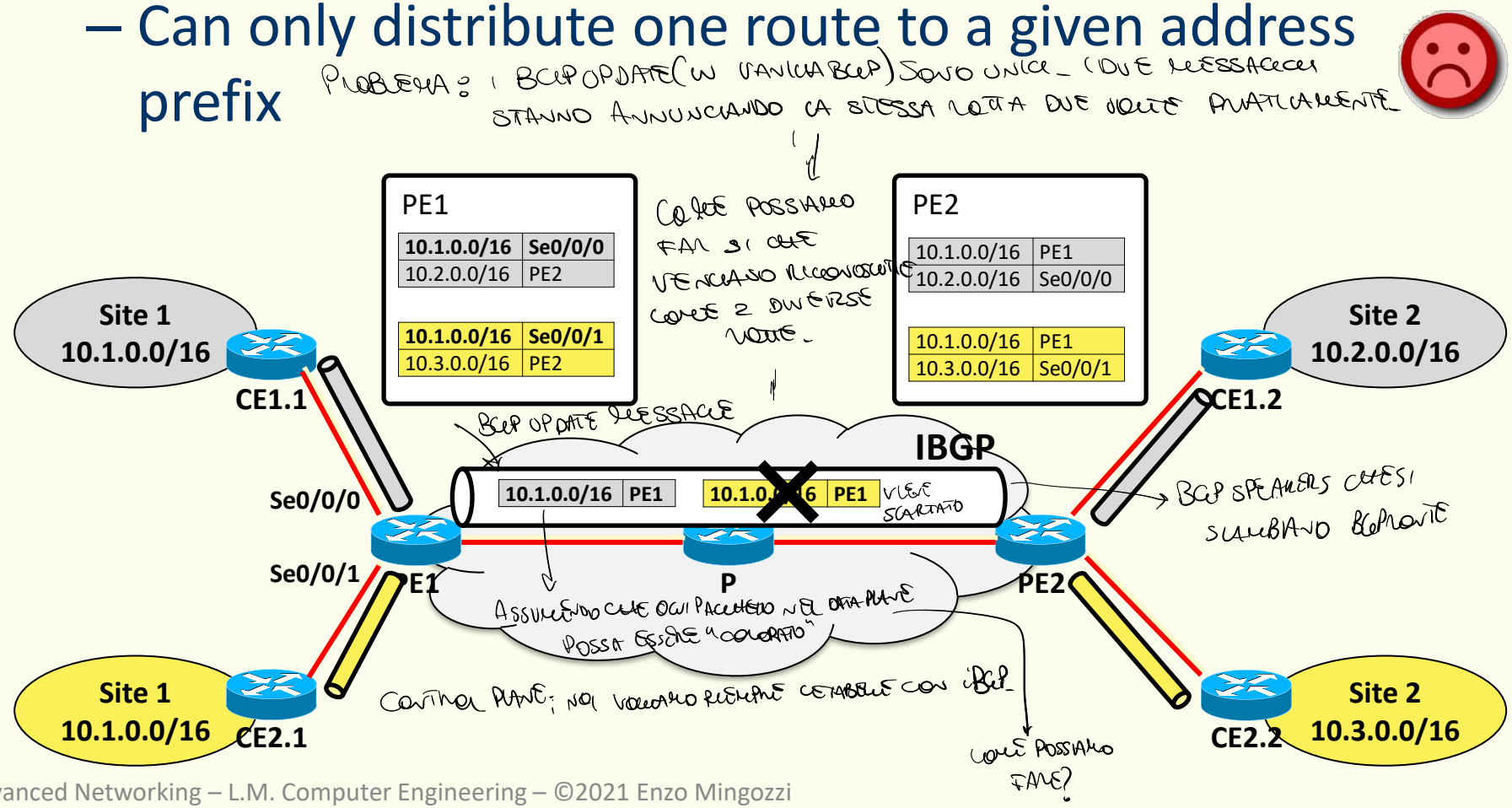
Route distribution

- Use iBGP to carry all routes
  - Supports route filtering
  - Supports route distribution between remote routers



Route distribution

- Use iBGP to carry all routes
  - Can only distribute one route to a given address prefix



Multiprotocol extensions for BGP

- BGP-4, originally supporting IPv4 only, has been **extended** to carry routing information for **multiple Network Layer protocols** (e.g. IPv6) [RFC 4760], referred as **MP-BGP**
- New attributes: **Multiprotocol Reachable NLRI**, and **Multiprotocol Unreachable NLRI**
- Network Layer protocol identified by the pair
  - **Address Family Identifier (AFI)**: e.g. 1 (IPv4), 2 (IPv6)
  - **Subsequent AFI**: e.g. 1 (unicast), 2 (multicast)

VPN-IP addresses

- Define a new address family **VPN-IPv4**
  - AFI=1 (*IPv4*), SAFI=128 (*MPLS-labeled VPN address*)
- VPN-IP addresses are obtained from customer site addresses by pre-pending an 8-byte identifier named **Route Distinguisher (RD)**
- RDs must be unique **globally**
  - E.g.,

TYPE (2)	AS number (2)	Locally assigned number (4)

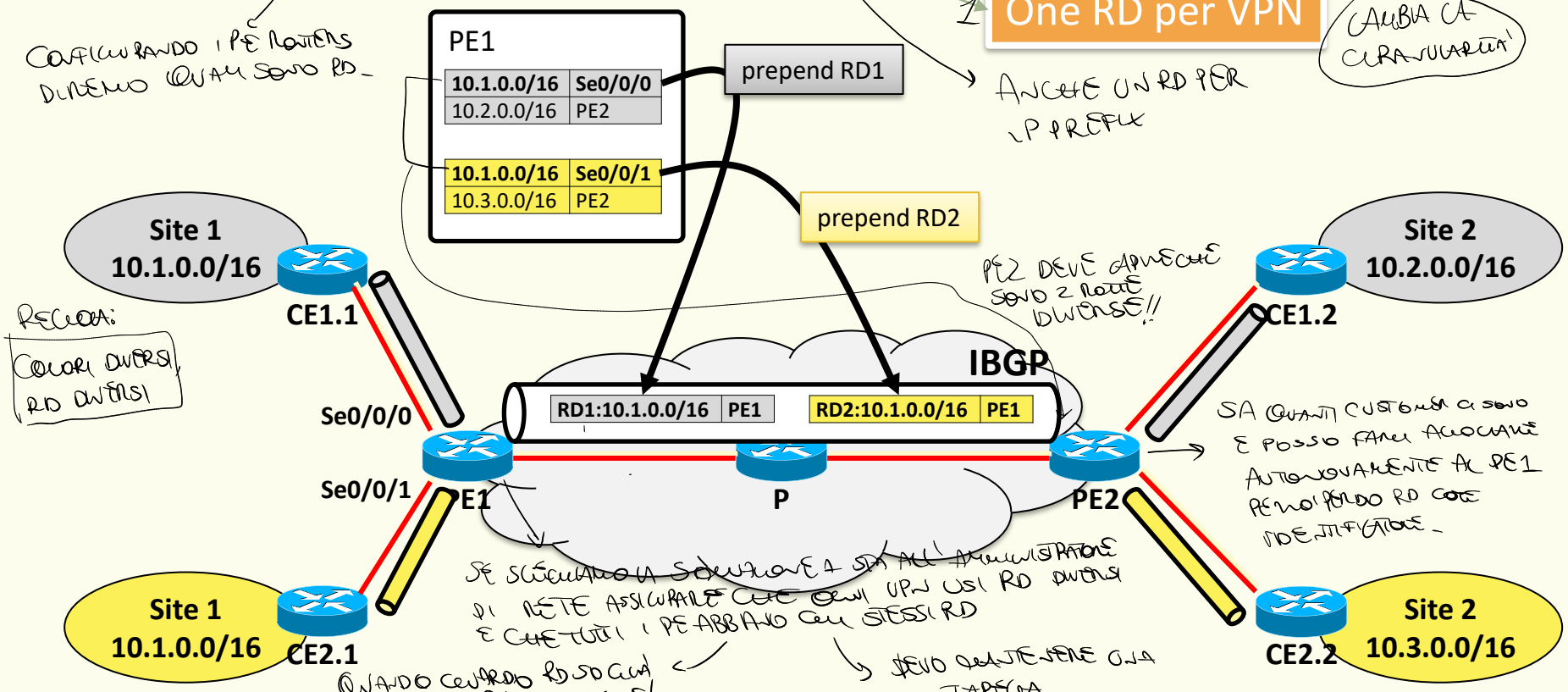
VPN-IP addresses

- RD – route association
  - By configuration only!!!

One RD per VPN per route

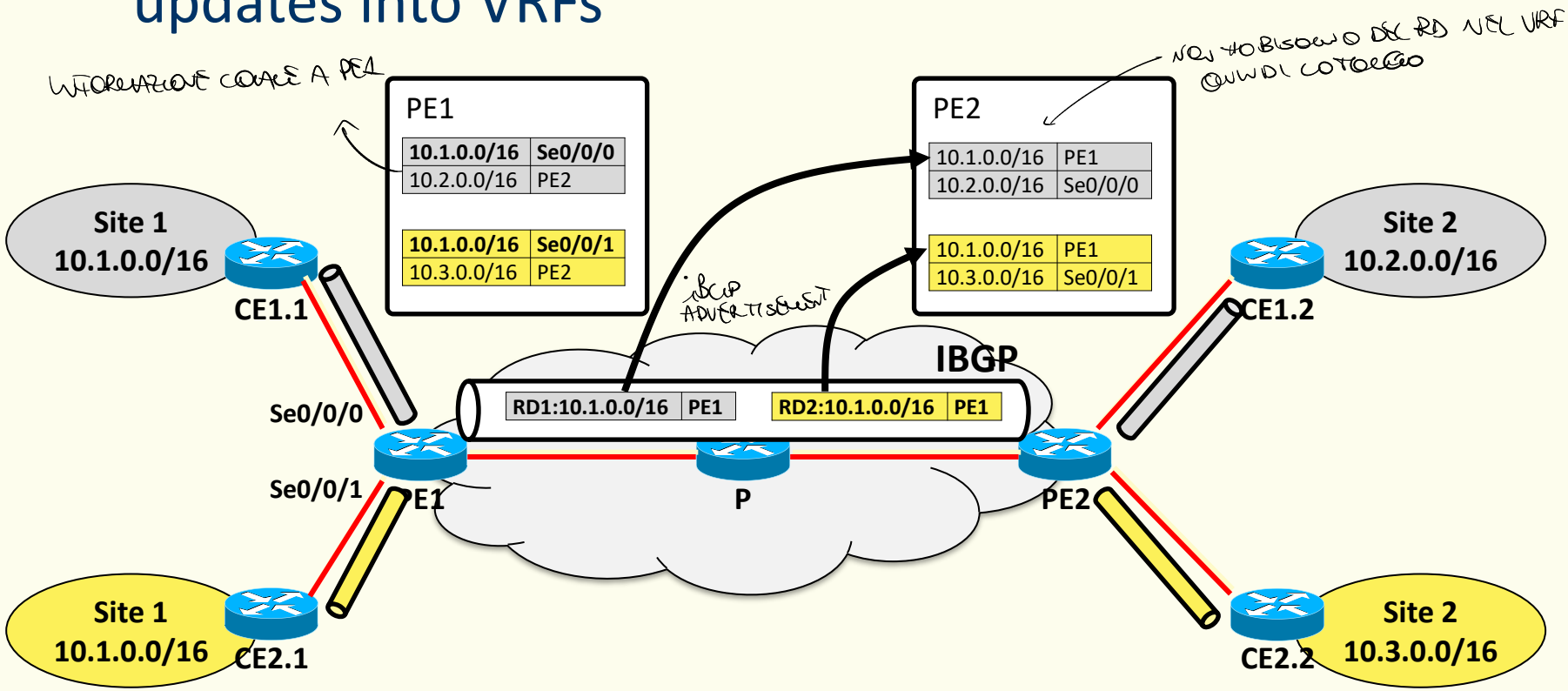
One RD per VPN per PE

One RD per VPN



Route distribution

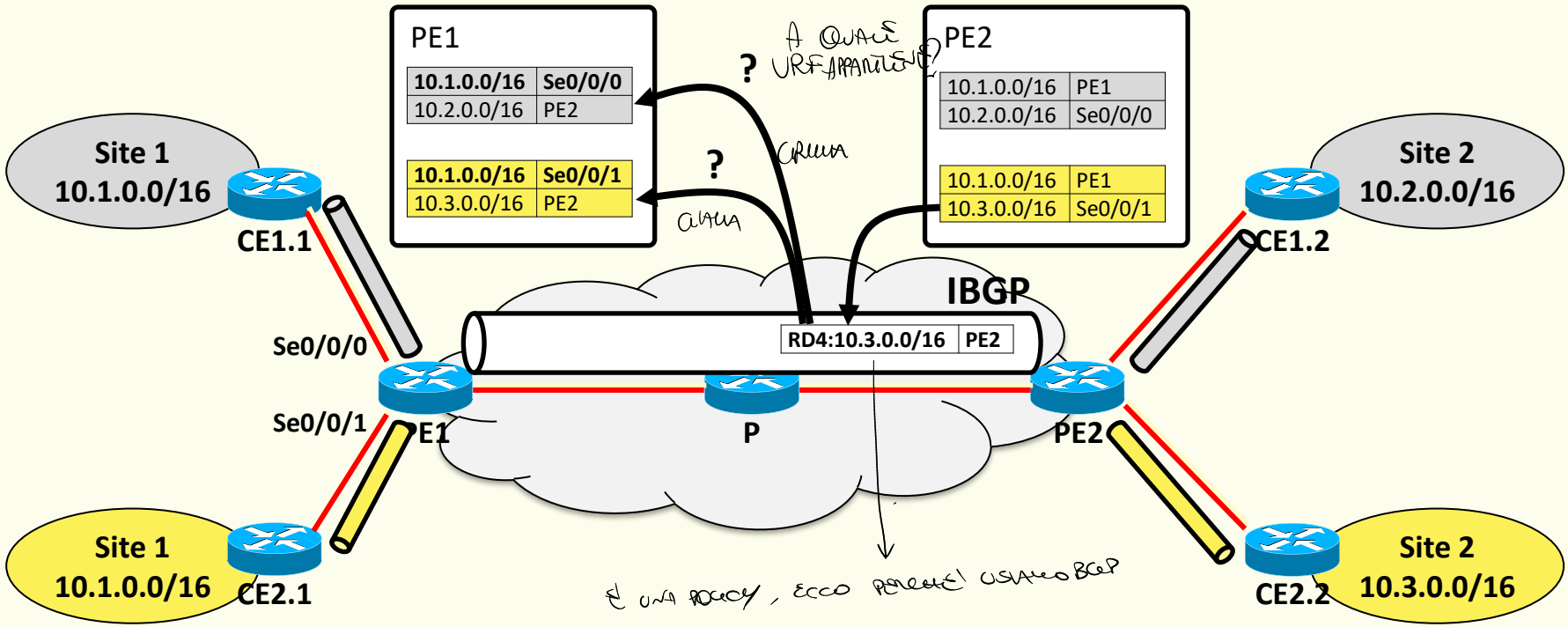
- Use iBGP to carry VPN-IP routes
  - RDs are stripped off when **redistributing** BGP updates into VRFs



Route distribution

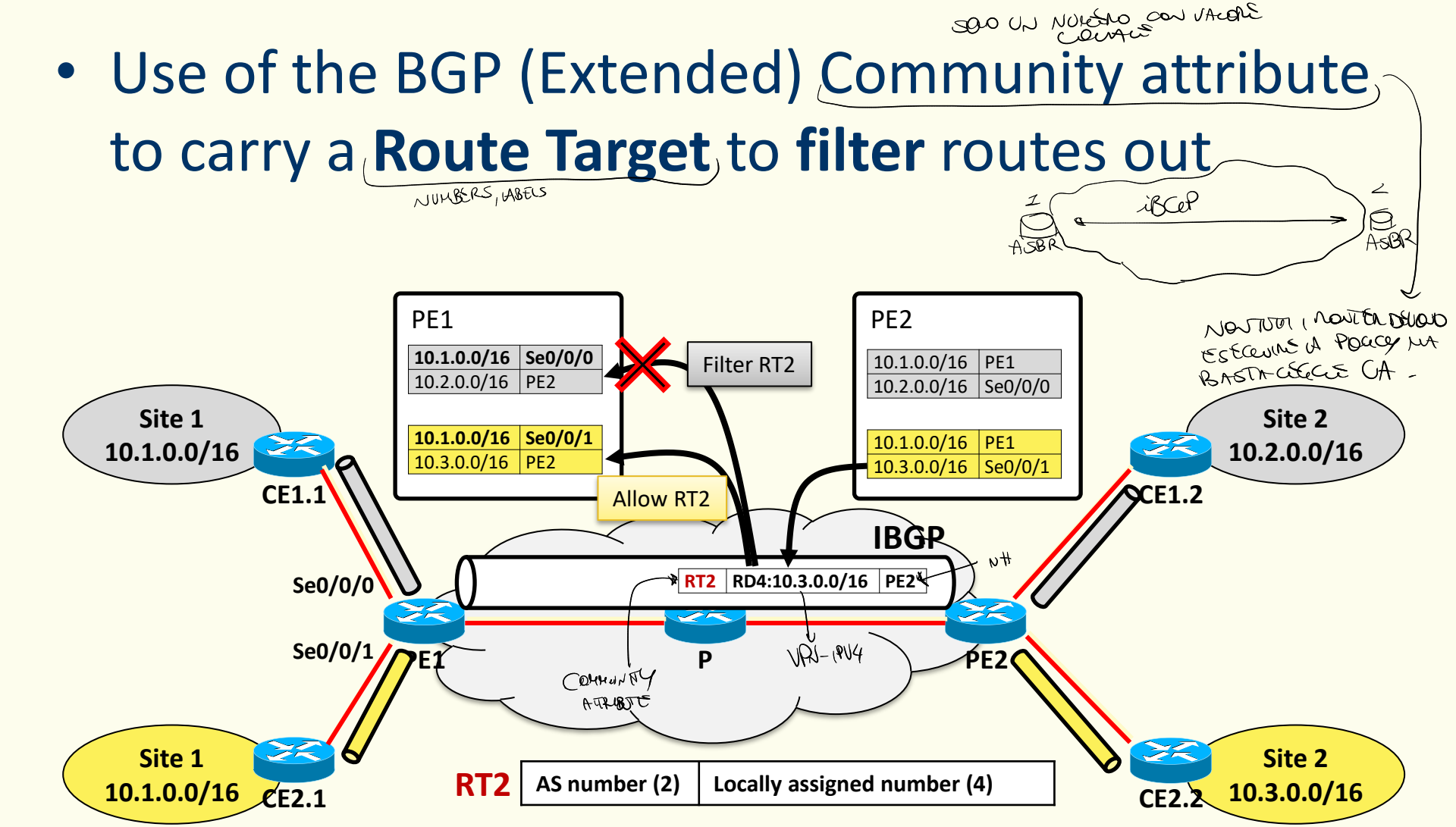
- The **only purpose** of RDs is to make the VPN routes unique

The target VRF **is not inferrable** in any manner from the RD



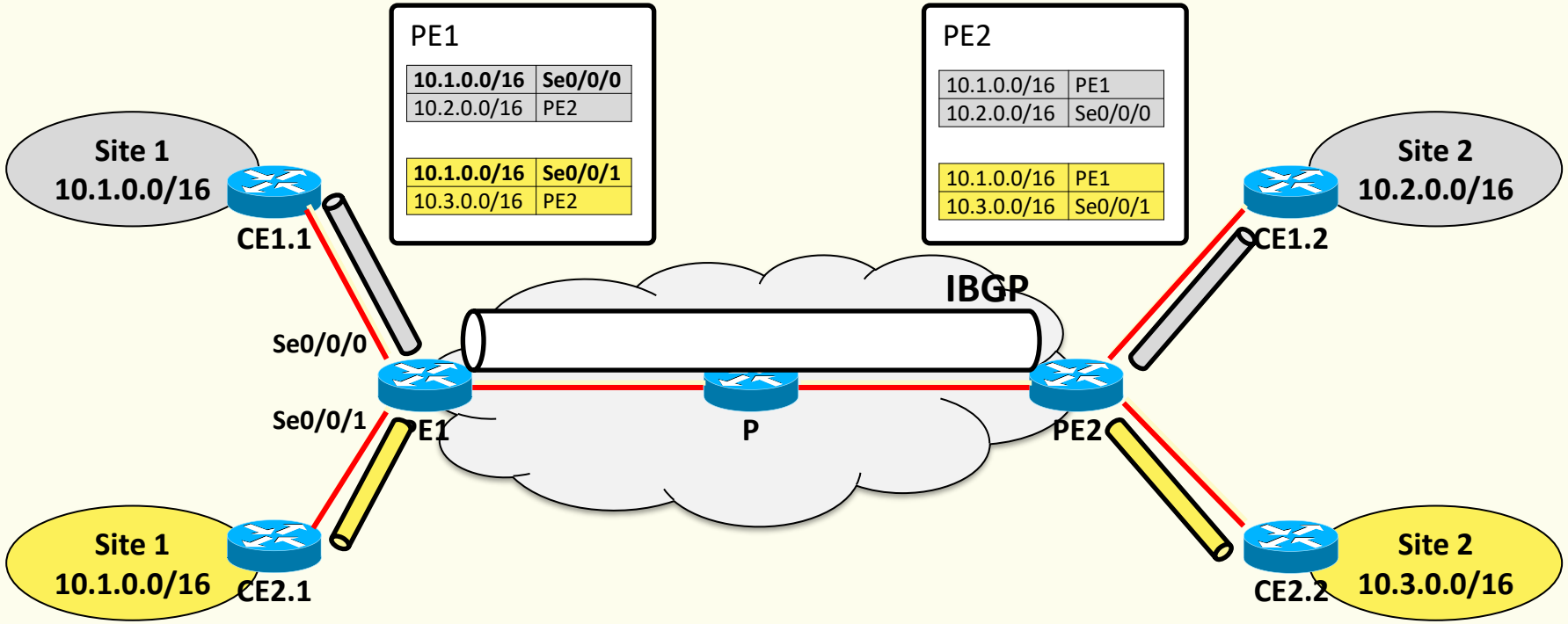
Constrained route distribution

- Use of the BGP (Extended) Community attribute to carry a **Route Target** to **filter** routes out



Constrained route distribution

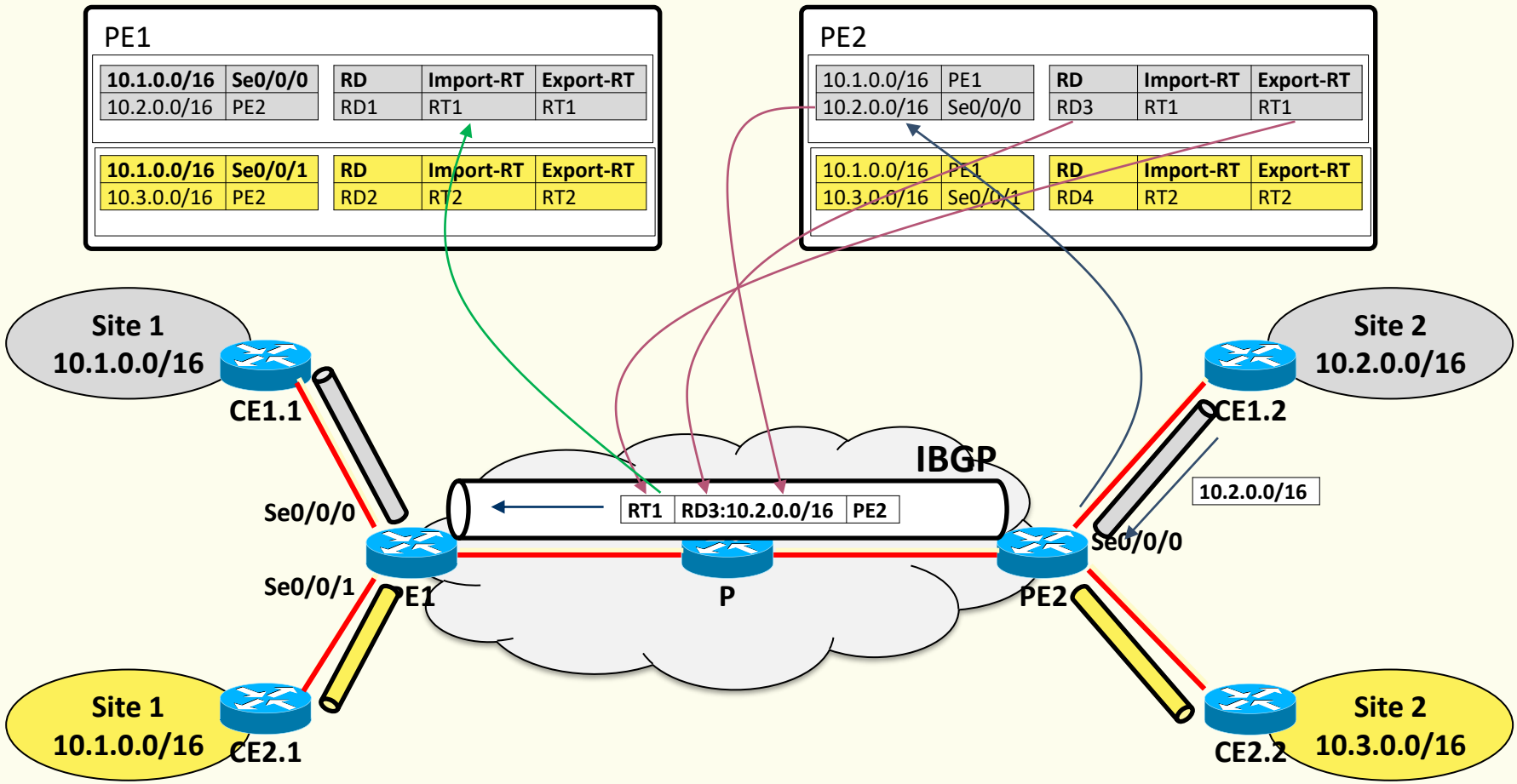
- Broader requirements than simple VPN isolation
  - Support for **overlapping** VPNs (one site belongs to multiple VPNs)
  - Arbitrary and complex connectivity models



Constrained route distribution

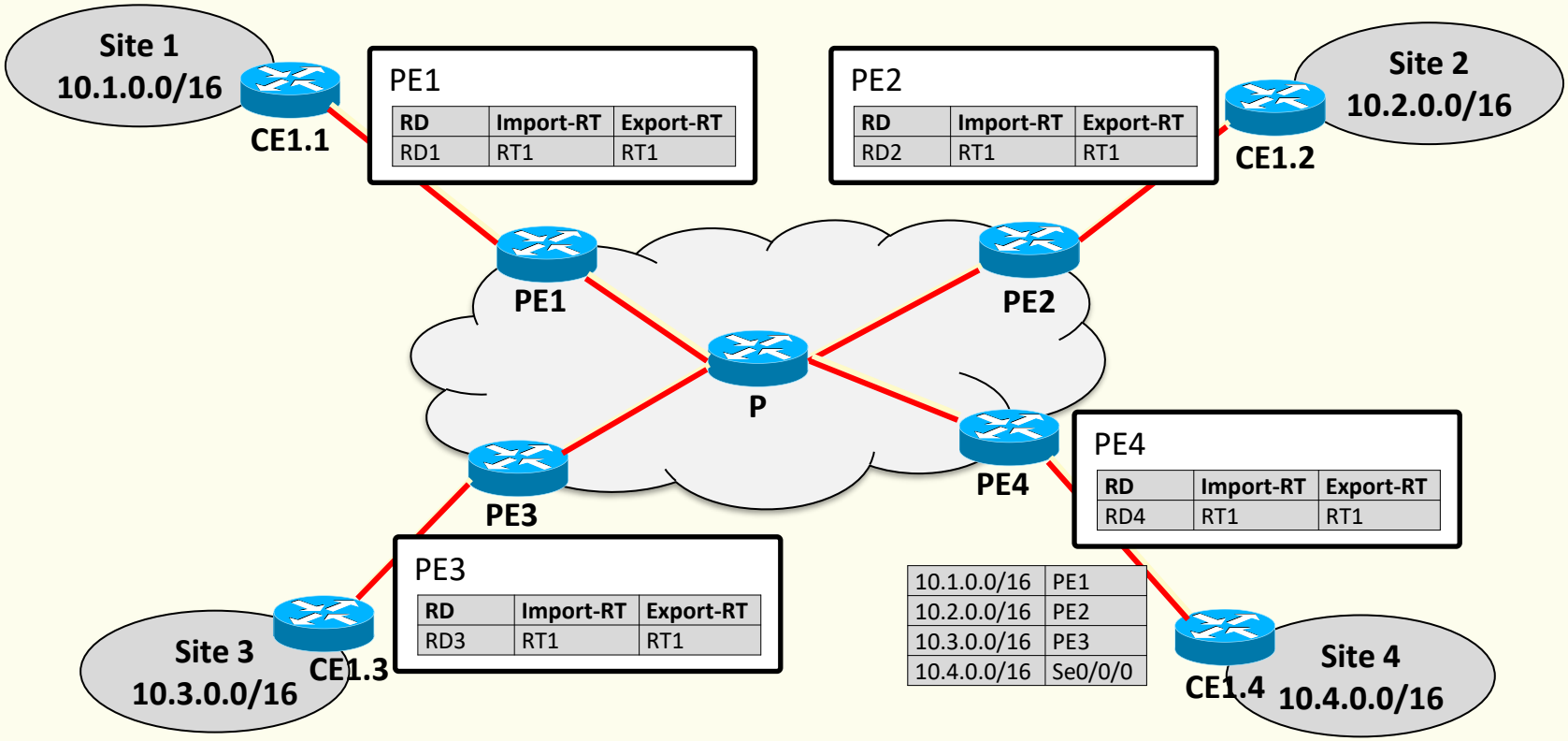
- RT **import** and **export** policies on a per-VRF basis

ONE RD PER VPN PER PE



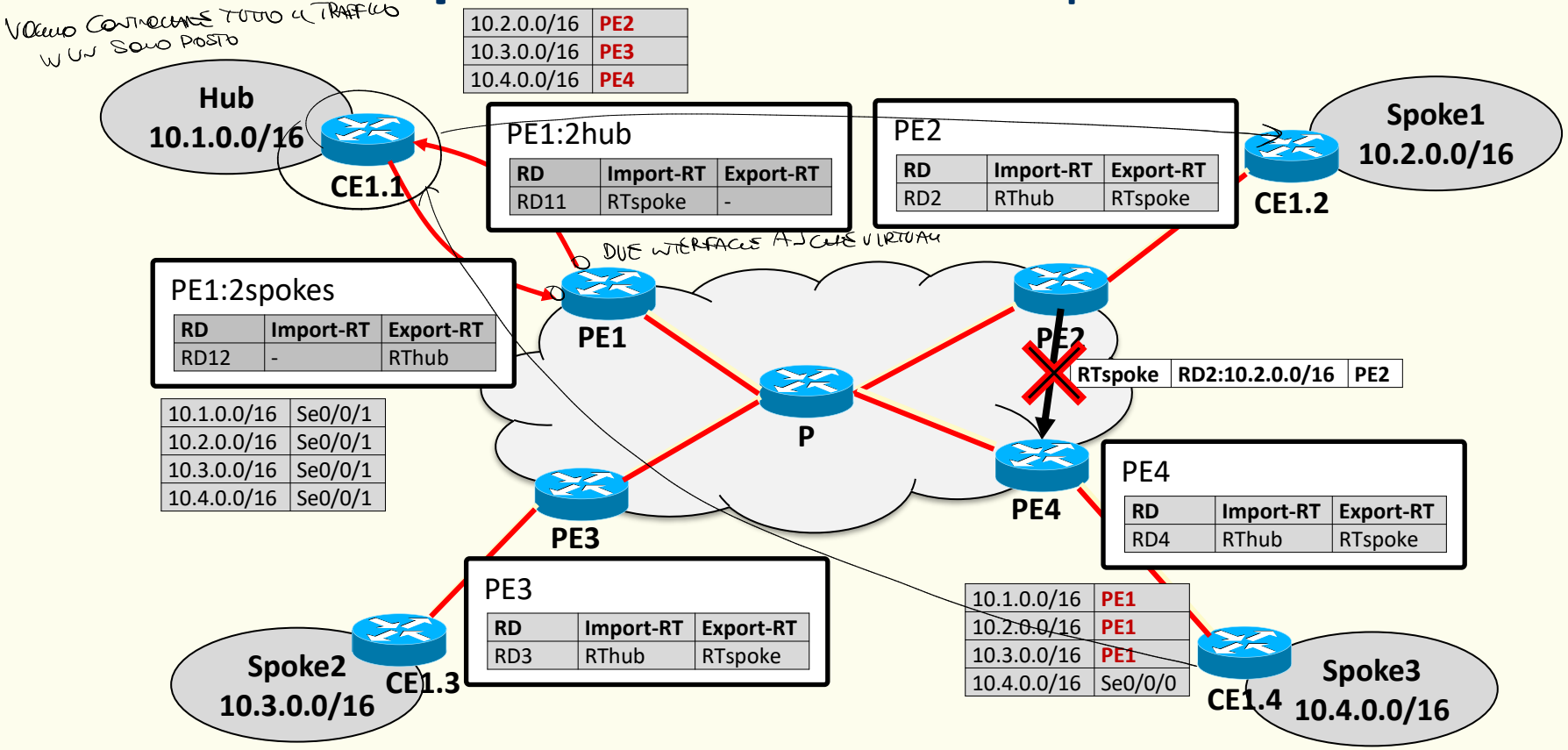
Constrained route distribution

- **Full-mesh**: single RT at all sites (in & out)



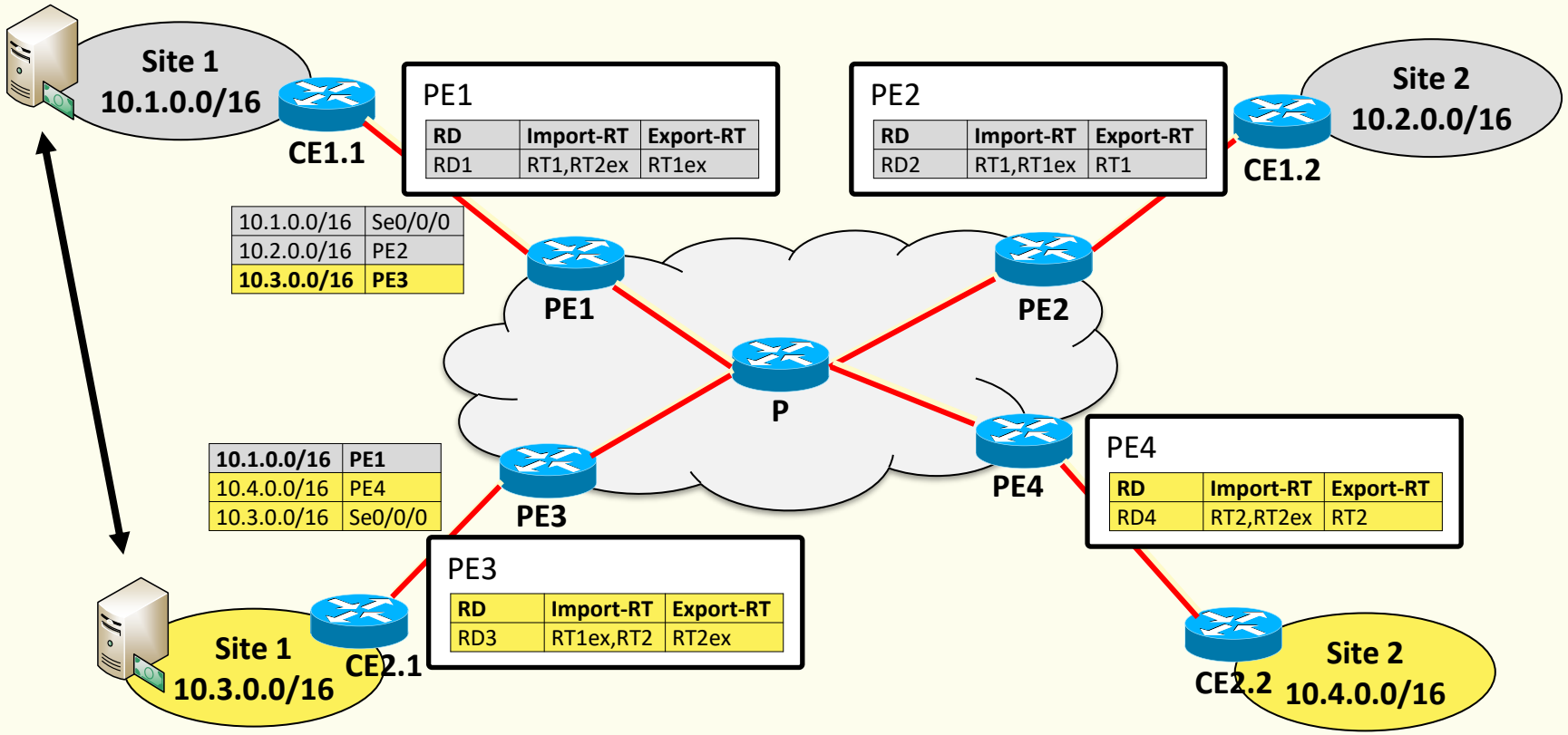
Constrained route distribution

- **Hub-and-spoke**: RThub and RTspoke



Constrained route distribution

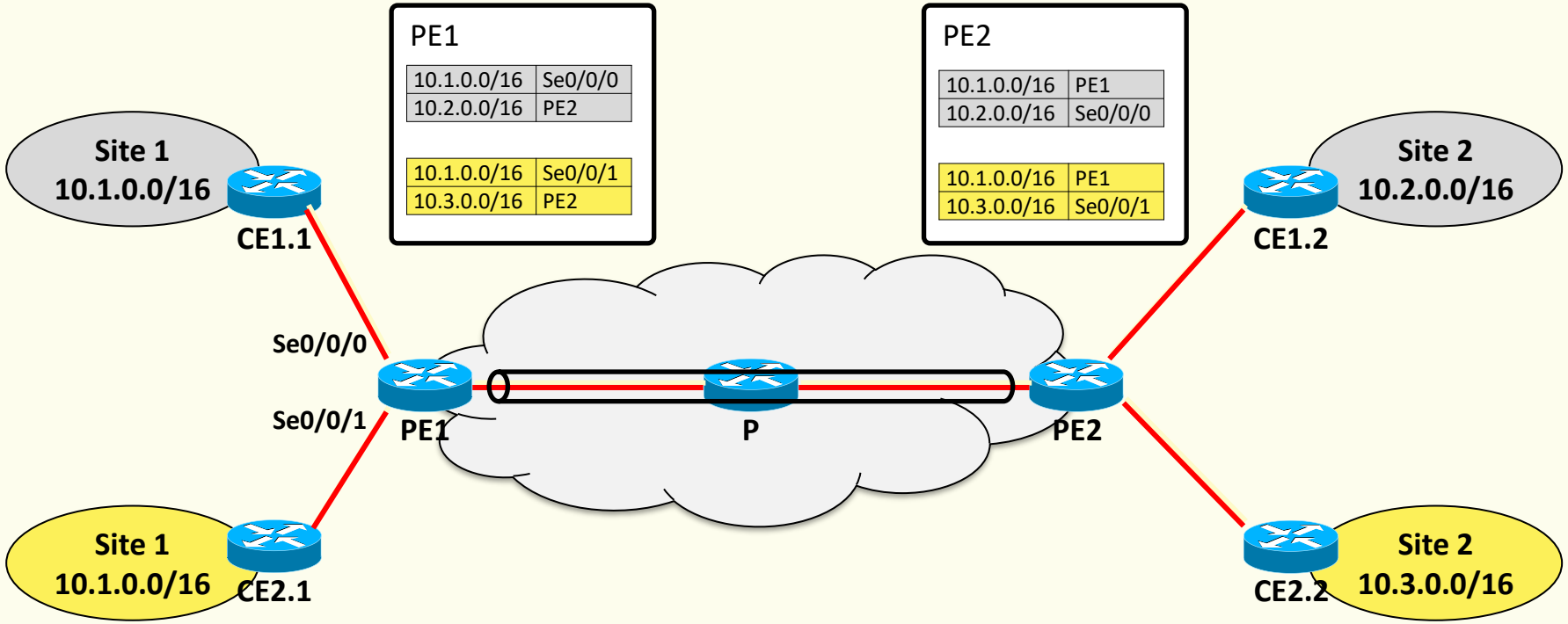
- **Overlapping VPNs** (extranets)



Provider network forwarding

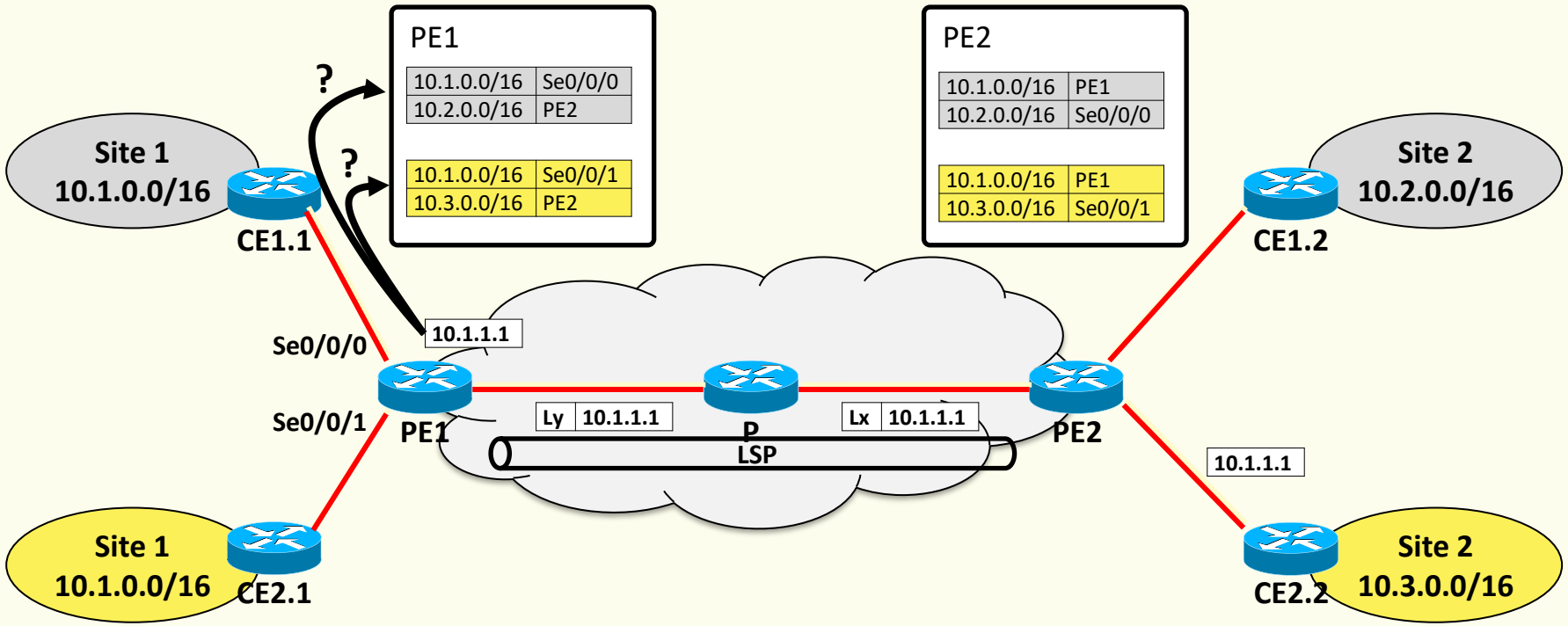
- The advertising PE is the next hop of a route
  - P has no information on the routes
  - VPN-IP addresses are not routable

Tunneling between PE is necessary



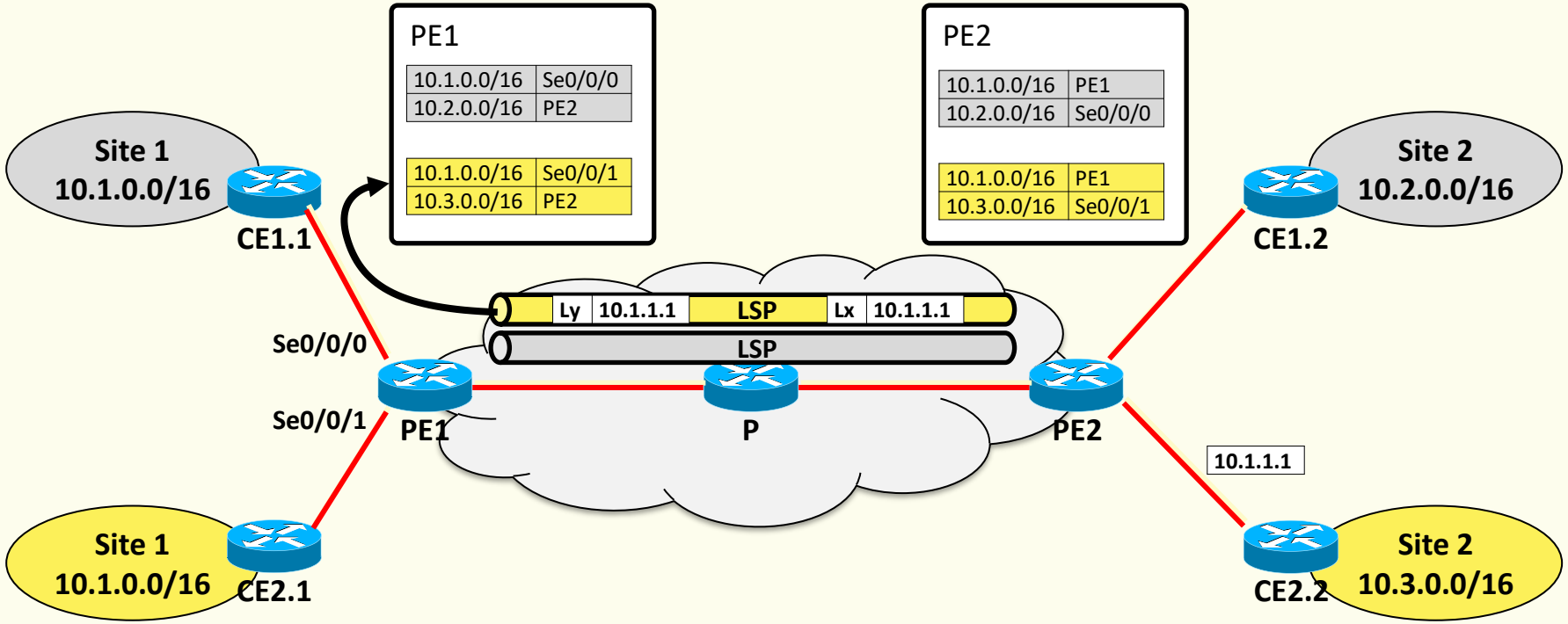
Provider network forwarding

- How traffic from a remote PE is demultiplexed?
  - One LSP per VPN is needed between PEs!



Provider network forwarding

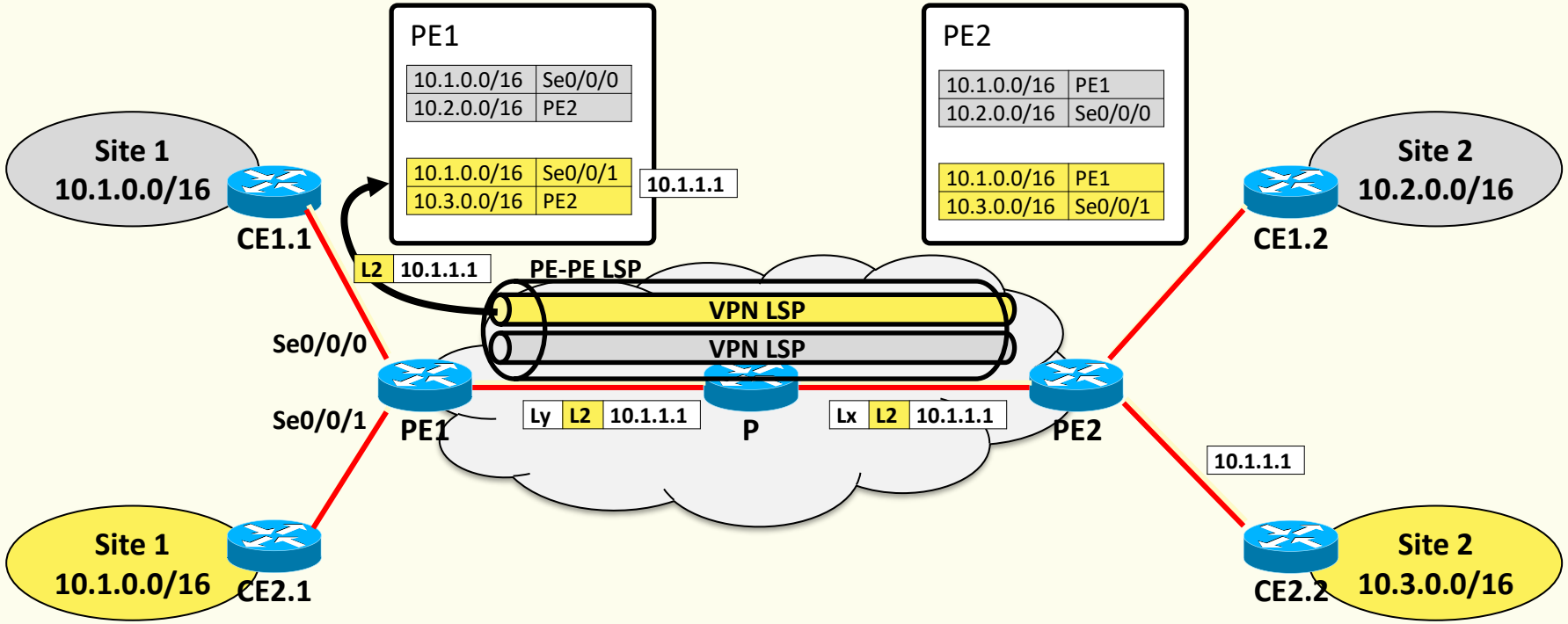
- No separate state at P for each PE-PE VPN LSP
- VPN label distribution must be automatic



Provider network forwarding

- No separate state at P for each PE-PE VPN LSP

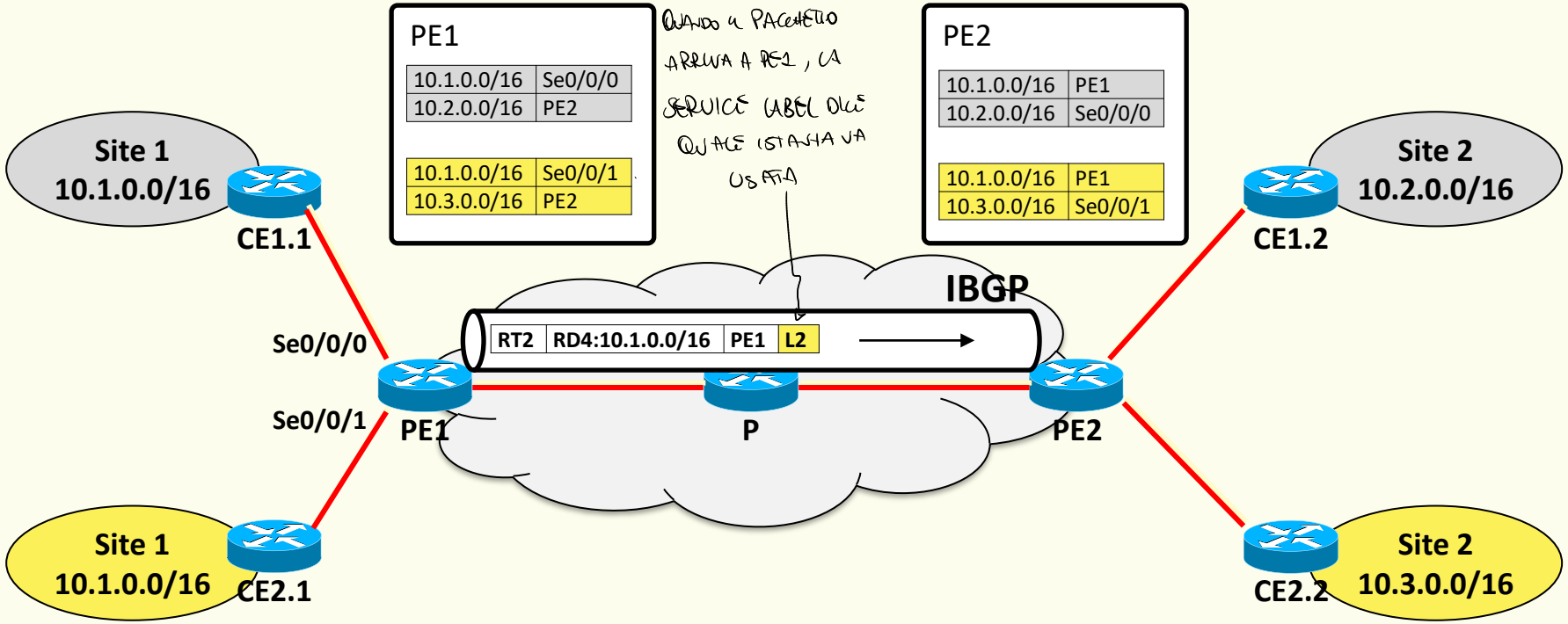
Use MPLS label stacking



Provider network forwarding

- VPN label distribution must be automatic

Use MP-iBGP for label distribution



Benefits of BGP/MPLS IP VPNs

- **Customer** VPN-AS-A-SERVICE
  - Offload routing management to the provider
  - Access added-value services (firewall, auth)

  ACCESSO AD UNA RETE FORNITA DAL PROVIDER E LE VPN FUNZIONANO/ NON DEVO FARE ROUTER CONFIGURATION SU ROUTER EDGE
- **Provider**
  - Service multiple VPN customers with a common infrastructure → [EFFICIENTE PERCHÉ POSSO USARE INFRASTRUTTURA CONDIVISA]
  - VPN management is hidden to the core
  - Scale by adding PEs when needed
- MPLS tunneling plays a key **enabling** role

References

- I. Minei and J. Lucek, **MPLS-Enabled Applications: Emerging Developments and New Technologies**, 3rd Edition, Wiley, Dec. 2010
- RFCs
  - **RFC4364**, BGP MPLS IP Virtual Private Networks (VPNs), Feb. 2006
  - **RFC4760**, Multiprotocol Extensions for BGP-4, Jan. 2007