Peer-to-Peer VPN

Peer-to-Peer VPN

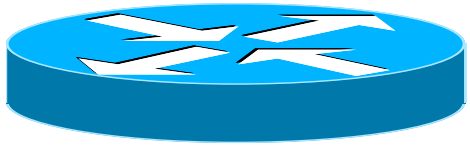
- **Scambio di informazioni di routing con i router dell'ISP, pertanto il routing avviene su un layer composto sia da entita che risiedono in azienda che da entità che risiedono nell'ISP**

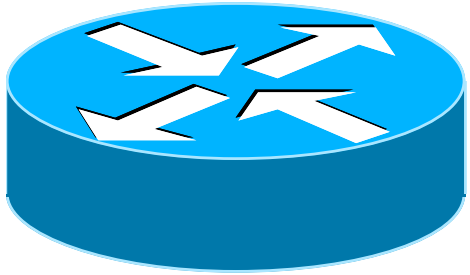
- **Sono di fatto basate sulla soluzione BGP/MPLS**
  - » **Il gateway aziendale trasferisce dati all'ISP e questo a sua volta si preoccupa del forwarding verso gli altri siti aziendali, pertanto il routing (topologia delle connessioni) è di fatto nelle mani dell'ISP**
  - » **Plug & Play, l'aggiunta di un sito richiede interventi di configurazione solo da parte dell'ISP e non dell'azienda**

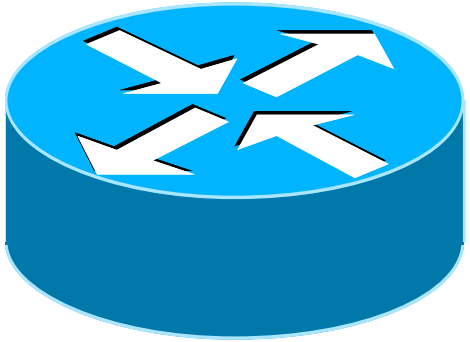
VPN BGP/MPLS

Peer-to-Peer VPN

Elementi di una VPN BGP/MPLS







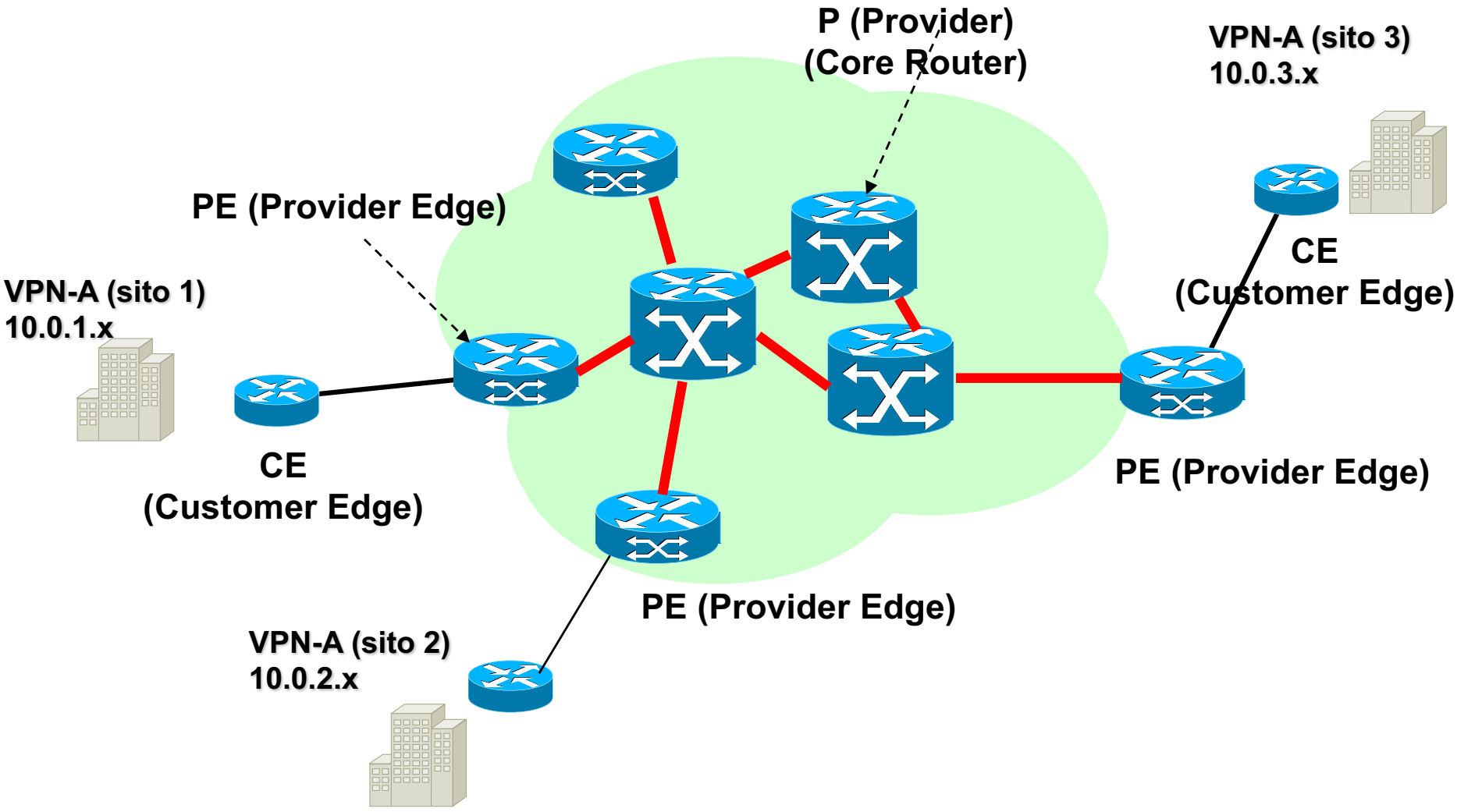
Customer Edge : è il router del sito aziendale che si interconnette con l'ISP fornitore del servizio VPN BGP/MPLS. Ha funzionalità di routing IP classiche. A livello di routing, il suo unico peer è il Provider edge con cui scabia info tramite BGP

Provider Edge : è il router d'accesso della rete dell'ISP dove sono attestati uno o più Customer edge. Oltre ad avere funzionalità IP svolge anche il ruolo di LER MPLS.

Provider Router : Label Switched Router (LSR) che compongono la backbone MPLS dell'ISP

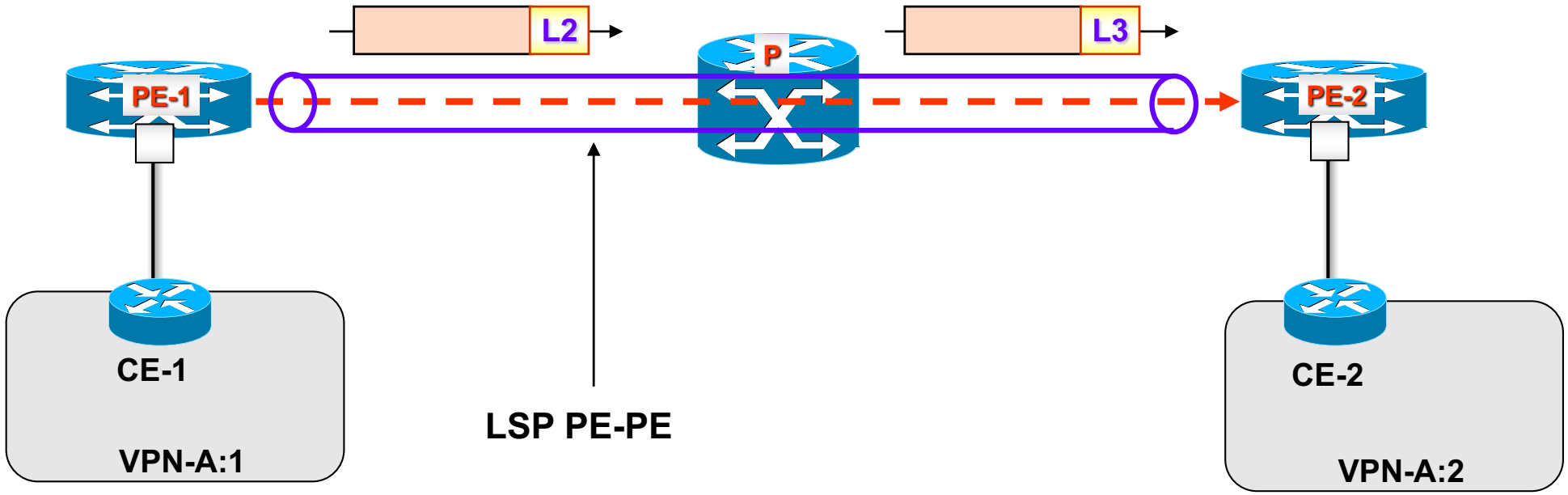
MPLS/VPN Backbone : rete MPLS con LSP opportunamente configurati per collegare fra loro tutti i PE

Architettura di servizio VPN MPLS



Meccanismo di inoltro dei pacchetti

- Problema: trasferire i pacchetti da due siti di una VPN: A:1-A:2
- Soluzione banale (A:1→A:2): incapsulare al PE (A:1) i pacchetti IP provenienti dal CE (A:1) nello LSP che connette PE(A:1)→PE(A:2)
- Alla fine dello LSP, il PE(A:2) instrada su base IP
- Che succede se gli stessi PE supportano più di una VPN con indirizzamenti non coordinati ? Può succedere che il PE(A:2) si trova a dover inoltrare a livello IP pacchetti di due VPN diverse ma che utilizzano gli stessi indirizzi di destinazione !

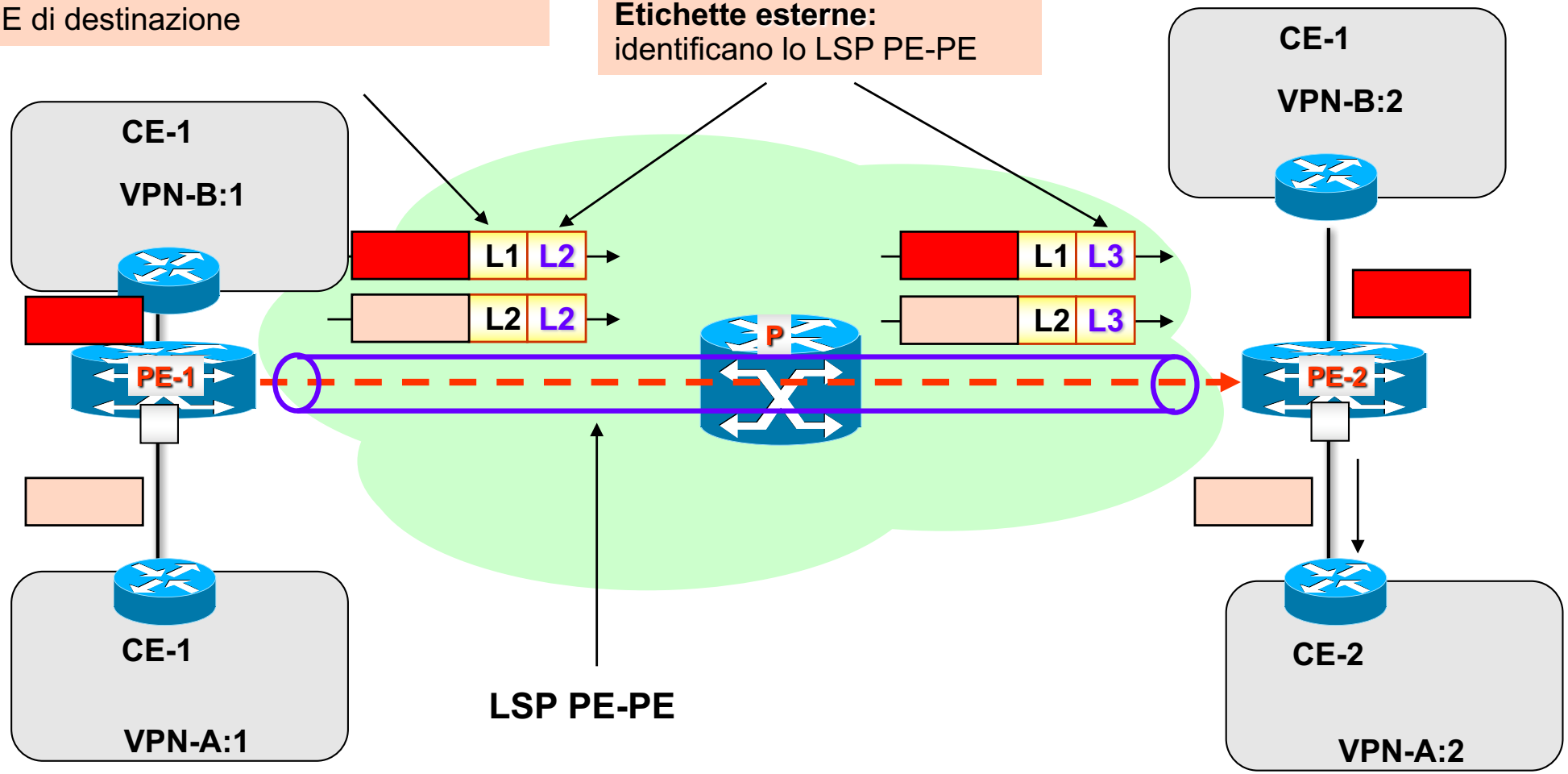


Meccanismo di inoltro dei pacchetti

Soluzione: label stacking con due etichette

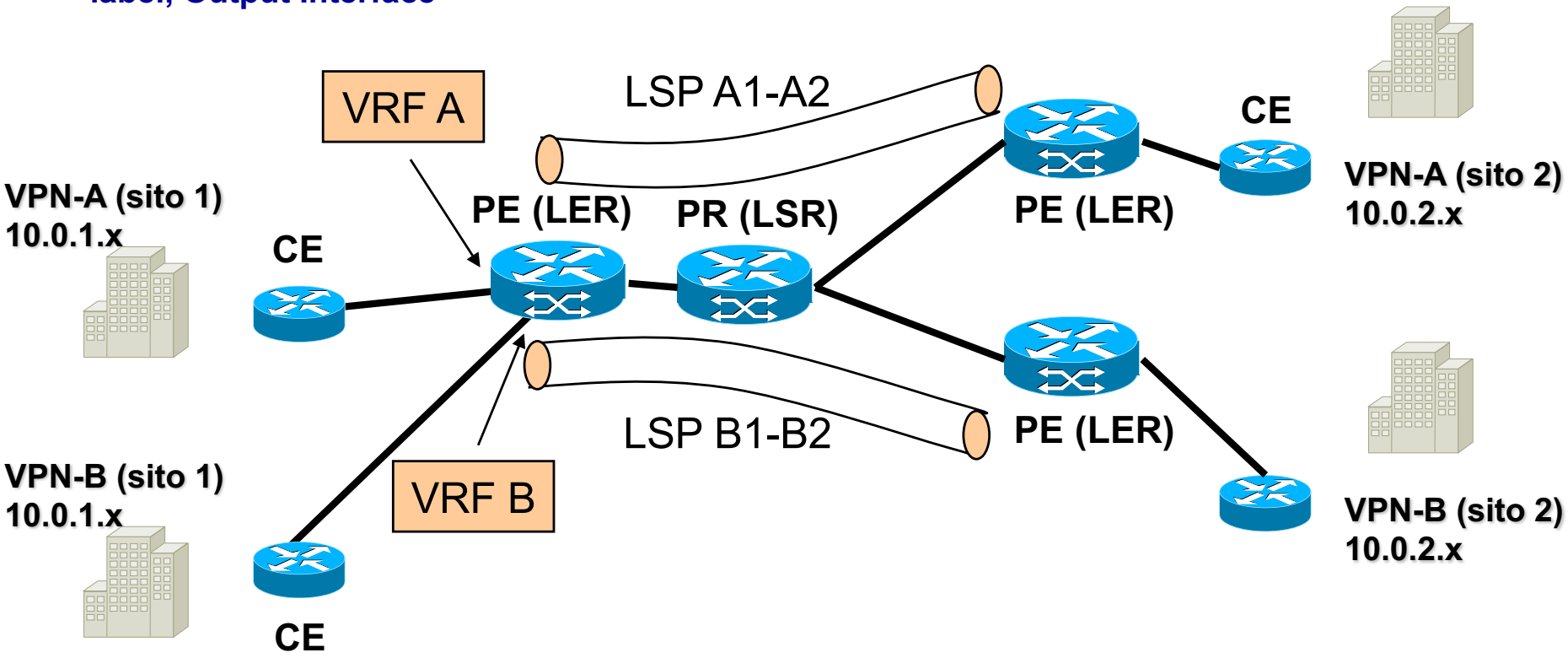
Etichetta interna: identifica l'interfaccia d'uscita che deve usare il PE di destinazione

Etichette esterne: identificano lo LSP PE-PE

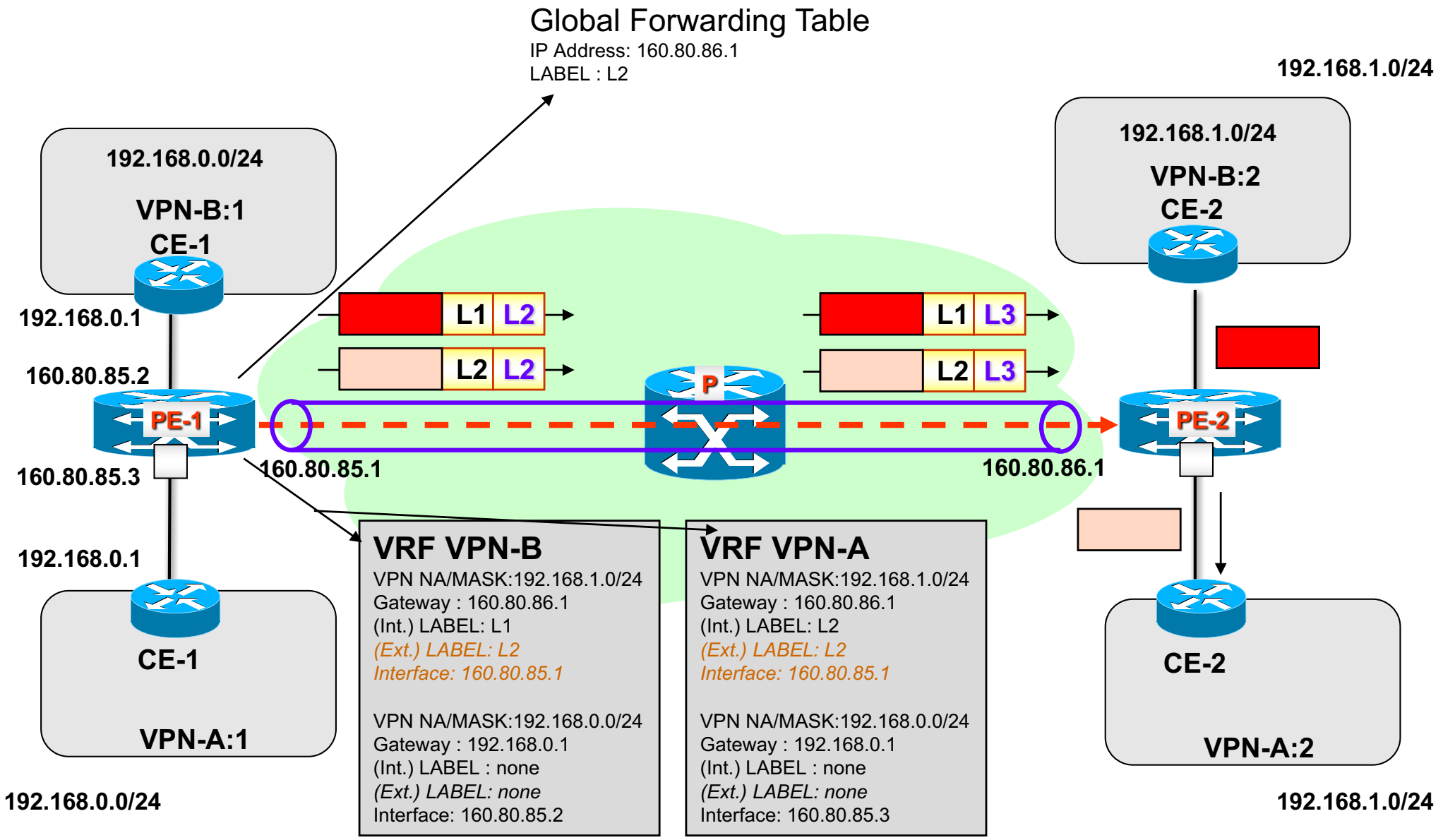


Classificazione del PE

- Problema: come fa il PE ad inoltrare/classificare sul giusto tunnel (e.s. (L1+L2) per i pacchetti provenienti dal CE VPN A:1) ?
- Soluzione: deve saper riconoscere a quale VPN appartengono i pacchetti. Praticamente, questa informazione è dedotta dall'interfaccia su cui un pacchetto è ricevuto
- Pertanto a seconda della VPN di appartenenza, il forwarding MPLS del pacchetto cambia. Tecnicamente, il PE possiede tante tabelle di forwarding quante sono le VPN a lui connesse. Ogni tabella *virtuale* prende il nome di VPN Routing and Forwarding (VRF)
- Una entry della VRF contiene (logicamente) la tupla <VPN network address, VPN mask, Next PE IP Address, Internal label, Output Interface>
- Oltre alla VRF, un PE possiede una Global Forwarding Table (GRT) che permette ad un PE di raggiungere un altro PE. Logicamente una entry della GRT è la tupla <PE IP address, external label, Output Interface>



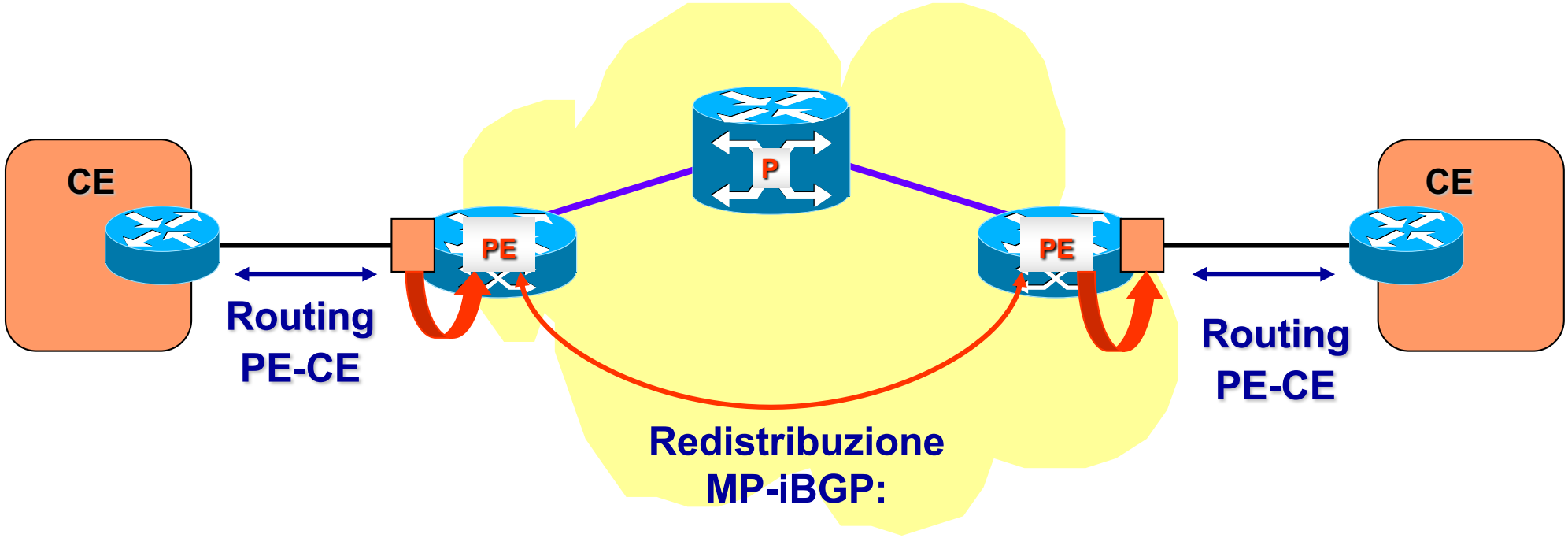
VRF e GFT


Global Forwarding Table
IP Address: 160.80.86.1
LABEL : L2
192.168.1.0/24
192.168.0.0/24
VPN-B:1
CE-1
192.168.1.0/24
VPN-B:2
CE-2
192.168.0.1
160.80.85.2
L1 L2
L2 L2
P
L1 L3
L2 L3
PE-1
PE-2
160.80.85.3
160.80.85.1
160.80.86.1
192.168.0.1
CE-1
VPN-A:1
CE-2
VPN-A:2
192.168.0.0/24
192.168.1.0/24
VRF VPN-B
VPN NA/MASK:192.168.1.0/24
Gateway : 160.80.86.1
(Int.) LABEL: L1
(Ext.) LABEL: L2
Interface: 160.80.85.1
VPN NA/MASK:192.168.0.0/24
Gateway : 192.168.0.1
(Int.) LABEL : none
(Ext.) LABEL: none
Interface: 160.80.85.2
VRF VPN-A
VPN NA/MASK:192.168.1.0/24
Gateway : 160.80.86.1
(Int.) LABEL: L2
(Ext.) LABEL: L2
Interface: 160.80.85.1
VPN NA/MASK:192.168.0.0/24
Gateway : 192.168.0.1
(Int.) LABEL : none
(Ext.) LABEL: none
Interface: 160.80.85.3

Popolamento della GFT e delle VRF

- La Global Forwarding Table è configurata dal provider durante le fasi di set-up della MPLS/VPN backbone (i.e., LSP fra PEs)
- Pertanto, la GFT può essere popolata o manualmente (nel caso di set-up di LSP manuali) oppure automaticamente nel caso di set-up gestiti da protocolli di segnalazione quali LDP, RSVP-TE o CR-LDP
- Le VRF constano di due categorie di instradamenti
  - » Instradamenti verso il sito locale
  - » Instradamenti verso i siti remoti
- Gli instradamenti verso i siti locali sono:
  - » Configurati a mano
  - » Ottenuti da specifici protocolli di routing (OSPF, RIP, etc.) che girano sulla tratta CE-PE
- Gli instradamenti remoti sono ottenuti attraverso un protocollo che è una estensione di BGP-4 e prende il nome di MultiProtocol (interior) BGP, ovvero MP-iBGP (anche MP-BGP)

Popolazione delle VRF



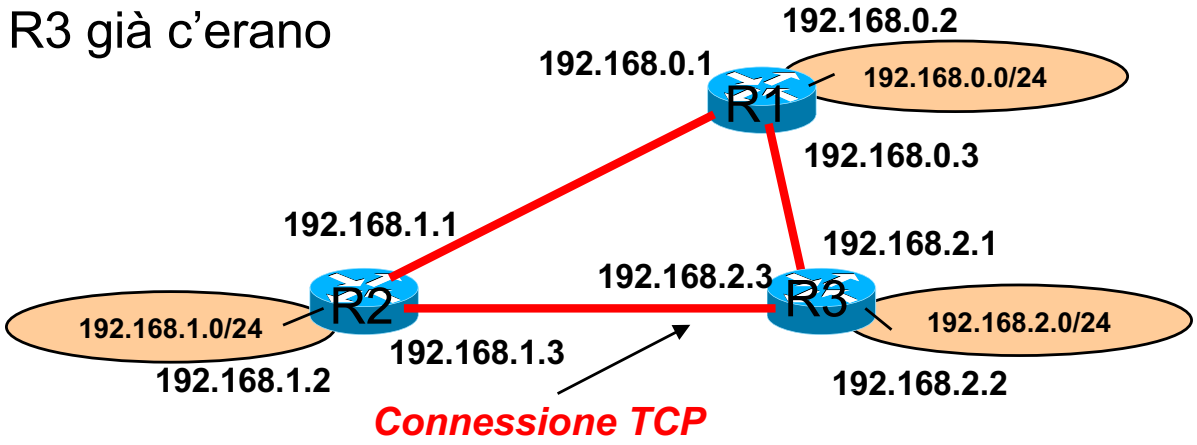
- Routing CE-PE: Statico, RIP, OSPF, eBGP
- Routing PE-PE: MP-iBGP = MultiProtocol-internal BGP

Principi di BGP (Border Gateway Protocol)

- **È un protocollo di routing di tipo Distance vector che gira su una overlay fatta da connessioni TCP**
  - » **Un router comunica ai suoi peer (vicini) la sua tabella di routing**
  - » **Da queste informazioni di raggiungibilità delle subnet i nodi della rete aggiornano le loro tabelle di routing inserendo nella tabella i percorsi più brevi**
  - » **La topologia della overlay ha un impatto su quelle che saranno le tabelle di routing**
  - » **Ogni link della overlay (i.e., TCP connection) è un link della underlay (i.e., un hop IP)…non è vero il viceversa**
  - » **I percorsi seguono lo shotest-path sulla overlay, se la overlay coincide con la rete fisica allora il risultato sarà anche lo shortest path fisico**

Principi di BGP (Border Gateway Protocol)

R1 entra in rete
R2 ed R3 già c'erano



Routing table R1

Net id	mask	interface	*(next-hop)* gateway	Metric
192.168.0.0	/24	192.168.0.2	0.0.0.0	0

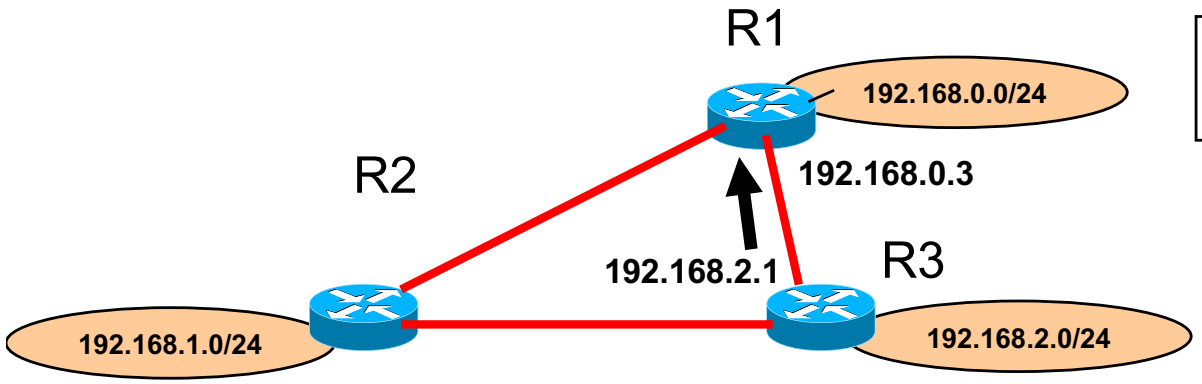
Routing table R2

Net id	mask	interface	gateway	Metric
192.168.1.0	/24	192.168.1.2	0.0.0.0 (local)	0
192.168.2.0	/24	192.168.1.3	192.168.2.3	1

Routing table R3

Net id	mask	interface	gateway	Metric
192.168.1.0	/24	192.168.2.3	192.168.1.3	1
192.168.2.0	/24	192.168.2.2	0.0.0.0	0

Principi di BGP (Border Gateway Protocol)



Routing table R1

Net id	mask	interface	gateway *(next-hop)*	Metric
192.168.0.0	/24	192.168.0.2	0.0.0.0	0

Routing table R3

Net id	mask	interface	gateway	Metric
192.168.1.0	/24	192.168.2.2	192.168.1.3	1
192.168.2.0	/24	192.168.2.0	0.0.0.0	0

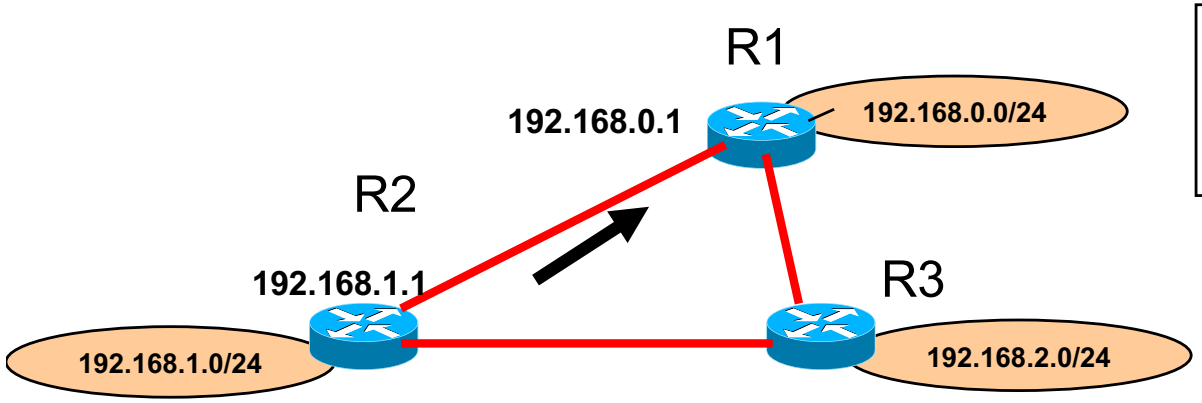
Annuncio BGP di R3

Net id	mask	nexthop	Metric
192.168.1.0	/24	192.168.2.1	1
192.168.2.0	/24	192.168.2.1	0

Routing table R1

Net id	mask	interface	gateway *(next-hop)*	Metric
192.168.0.0	/24	192.168.0.2	0.0.0.0	0
192.168.1.0	/24	192.168.0.3	192.168.2.1	2
192.168.2.0	/24	192.168.0.3	192.168.2.1	1

Principi di BGP (Border Gateway Protocol)



Routing table R1

Net id	mask	interface	*(next-hop)* gateway	Metric
192.168.0.0	/24	192.168.0.2	0.0.0.0	0
192.168.1.0	/24	192.168.0.3	192.168.2.1	2
192.168.2.0	/24	192.168.0.3	192.168.2.1	1

Routing table R2

Net id	mask	interface	gateway	Metric
192.168.1.0	/24	192.168.1.2	0.0.0.0 (local)	0
192.168.2.0	/24	192.168.1.3	192.168.2.3	1

Annuncio BGP di R2

Net id	mask	nexthop	Metric
192.168.1.0	/24	192.168.1.1	0
192.168.2.0	/24	192.168.1.1	1

Routing table R1

Net id	mask	interface	*(next-hop)* gateway	Metric
192.168.0.0	/24	192.168.0.2	0.0.0.0	0
192.168.1.0	/24	192.168.0.1	192.168.1.1	1
192.168.2.0	/24	192.168.0.3	192.168.2.1	1

Popolamento delle VRF

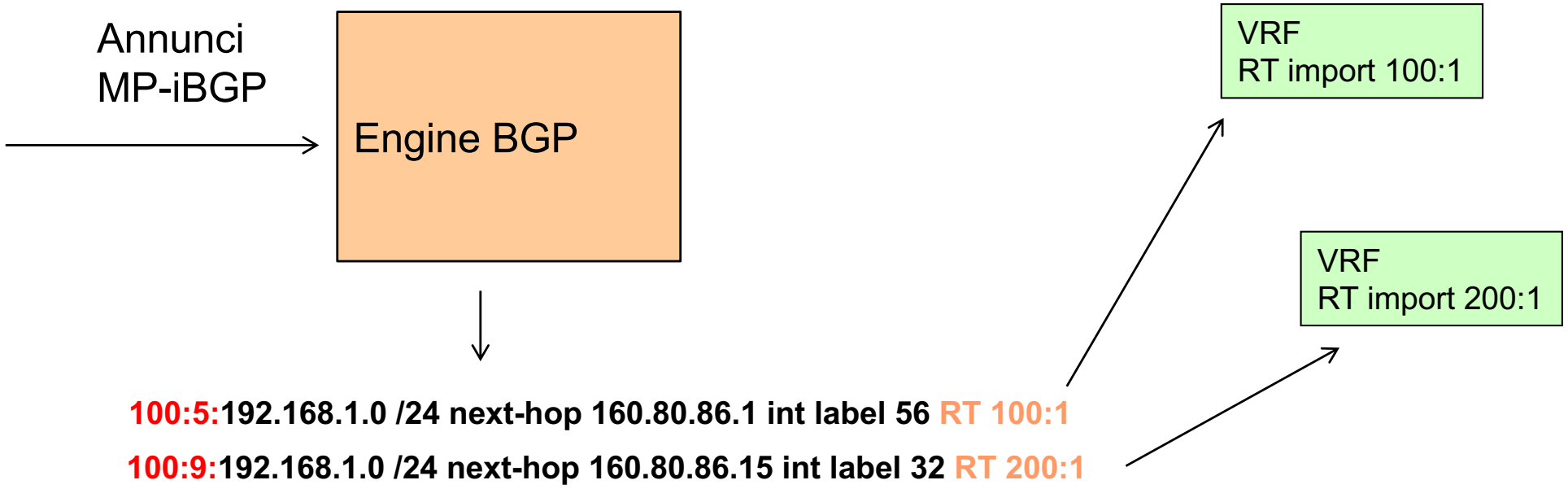
- Le VRF si “sincronizzano” fra loro scambiandosi le informazioni di raggiungibilità all’interno di annunci BGP (MP-iBGP)
- Un annuncio MP-iBGP è mandato da un PE a tutti gli altri PE; i.e., esiste una overlay full mesh fra PE.
- Assunzione: il costo dell’*hop diretto* tra due PE è unitario essendo questo un solo hop di livello IP (+ hops di livello MPLS)
- Uno stesso annuncio MP-iBGP porta informazioni di raggiungibilità relative ai prefissi più VRF

Route Distinguisher

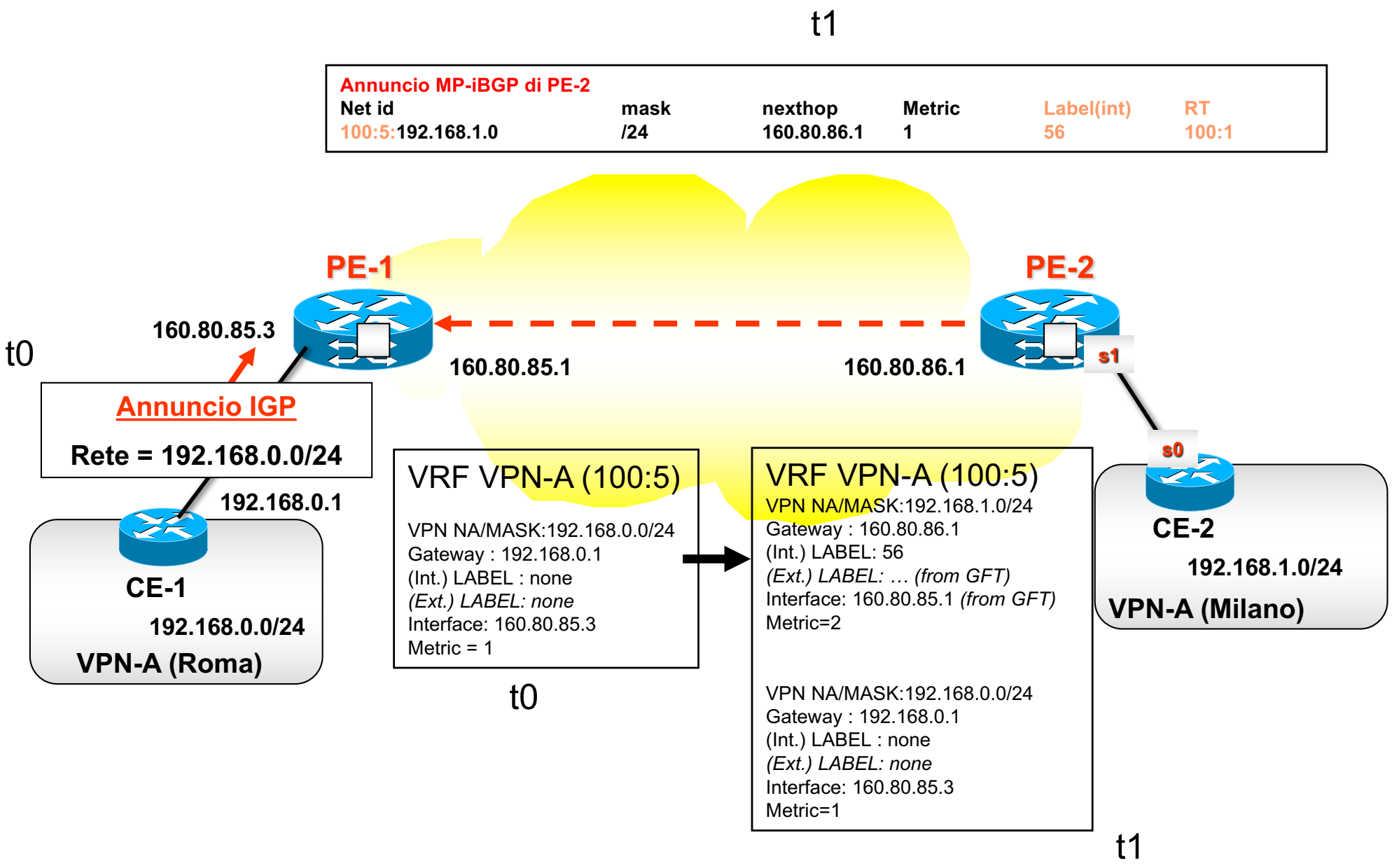
- Attraverso gli annunci MP-iBGP, l'engine BGP del PE calcola il next-hop (e la label interna) verso ogni prefisso avvertito.
- VRF appartenenti a VPN diverse possono avvertire un stesso prefisso privato in quanto possono avere spazi di indirizzamento overlapped.
- Per differenziare prefissi overlapped (ovvero farli vedere all'engine BGP come reti diverse), una VRF è caratterizzata da un identificativo denominato Route Distinguisher (64 bit)
  - » Solitamente tutte le VRF di una stessa VPN usano lo stesso Route Distinguisher, poichè i prefissi di una stessa VPN non andranno in conflitto, quindi si può riusare lo stesso distinguisher

Route Distinguisher

- Lo RD è anteposto alle net_id delle entry dell'annuncio MP-iBGP
- Le rotte calcolate dal BGP sono inserite nelle **VRF abilitate (vedi Route Target)**



Popolazione delle VRF



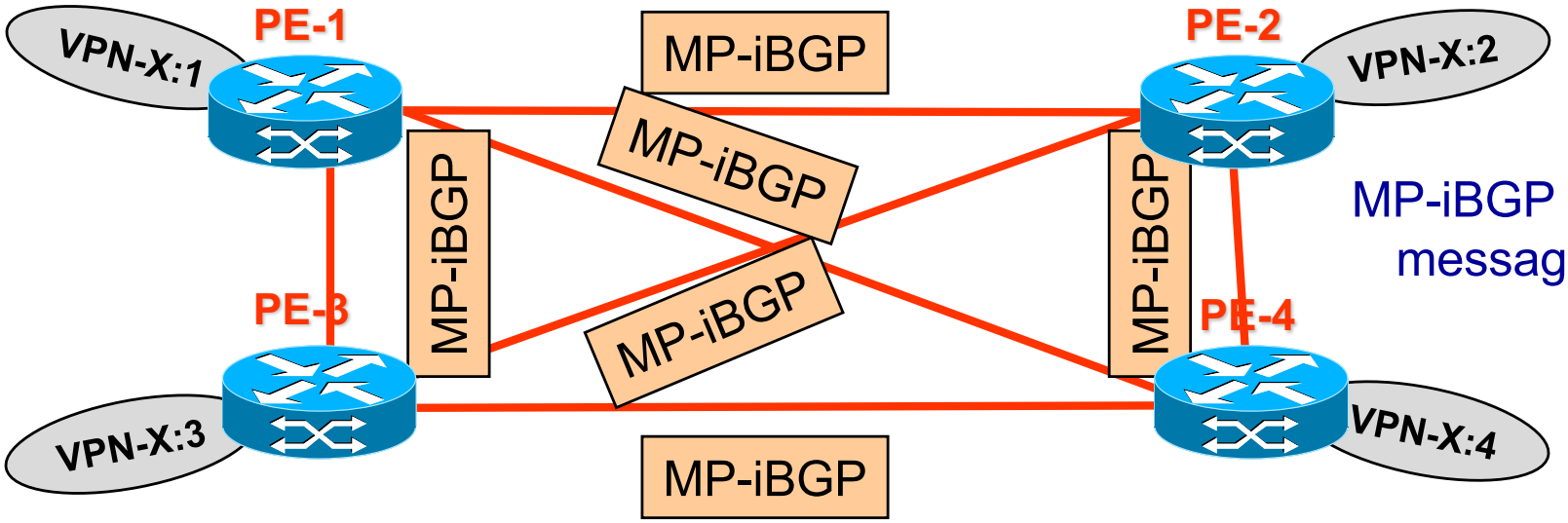
Route Target

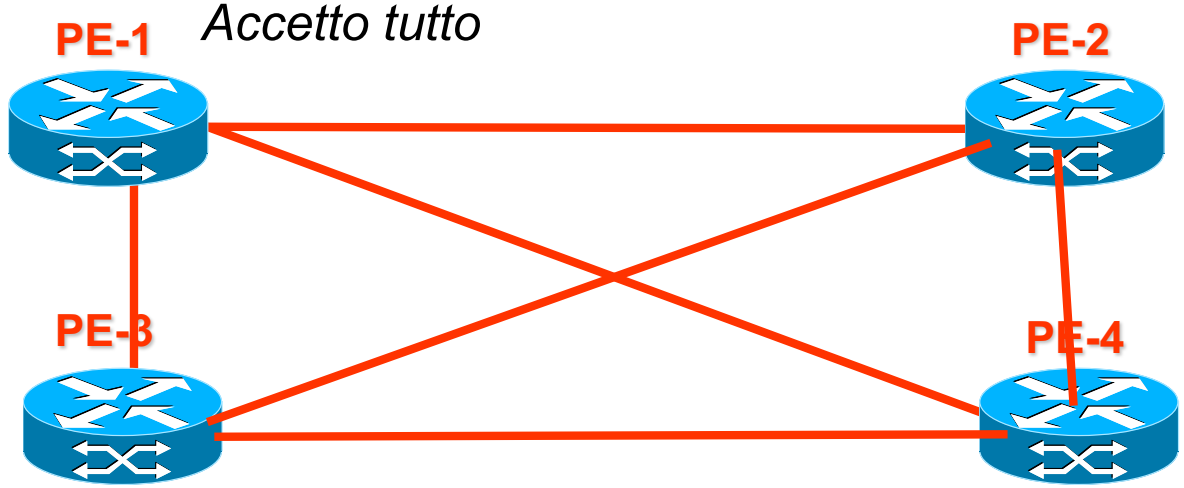
- Se i messaggi MP-iBGP sono diffusi fra tutti i PEs, tutte le VPN hanno una topologia full-mesh
- Problema: e se volessi topologie diverse per le diverse VPN ?
- Per i principi del BGP, data una topologia overlay su cui si diffondono i messaggi MP-iBGP, la topologia (di forwarding) della VPN-x è l'insieme degli overlay shortest-path fra una qualsiasi coppia di nodi.
- Poichè i collegamenti diretti fra due PE hanno metrica 1→ la topologia della VPN-x coincide con la topologia della overlay su cui si diffondono i messaggi MP-iBGP
- Se la overlay su cui diffondono gli annunci MP-iBGP è full-mesh, allora la topologia della VPN è full-MESH,

Route Target

- **Per cambiare la topologia logica della VPN-x bisogna cambiare la overlay su cui si diffondono i messaggi MP-iBGP della VPN-x**
  - » **Soluzione 1: creare una overlay di diffusione MP-iBGP diversa per ogni VPN**
    - » **Cons: elevata gestione, impossibilità di aggregare dentro lo stesso messaggio MP-iBGP informazioni di routing relative a più VPN, etc.**
  - » **Soluzione 2:**
    - » **Avere una overlay full-mesh di diffusione MP-iBGP comune fra tutti i PE**
    - » **Definire la overlay specifica che si vuole avere per una data VPN-x;**
    - » **Fare flooding sulla overlay comune degli annunci MP-iBGP,**
    - » **I riceventi elaborano solo gli annunci provenienti dai link della overlay specifica**

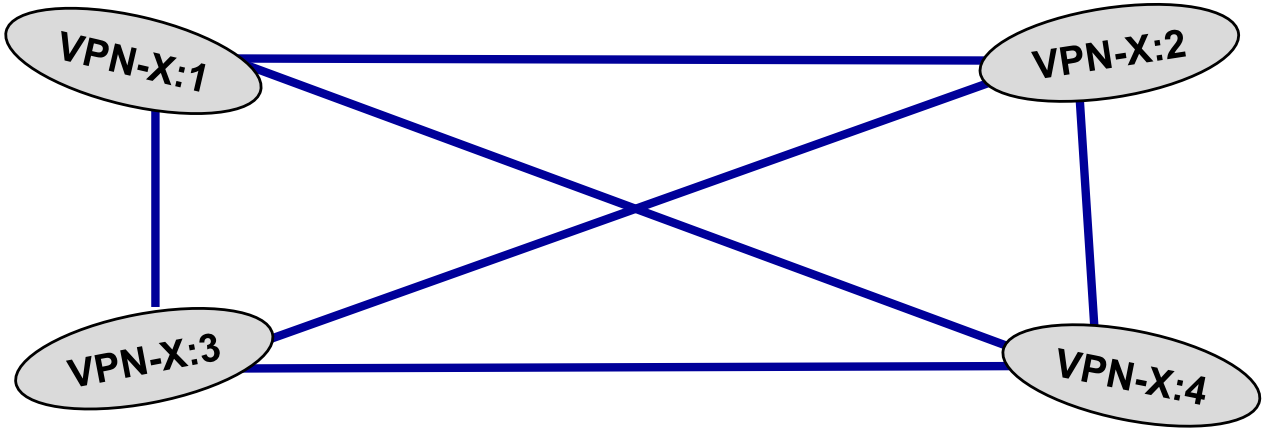
Popolamento delle VRF - VPN Full Mesh



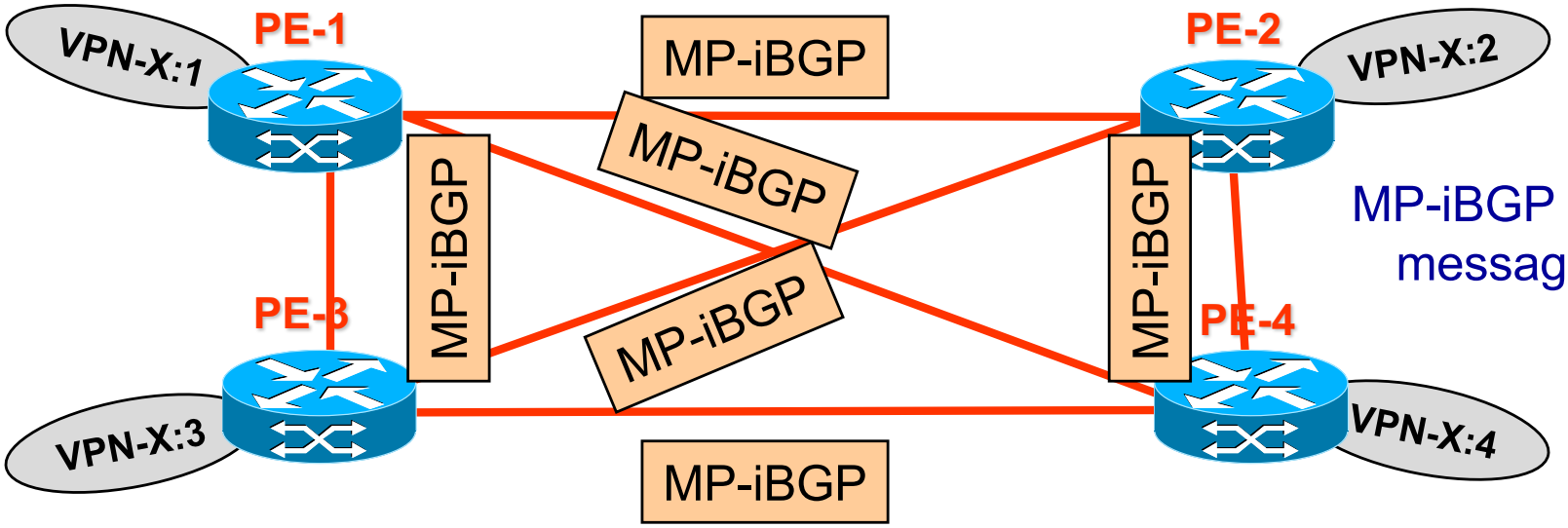


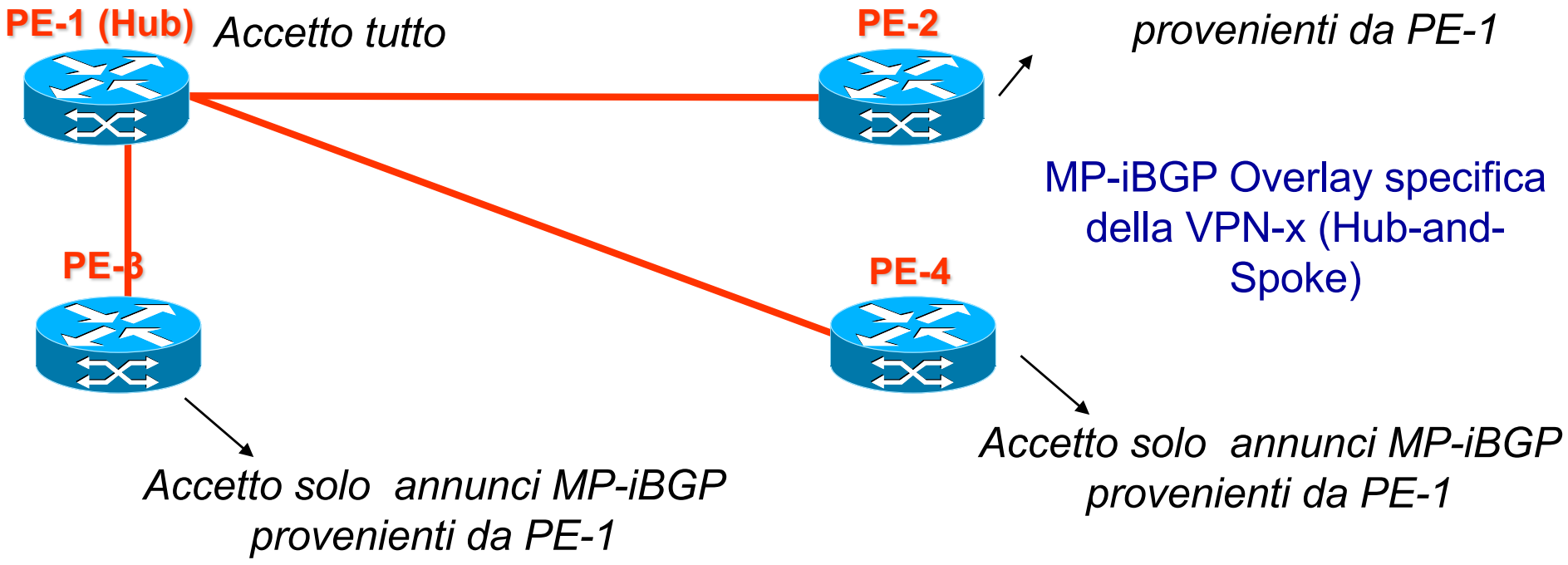
Popolamento delle VRF - VPN Full Mesh

Topologia VPN risultante



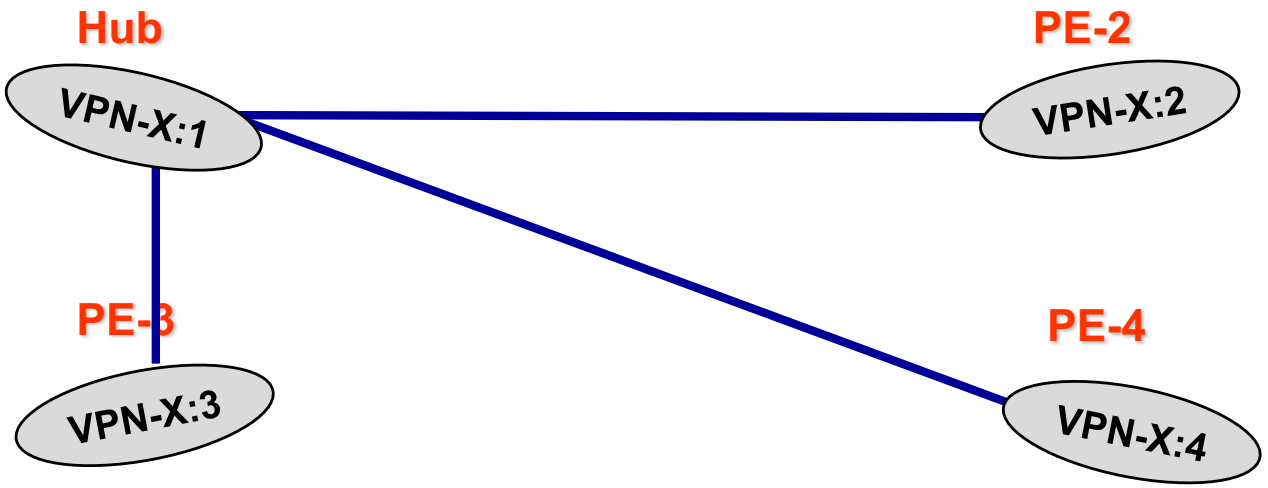
Popolamento delle VRF - VPN Hub and Spoke





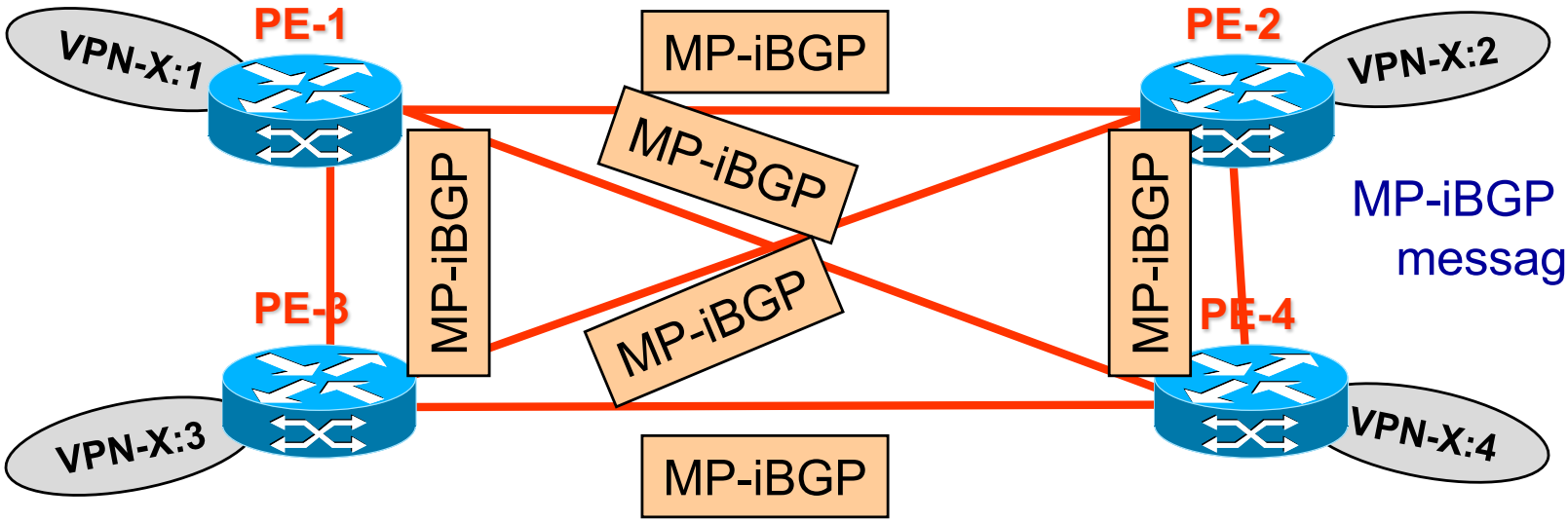
Popolamento delle VRF - VPN Hub and Spoke

Topologia VPN risultante

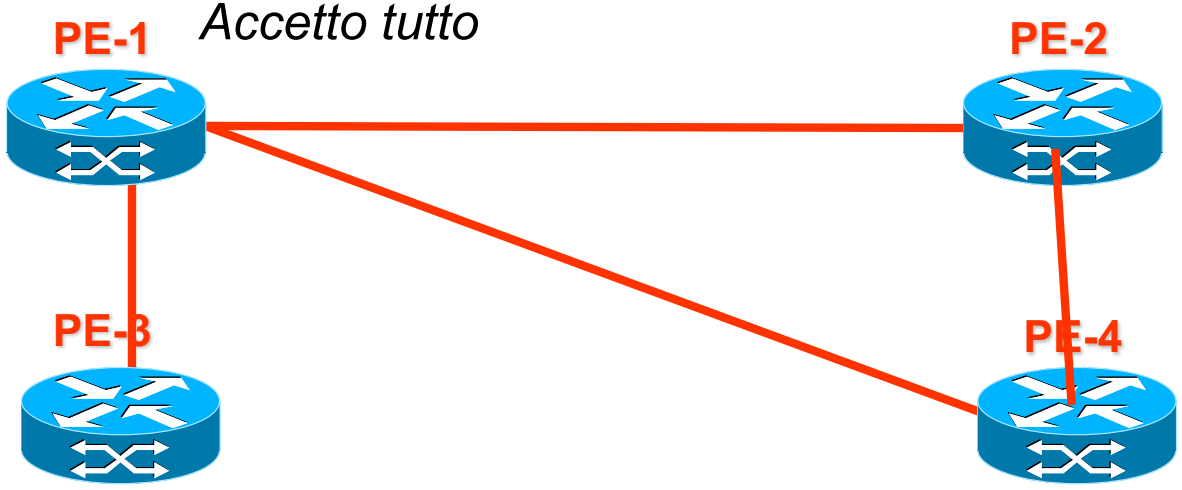


Nota: annunci MP-iBGP (come nnunci iBGP) non si ripropagano su link iBGP. Quindi per permettere agli spoke di comunicare tra loro la VRF dell'hub deve esportare una default

Popolamento delle VRF - VPN Partial Mesh



MP-iBGP Overlay comune su cui i messaggi vengono mandati in flooding



Accetto tutto

Accetto solo annunci MP-iBGP provenienti da PE-1, PE-4

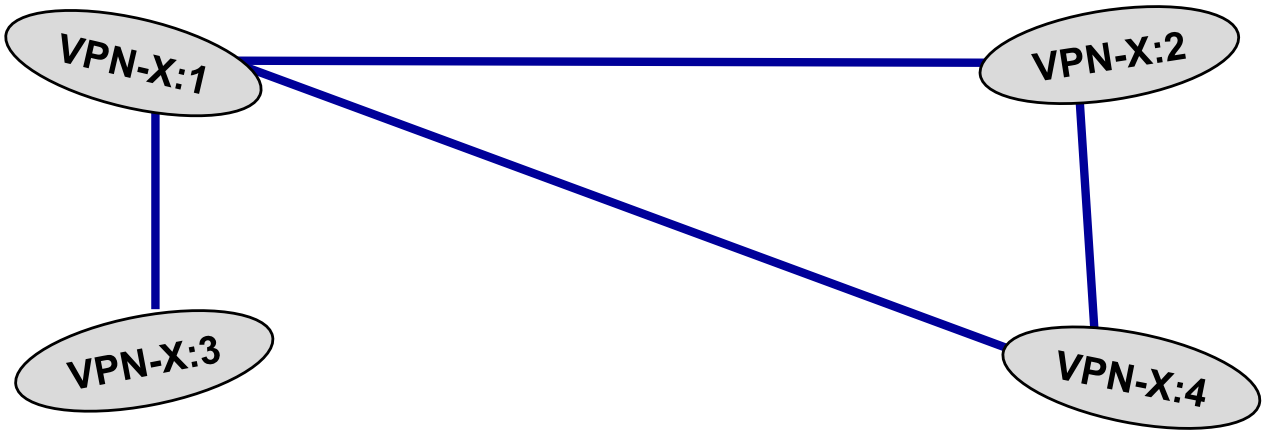
MP-iBGP Overlay specifica della VPN-x (Partial-MESH)

Accetto solo annunci MP-iBGP provenienti da PE-1

Accetto solo annunci MP-iBGP provenienti da PE-1, PE-2

Popolamento delle VRF - VPN Full Mesh

Topologia VPN risultante

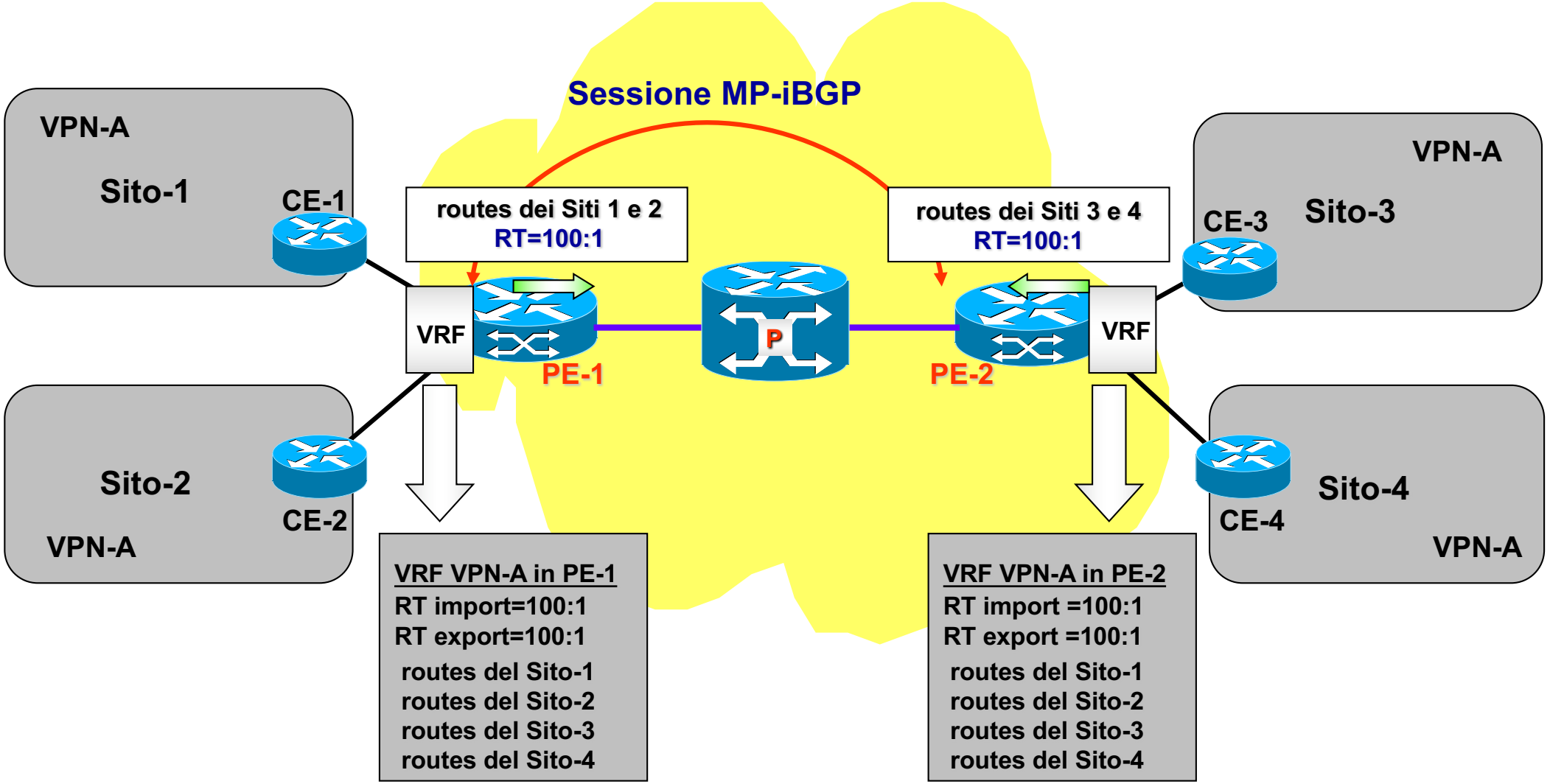


Route Target

- **Il concetto di Route Target concretizza l'approccio di realizzazione della overlay specifica della VPN-x precedentemente discusso e quindi permette di definire la topologia della VPN-x**
- **E' il modo VPN/MPLS per dire ad una VRF-x di "accettare solo un subset di annunci MP-iBGP"**
- **Tecnica:**
  - **Ogni VRF che transmette annunci, etichetta (*export*) questi annunci con unn identificativo configurabile da 8 bytes chiamato Route Target**
  - **Ogni VRF è abilitata a ricevere (*import*) solo annunci con un subset configurabile di Route Targets**

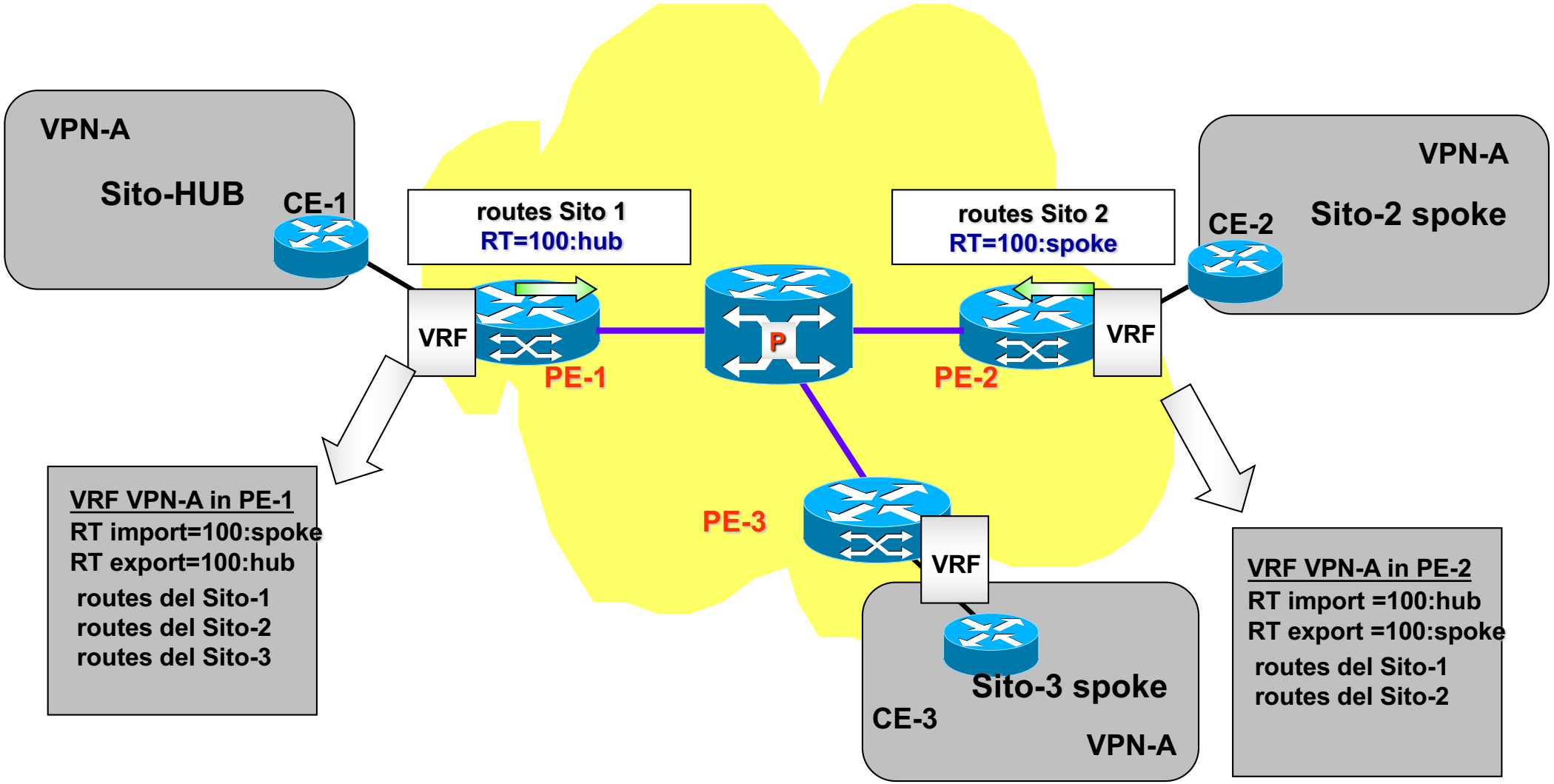
Utilizzo del “Route Target”: Esempio 1

- VPN full mesh



Utilizzo del “Route Target”: Esempio 2

- VPN Hub and spoke



Configurazione VPN/MPLS

- **Inizializzazione**
  - **Configurazione LSP MPLS (es. con LDP) tra tutti i PE**
  - **Attivazione peering BGP per prefissi di tipo *vpnv4* (RD+net_id) tra tutti i PE**
- **Cosa fare per aggiungere un altro sito**
  - **Cliente:**
    - **Comunicare al provider la necessità di un altro sito VPN e la relativa topologia della VPN**
    - **Installare un CE come gateway aziendale**
    - **Configurare il *default gateway* del CE con l'indirizzo IP del PE di accesso**
    - **Opzionale: attivare sul CE un protocollo di routing sulla tratta CE-PE (e.s, OSPF)**
  - **Provider**
    - **Inizializzare una nuova VRF sul PE d'accesso**
    - **Definire/Configurare Route Distinguisher**
    - **Definire/Configurare Route Import e Route Export sul PE locale ed eventualmente aggiornare I RT import/export sugli altri PE della VPN coerentemente alla topologia richiesta dal cliente**
    - **Associare interfaccia del PE alla VRF**
    - **Attivare MP-iBGP sulla VRF appena definita**

VPN/MPLS conclusioni

- Approccio semplice per il cliente
- La sicurezza delle comunicazioni in gioco è affidata al provider
- Possibile costo elevato
- Complessita di configurazione da parte del provider modesta
- Necessità del provider di ingegnerizzare il traffico nella Backbone VPN/MPLS in modo tale da offrire la QoS richiesta dalle VPNs che insitono sul Backbone MPLS
  - » Traffic engineering per gli LSP fra PEs

Cisco IOS configuration

On all involved PE

- Create user VRF
  - PE-1(config)# ip vrf vpnB
  - PE-1(config-vrf)#rd 200:0
  - PE-1(config-vrf)#route-target import 200:2
  - PE-1(config-vrf)#route-target export 200:1
  - PE-1(config-vrf)#exit
- Add to the VRF a manual route towars local CE in case of no routing protool on the PE-CE link
  - PE-1(config)#ip route vrf vpnB 192.168.0.0 255.255.255.0 160.2.11.2
- Associate interface to the VRF
  - PE-1(config)#int f0/1
  - PE-1(config-if)#ip vrf forwarding vpnB
  - PE-1(config-if)#ip address 160.2.11.1 255.255.255.25

Cisco IOS configuration

- Configure BGP
- Optionally disable IPv4 peering
  - router bgp 3269
    - no bgp default ipv4-unicast
- Create peering with all PEs (if not existent)
  - neighbor 2.2.2.2 remote-as 3269
  - neighbor 2.2.2.2 update-source Loopback0
  - neighbor 3.3.3.3 remote-as 3269
  - neighbor 3.3.3.3 update-source
- Activate vpnv4 peerings
  - address-family vpnv4
    - neighbor 2.2.2.2 activate
    - neighbor 2.2.2.2 send-community extended
    - neighbor 2.2.2.2 next-hop-self
    - exit-address-family

Cisco IOS configuration

- Switch on the BGP advertisements of VRF in case eBGP was not active in the PE-CE link
  - address-family ipv4 vrf vpnB
  - network 192.168.0.0

- In case BGP was active on PE-CE
  - Configure BGP global peering with PE
    - neighbor 160.2.11.2 remote-as 200
    - neighbor 160.2.11.2 update-source FastEthernet0/1
  - Bind VRF to the neighbour
    - address-family ipv4 vrf vpnB
    - neighbor 160.2.11.2 remote-as 200
    - neighbor 160.2.11.2 activate
    - neighbor 160.2.11.2 as-override

Cisco IOS configuration

- **Debug**
  - **show ip vrf**
  - **show ip route vrf vpnB**
  - **show mpls forwarding-table**
    - **Useful to know the external label towards the remote PE**
  - **show ip bgp vpnv4 vrf vpnB labels**
    - **Useful to know the internal label**