Virtual Private Network

Tecnologie e protocolli per Internet II (TPI2)

rev 1.0

Andrea Detti

University of Roma "Tor Vergata"

Electronic Engineering dept.

E-mail: andrea.detti@uniroma2.it

Ringraziamenti: devo un ringraziamento al Prof. Nicola Blefari-Melazzi, al Prof. Stefano Salsano, autori di presentazioni da cui sono alcune delle seguenti slides.

Introduzione

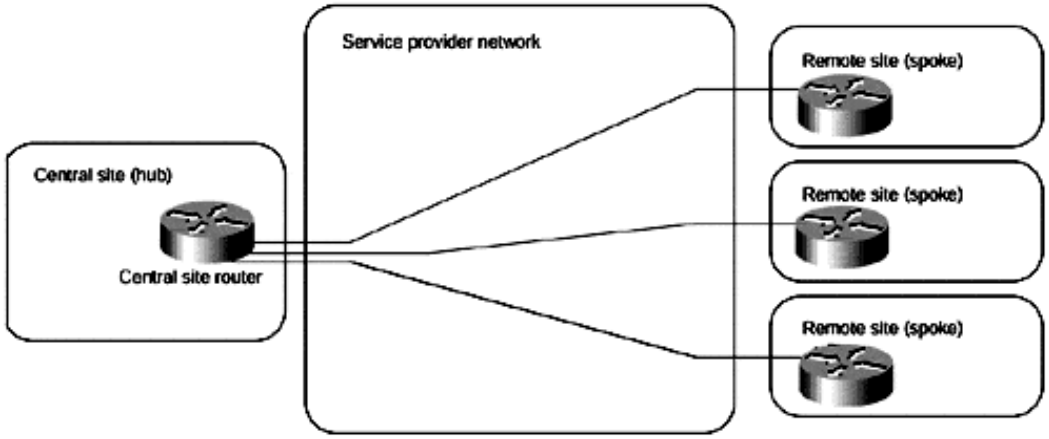
- Permettono lo scambio dei dati tra sedi aziendali distribuite sul territorio
- Rappresenta un servizio di maggiore interesse per i clienti Business
- Reti Private Virtuali
  - » **Private**: permettono comunicazioni private tra i siti aziendali, alla stessa stregua di una rete privata fisica (es. sono mantenuti gli schemi di routing e indirizzamento)
  - » **Virtuali**: i collegamenti sono virtuali e non fisisci. La rete fisica di supporto è pubblica e non privata, ma la gestione delle risorse e le tecniche di sicurezza sono tali da "virtualizzarla" come se fosse privata
- Indirizzamento IP privato
  - » 10.0.0.0/8
  - » 172.16.0.0/12
  - » 192.168.0.0/16
- **Condizione necessaria**: all'interno di una stessa VPN l'indirizzamento deve essere unico

Modelli di VPN

- **Modello di comunicazione**
  - » **Intra-aziendale, ossia esclusivamente tra i siti della stessa azienda (Intranet)**
  - » **Inter-aziendale, ossia tra aziende che hanno interessi comuni (Extranet)**
    - » **Probelma di univocità degli indirizzi**
  - » **VPDN, se è possibile accedere alla VPN dell'azienda dall'esterno dell'azienda stessa con collegamenti di tipo dial-up (es. Radiomobile, PSTN)**
    - » **Problema di assegnazione dell'indirizzo**
- **Modalità di trasporto dell'informazione**
  - » **Overlay: la rete pubblica offerta dall'ISP offre solo funzionalità di trasporto (e.s., leased-line con QoS o trasporto Internet pubblica senza QoS). Le informazioni di routing sono scambiate solo fra i siti aziendali (Customer Edges). La topologia (logica e fisica) è composta da collegamenti punto-punto definiti dal customer (cliente)**
  - » **Peer-to-peer: estende il modello overlay nel senso che la rete pubblica offerta dall'ISP scambia con i siti aziendali anche informazioni di routing. La topologia logica è definita dal customer, la topologia fisica che realizza la topologia logica è decisa dal provider secondo specifici criteri di traffic engineering nella sua rete**

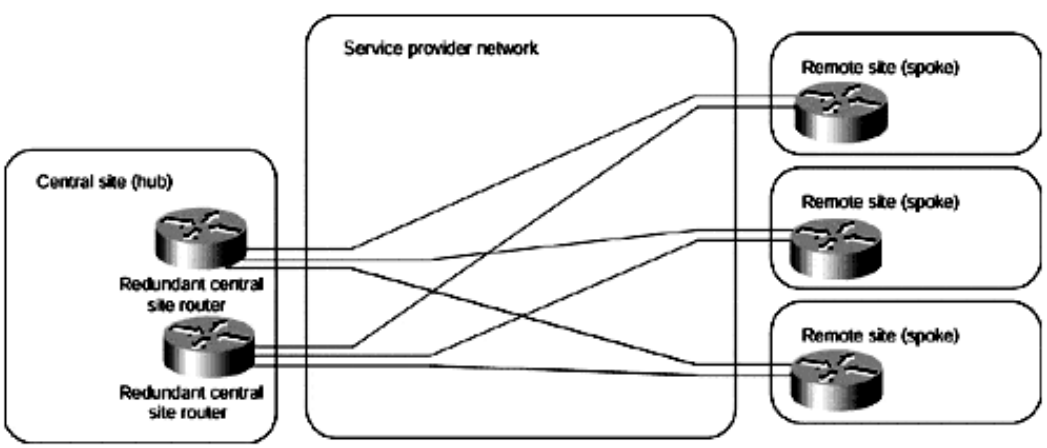
Topologie VPN– Hub and Spoke

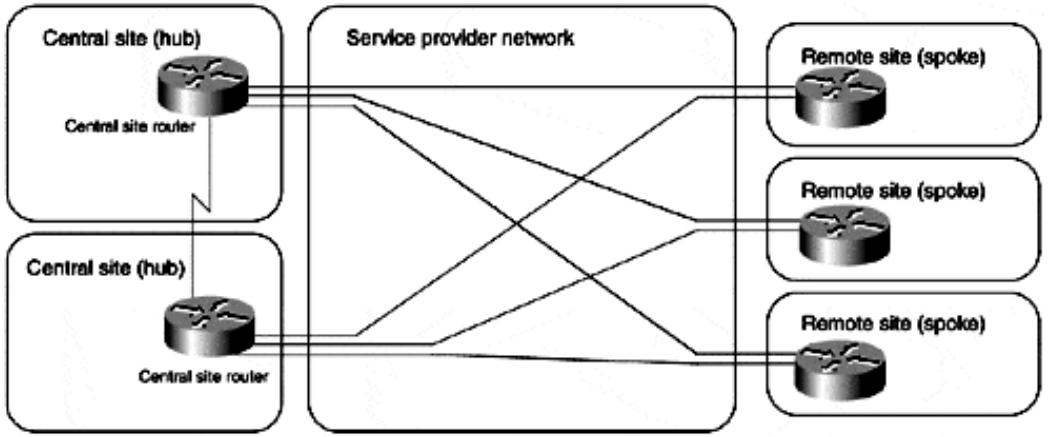
- La topologia di una VPN dipende dalle esigenze dell'azienda, tuttavia molto spesso topologie classiche risolvono i problemi di business dell'azienda
- Hub-and-spoke Topology:
  - » gli uffici remoti (spoke) sono connessi ad un sito centrale (hub).
  - » Fra di loro gli spokes possono scambiare dati, ma questa topologia è adatta quando il traffico inter-spoke è trascurabile rispetto al traffico spoke-hub
  - » Adatta per aziende con una stringente organizzazione gerarchica (e.s., banche)



Topologie VPN– Hub and Spoke

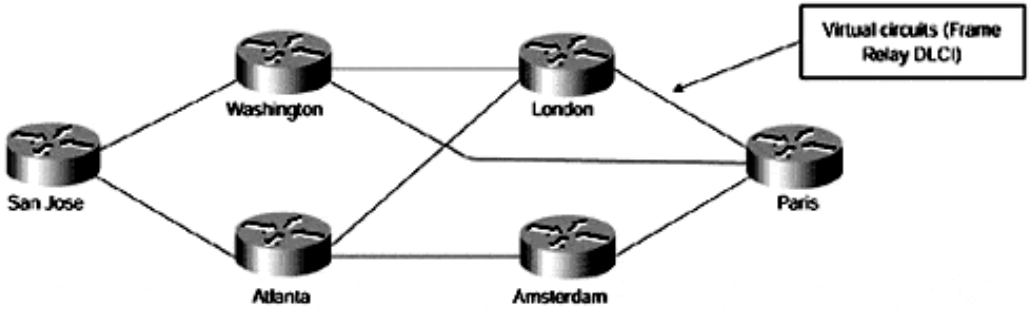
- **Hub Backup**
  - » **Due hub nello stesso sito**
  - » **Due hub in siti diversi connessi con una linea ad alta velocità**





Topologie VPN– Partial- Full-Mesh

- Quando vi è un cospicuo scambio di dati fra i siti aziendali la topologia Hub-and-Spoke è poco efficace in quanto tutto il traffico spoke-spoke attraversa l'hub che diventa quindi il collo di bottiglia
- In questo caso topologie parzialmente o totalmente connesse sono preferibili
- Business case:
  - » Aziende senza una stretta organizzazione gerarchica
  - » Applicazioni di tipo peer-to-peer (messaging o collaboration system)
  - » Per aziende multinazionali in cui il costo della soluzione hub-and-spoke può essere elevato a causa del costo eccessivo di link internazionali.

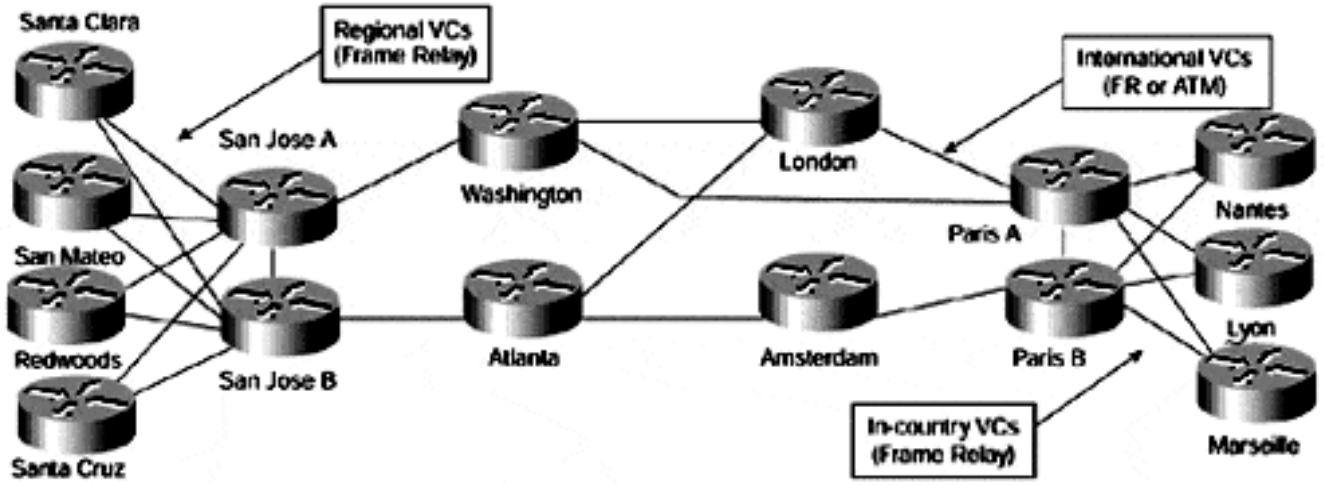


Topologie VPN– Partial- Full-Mesh

- La topologia full-mesh è di facile pianificazione basta avere la matrice di traffico *A(i,j)=x* Mbps e chiedere all'ISP un collegamento fra il sito *i* ed il sito *j con x* Mbps
- Il costo full-mesh può essere elevato poiché il numero di collegamenti affittati è n*(n-1)
- Pertanto si opta spesso per una partial-mesh
- Approccio di pianificazione topologica di una partial mesh
  - » 1) Creare una topologia connessa attraverso collegamenti solo fra sedi che hanno un elevato scambio di dati
  - » 2) Dalla matrice di traffico ed assumendo un routing shortest-path calcolare l'ammontare di banda richiesta su tutti i collegamenti installati
  - » 3) ordinare i collegamenti all'ISP + economico ;-)

Topologie VPN– Hybrid

- VPN molto grandi internazionali sono spesso composte da VPN nazionali di tipo hub-and-spoke e la parte internazioanle (backbone) è una partial-mesh fra gli hubs



Peer-to-Peer VPN

Peer-to-Peer VPN

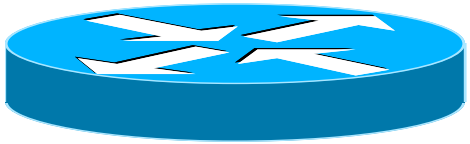
- **Scambio di informazioni di routing con i router dell'ISP, pertanto il routing avviene su un layer composto sia da entita che risiedono in azienda che da entità che risiedono nell'ISP**

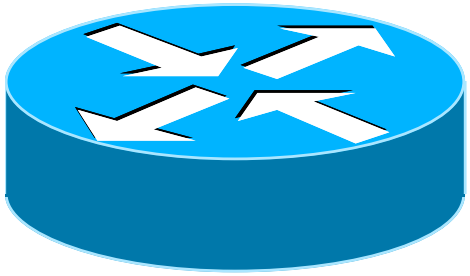
- **Sono di fatto basate sulla soluzione BGP/MPLS**
  - **Il gateway aziendale trasferisce dati all'ISP e questo a sua volta si preoccupa del forwarding verso gli altri siti aziendali, pertanto il routing (topologia delle connessioni) è di fatto nelle mani dell'ISP**
  - **Plug & Play, l'aggiunta di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

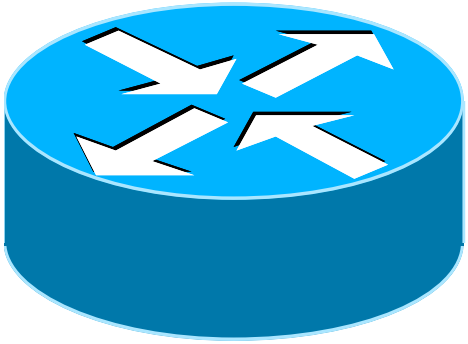
VPN BGP/MPLS

Peer-to-Peer VPN

Elementi di una VPN BGP/MPLS







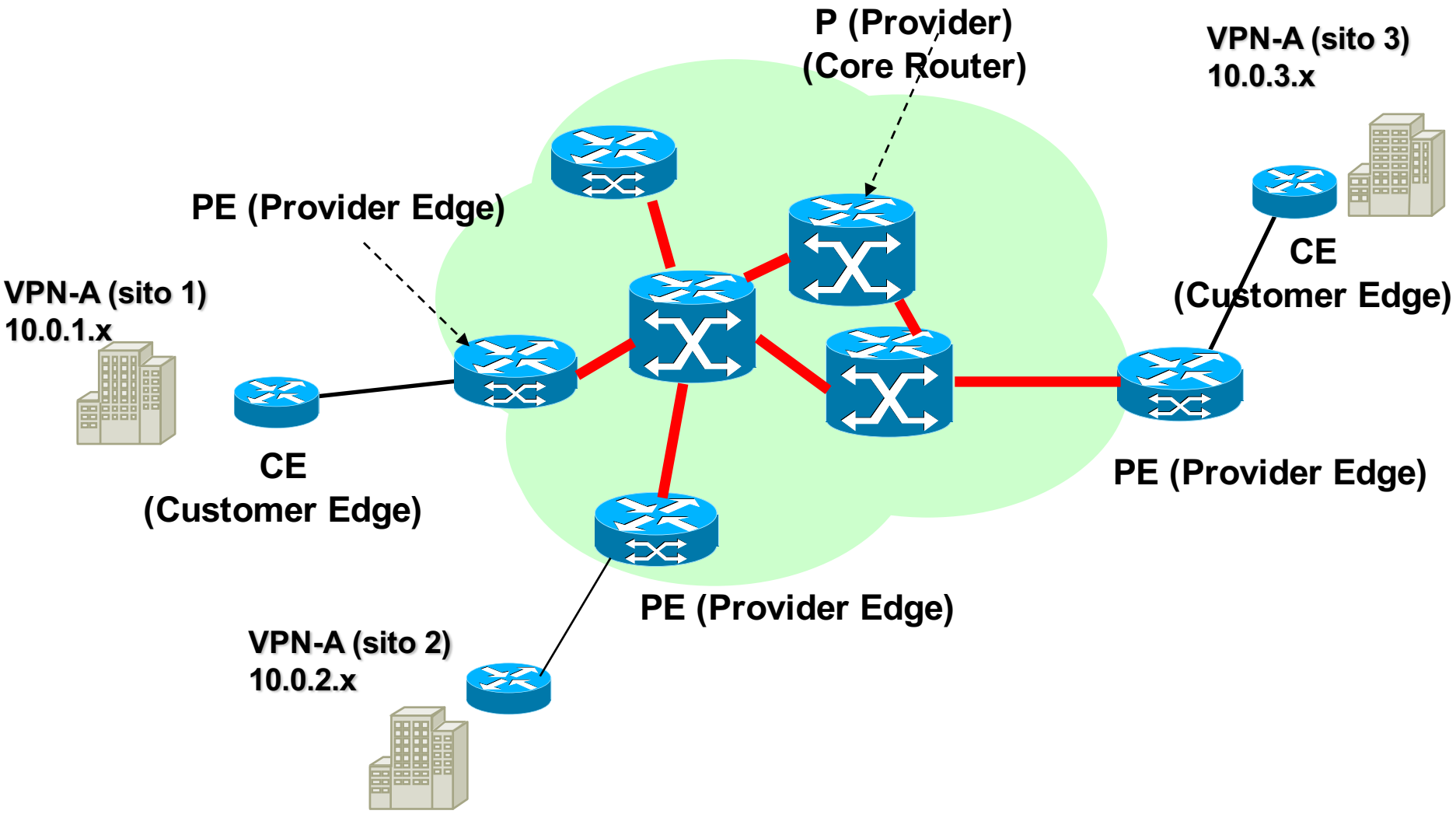
Customer Edge : è il router del sito aziendale che si interconnette con l'ISP fornitore del servizio VPN BGP/MPLS. Ha funzionalità di routing IP classiche. A livello di routing, il suo unico peer è il Provider edge con cui scabia info tramite BGP

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

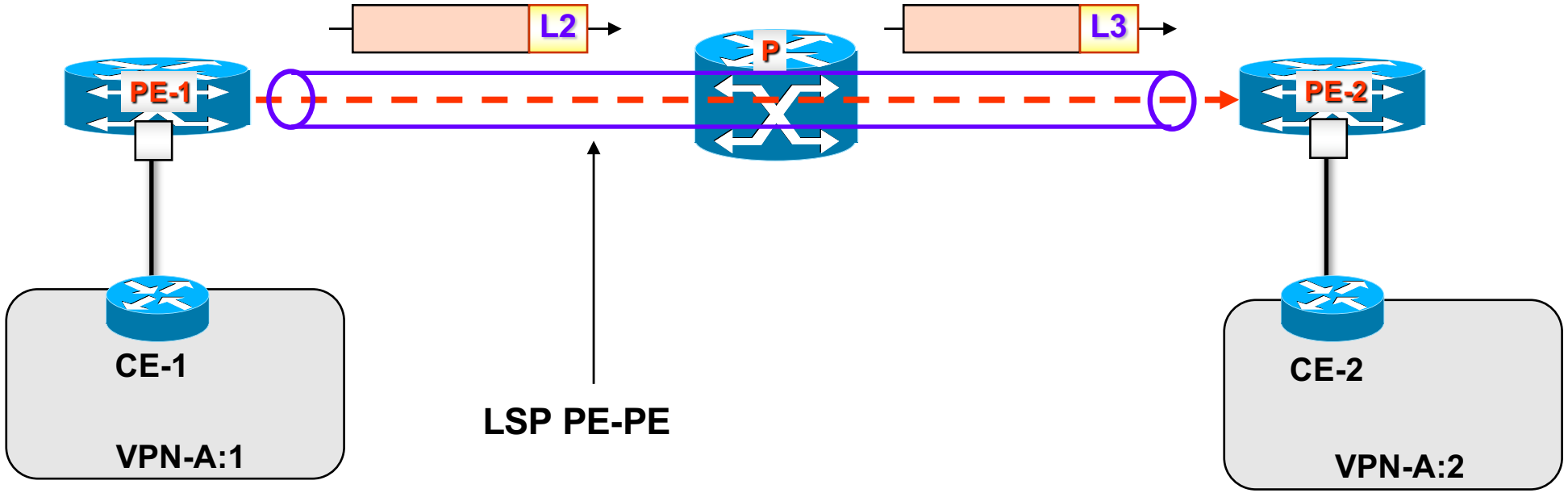
MPLS/VPN Backbone : rete MPLS con LSP opportunamente configurati per collegare fra loro tutti i PE

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 !

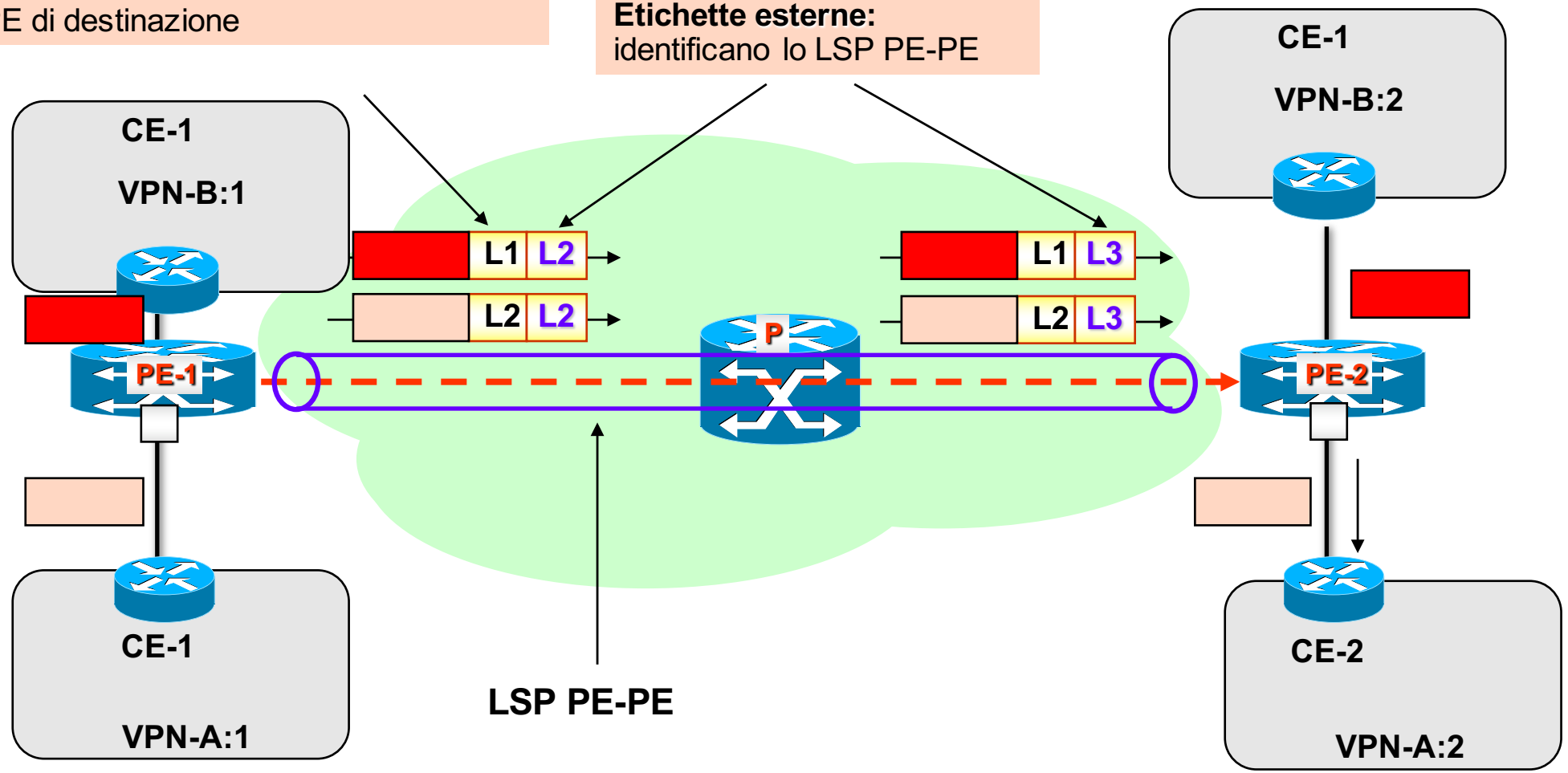


Meccanismo di inoltro dei pacchetti

Soluzione: label stacking con due etichette

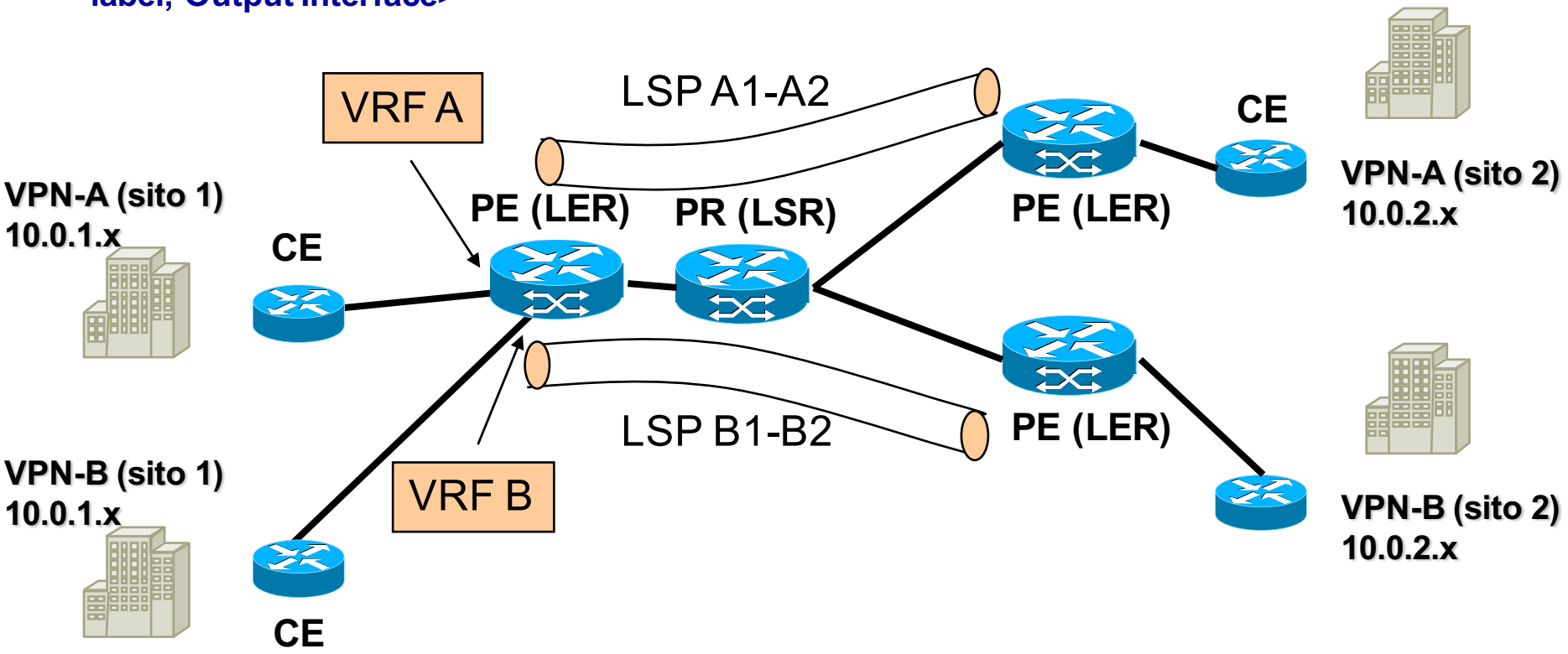
Etichetta interna: identifica l'interfaccia d'uscita che deve usare il PE di destinazione

Etichette esterne: identificano lo LSP PE-PE

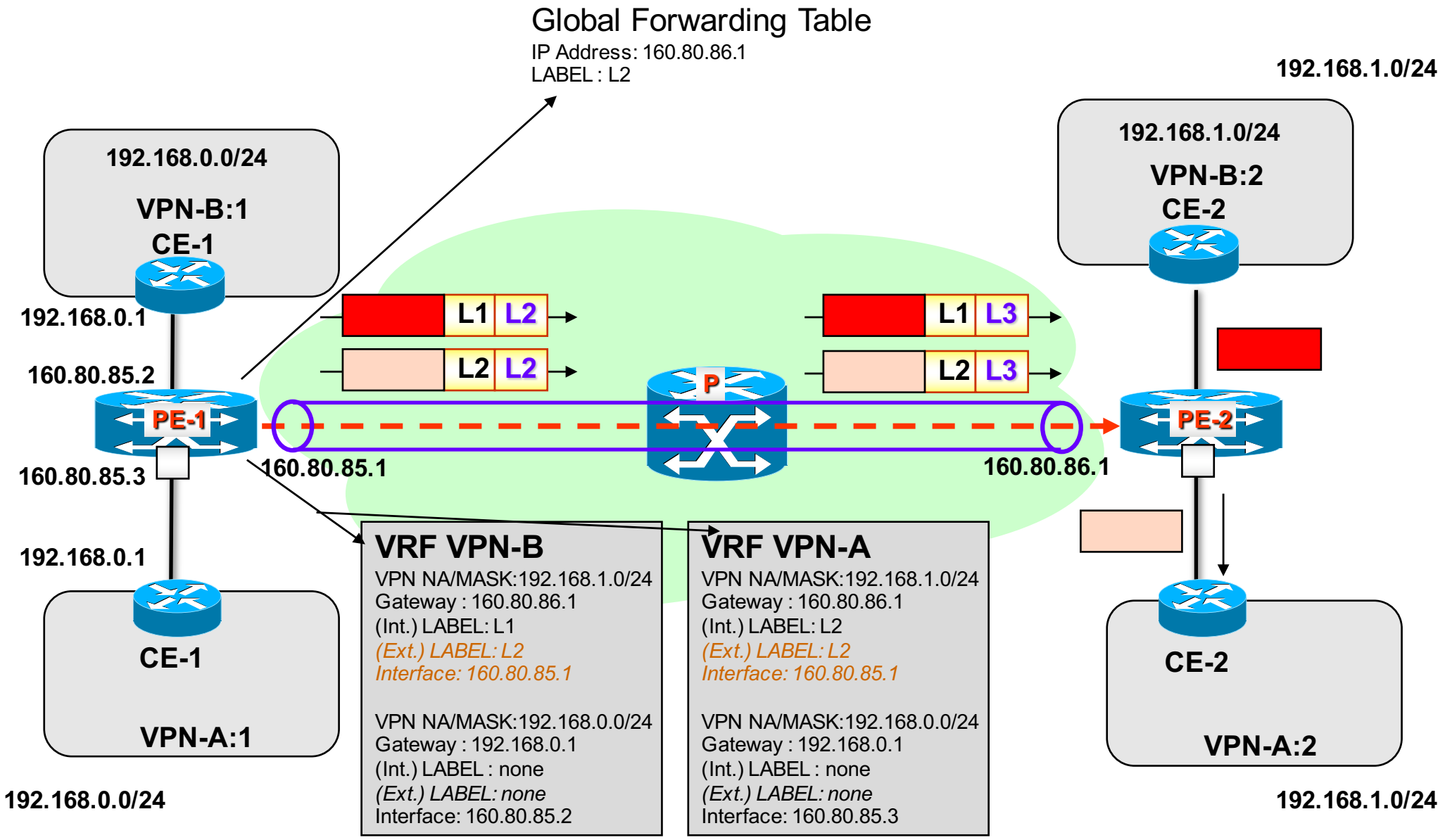


Classificazione del PE

- 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>



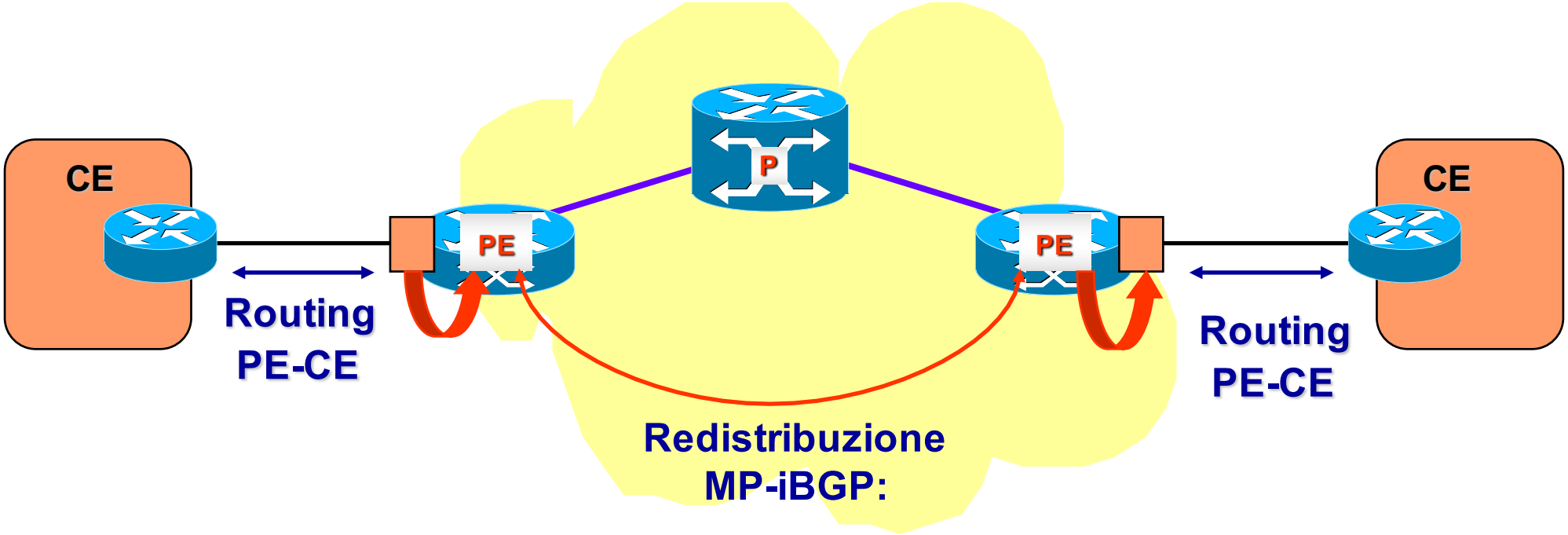
VRF e GFT


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
L1 L3
L2 L3
P
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



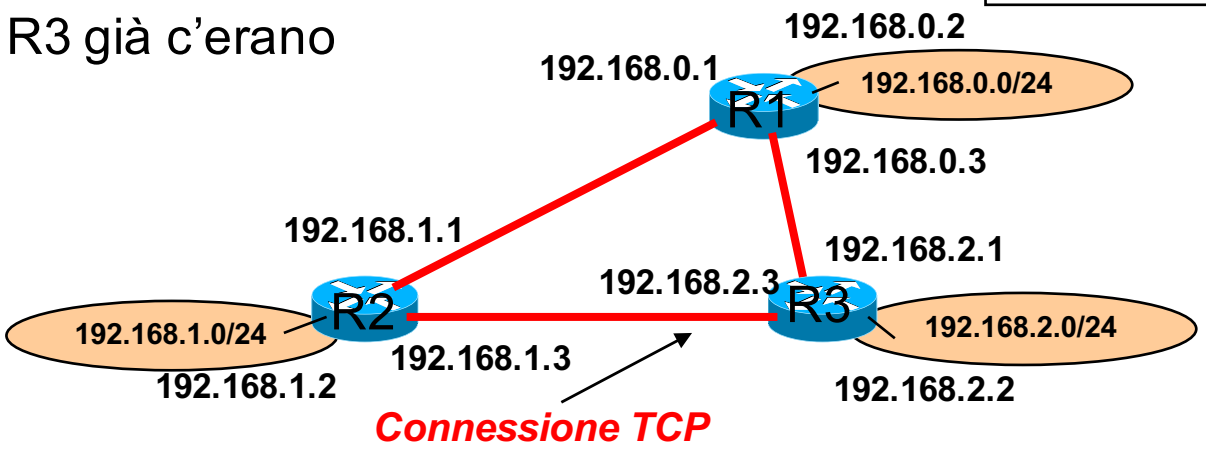
- Routing CE-PE: Statico, RIP, OSPF, eBGP
- Routing PE-PE: MP-iBGP = MultiProtocol-internal BGP

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 *(next-hop)*

Net id	mask	interface	gateway	Metric
192.168.0.0	/24	192.168.0.2	0.0.0.0	0

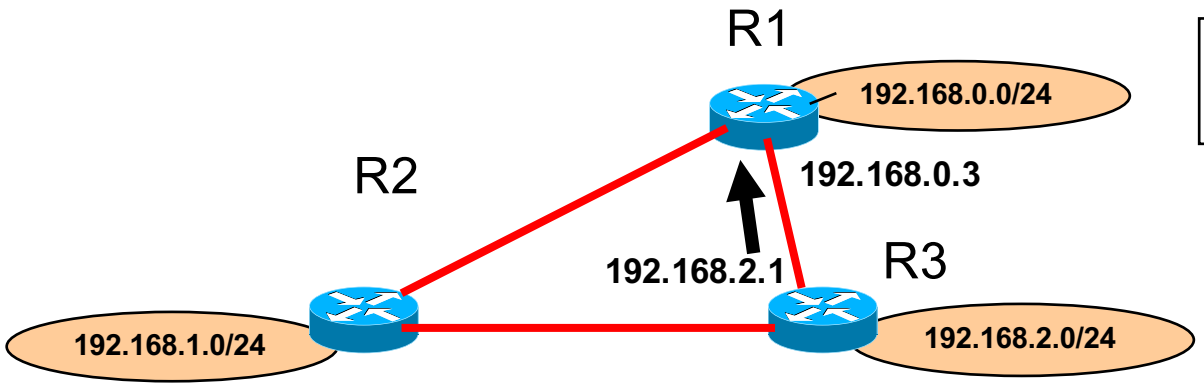
Routing table R2

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

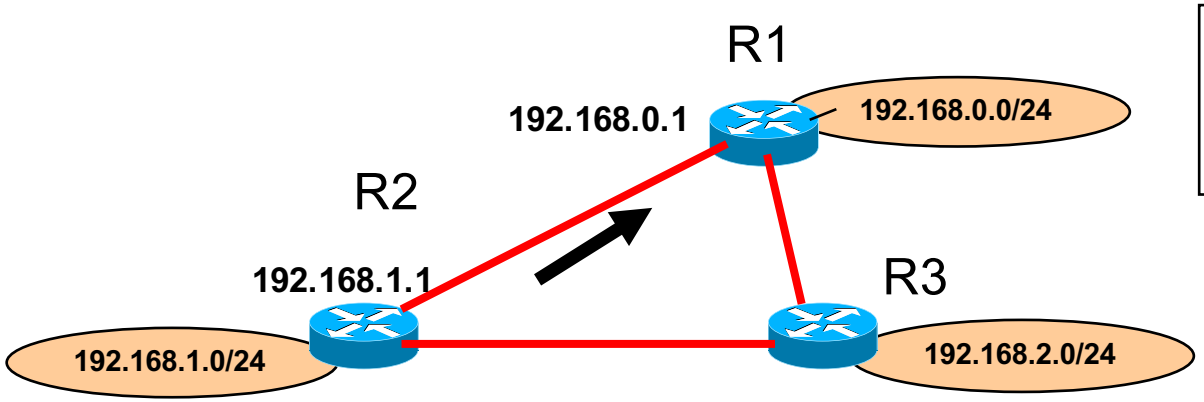
Annuncio BGP di R3

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	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

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

Popolamento delle VRF

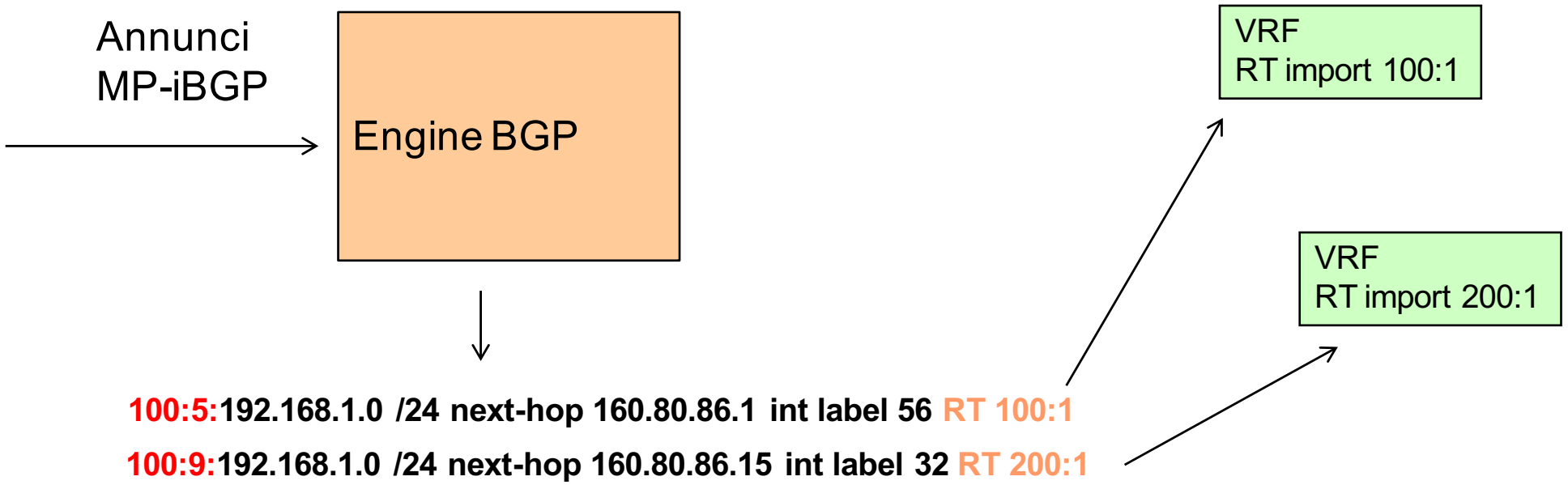
- Le VRF si “sincronizzano” fra loro scambiandosi le informazioni di raggiungibilità all’interno di annunci BGP (MP-iBGP)
- Un annuncio MP-iBGP è mandato da un PE a tutti gli altri PE; i.e., esiste una overlay full mesh fra PE.
- Assunzione: il costo dell’*hop diretto* tra due PE è unitario essendo questo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

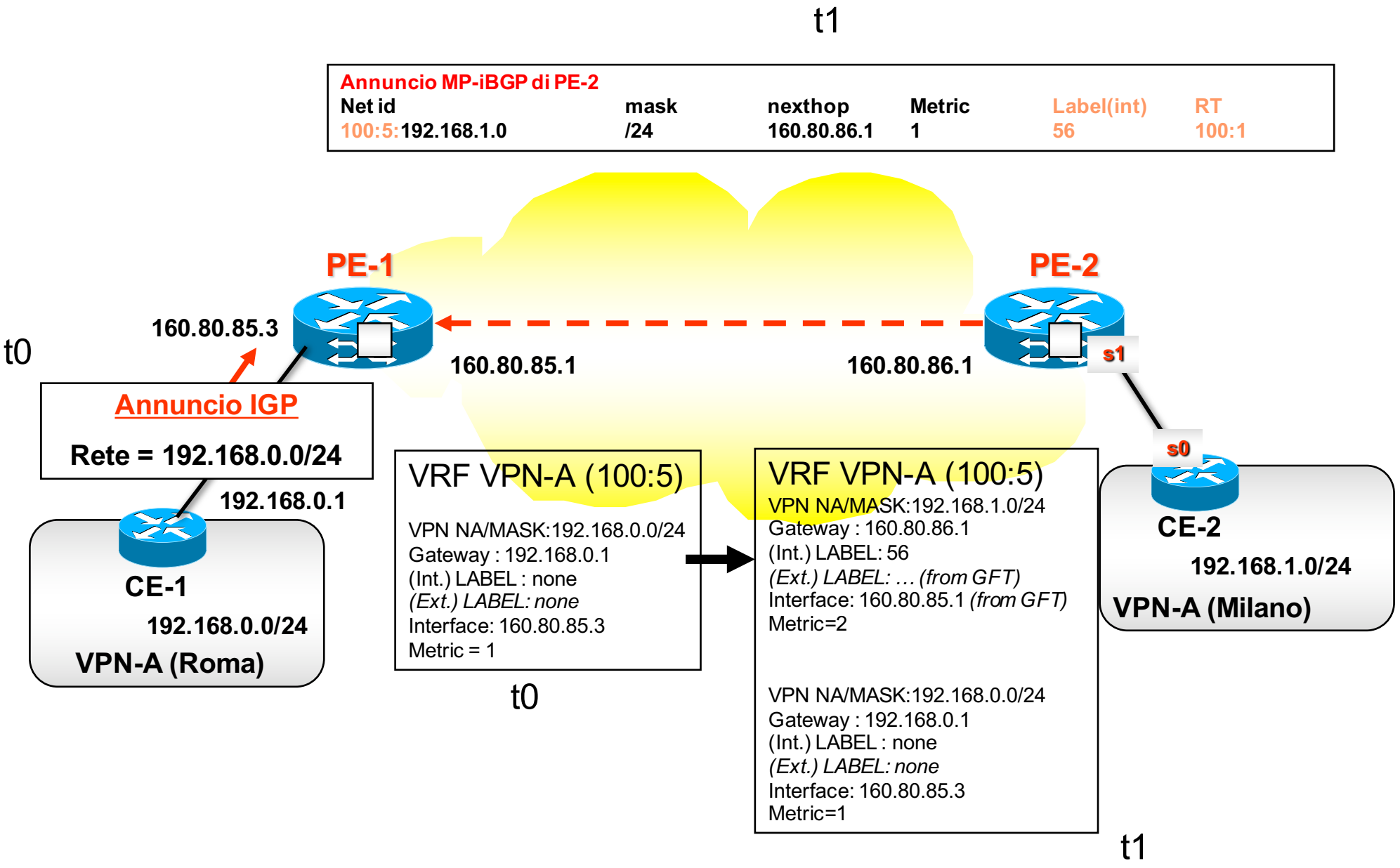
- Attraverso gli annunci MP-iBGP, l'engine BGP del PE calcola il next-hop (e la label interna) verso ogni prefisso avvertito.
- VRF appartenenti a VPN diverse possono avvertire un stesso prefisso privato in quanto possono avere spazi di indirizzamento overlapped.
- Per differenziare prefissi overlapped (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



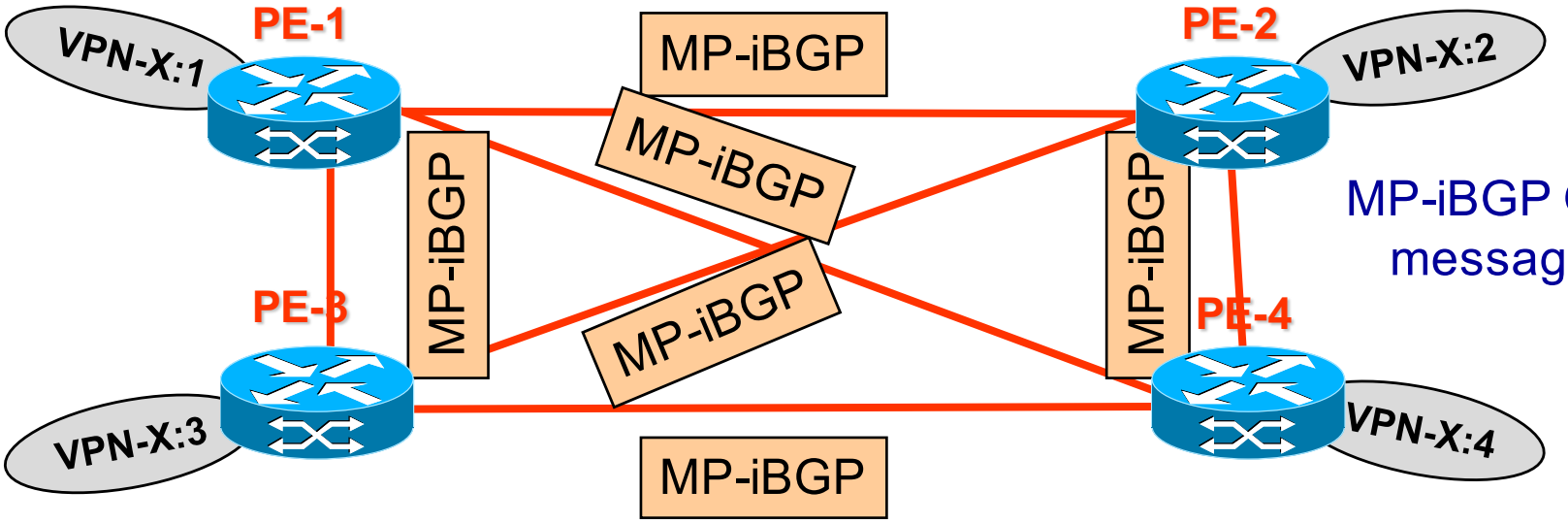
Route Target

- 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**

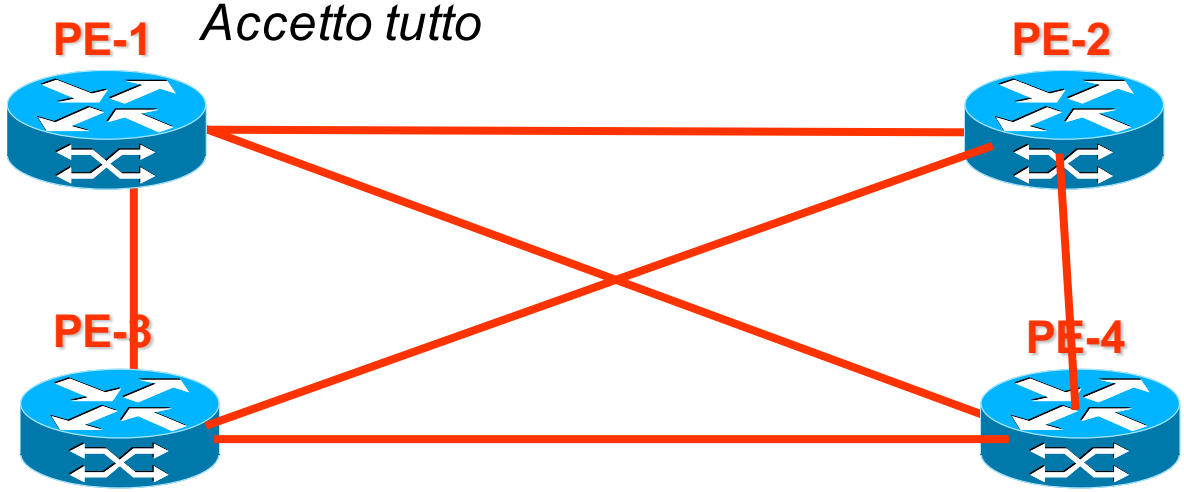
Popolamento delle VRF - VPN Full Mesh



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

Accetto tutto

Accetto tutto



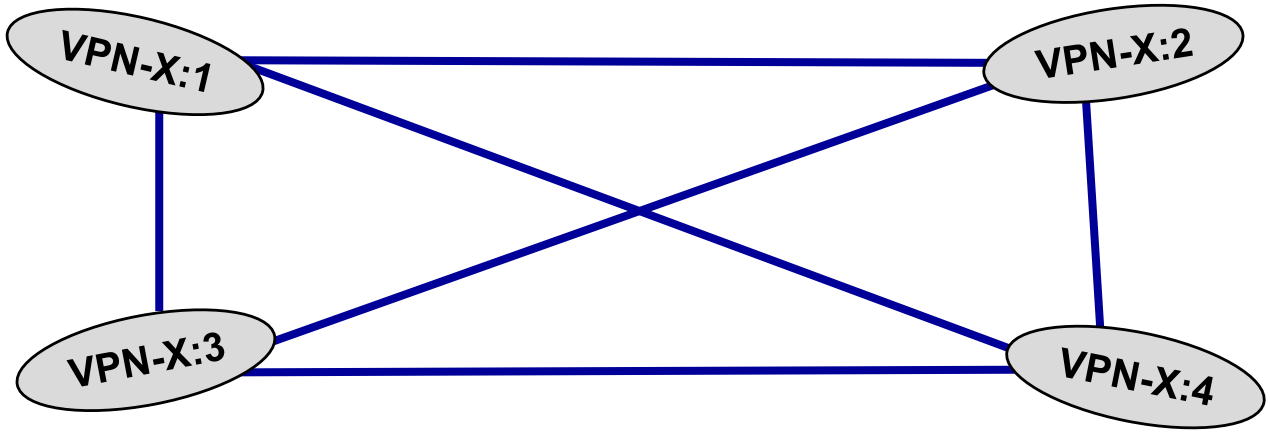
MP-iBGP Overlay specifica della VPN-x (full-MESH)

Accetto tutto

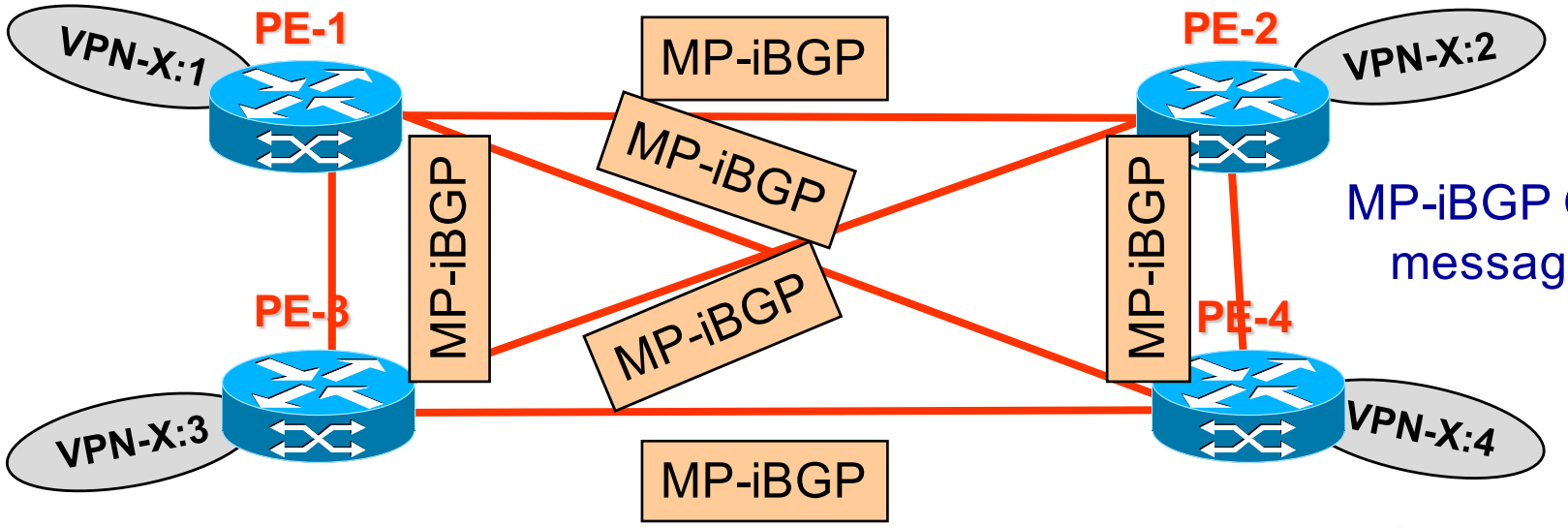
Accetto tutto

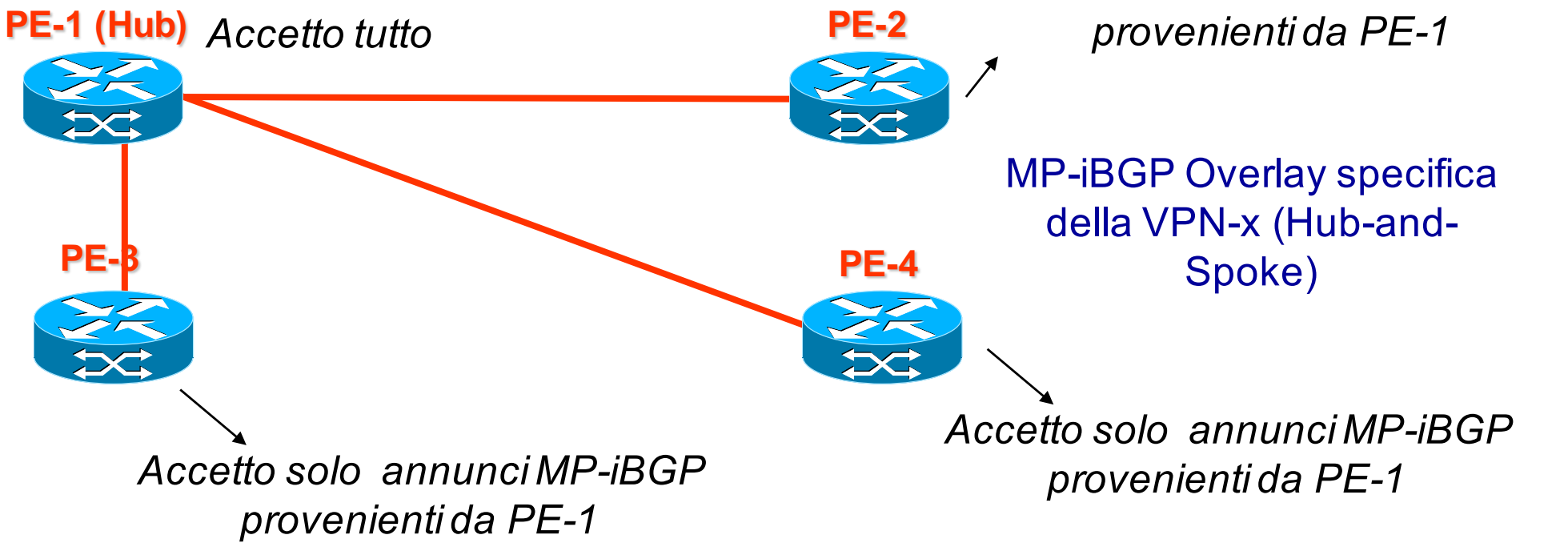
Popolamento delle VRF - VPN Full Mesh

Topologia VPN risultante



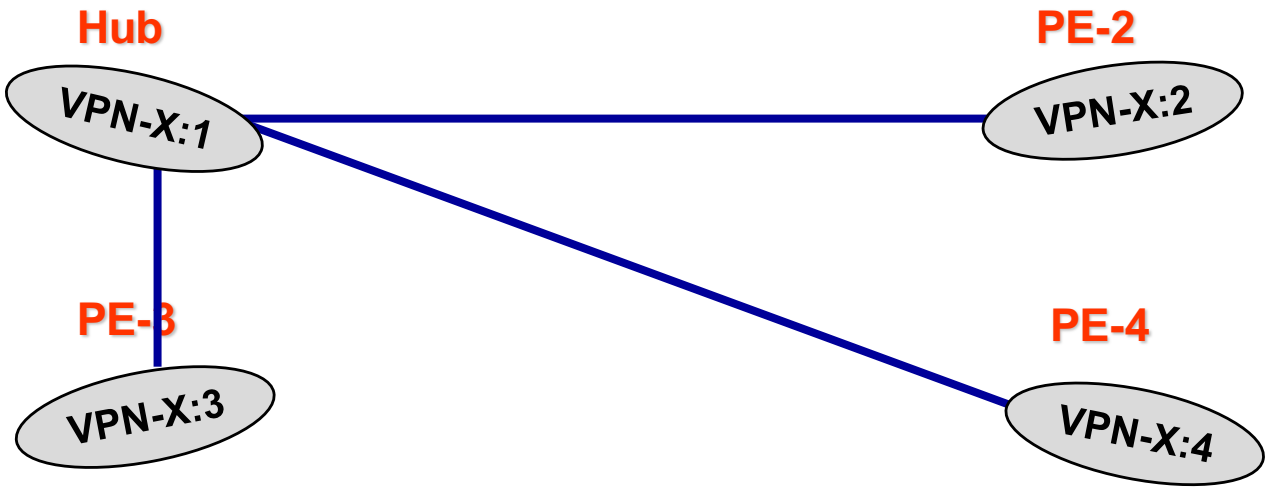
Popolamento delle VRF - VPN Hub and Spoke





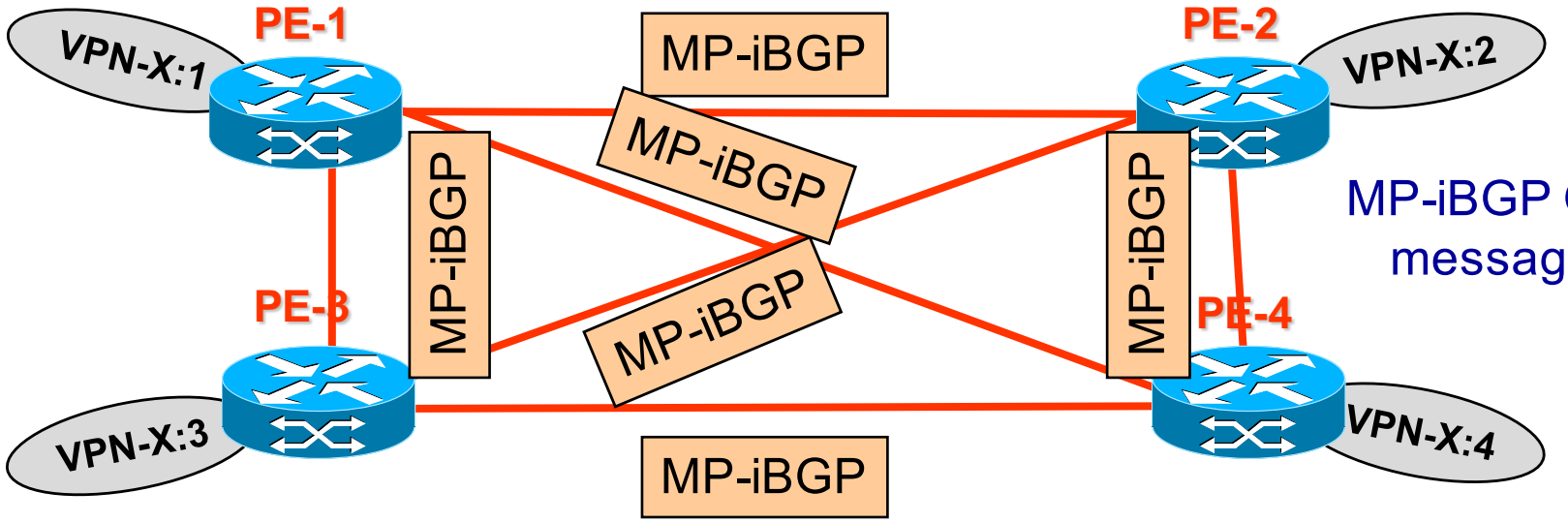
Popolamento delle VRF - VPN Hub and Spoke

Topologia VPN risultante

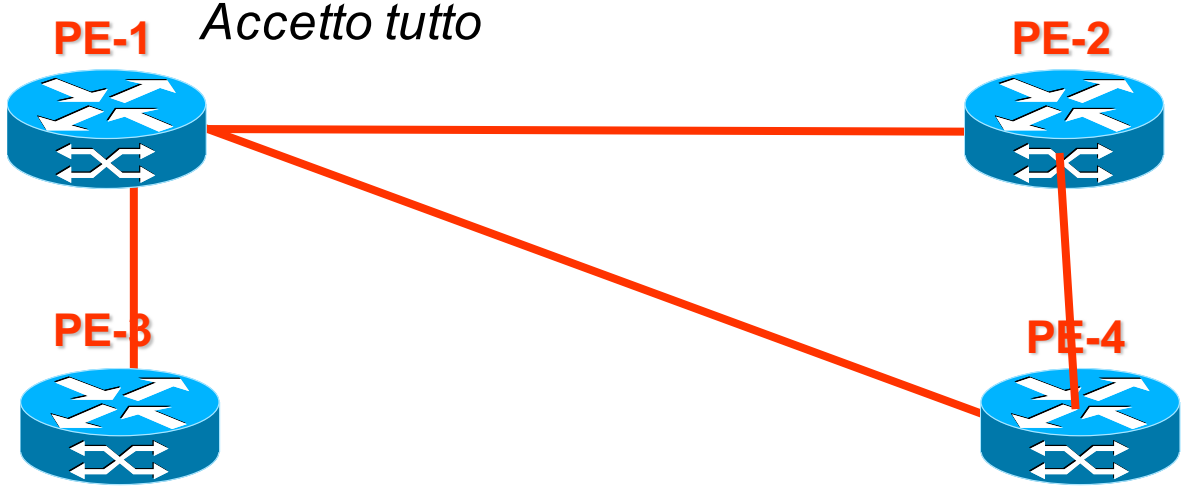


Nota: annunci MP-iBGP (come nnunci iBGP) non si ripropagano su link iBGP. Quindi per permettere agli spoke di comunicare tra loro la VRF dell'hub deve esportare una default

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

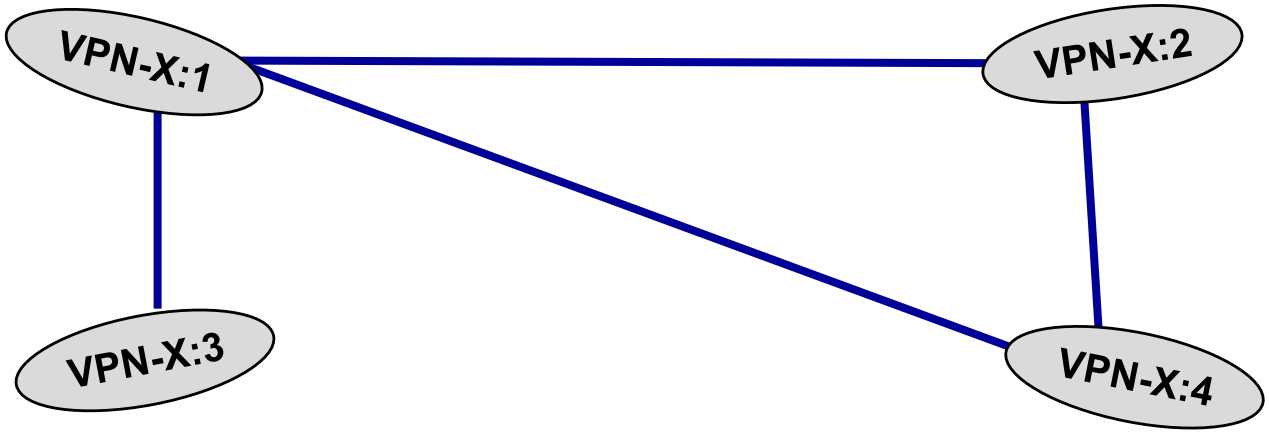
MP-iBGP Overlay specifica della VPN-x (Partial-MESH)

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

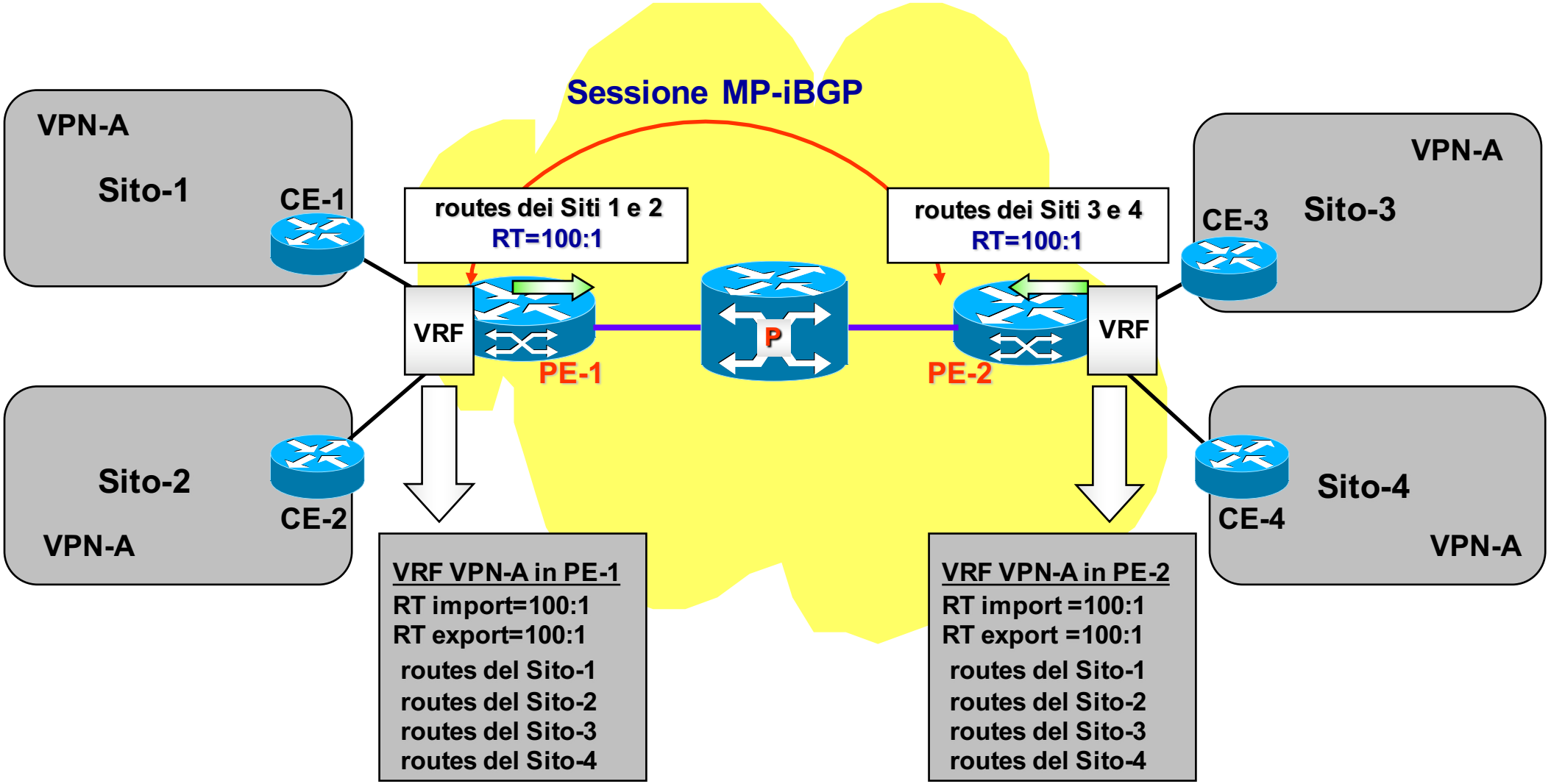


Route Target

- **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**

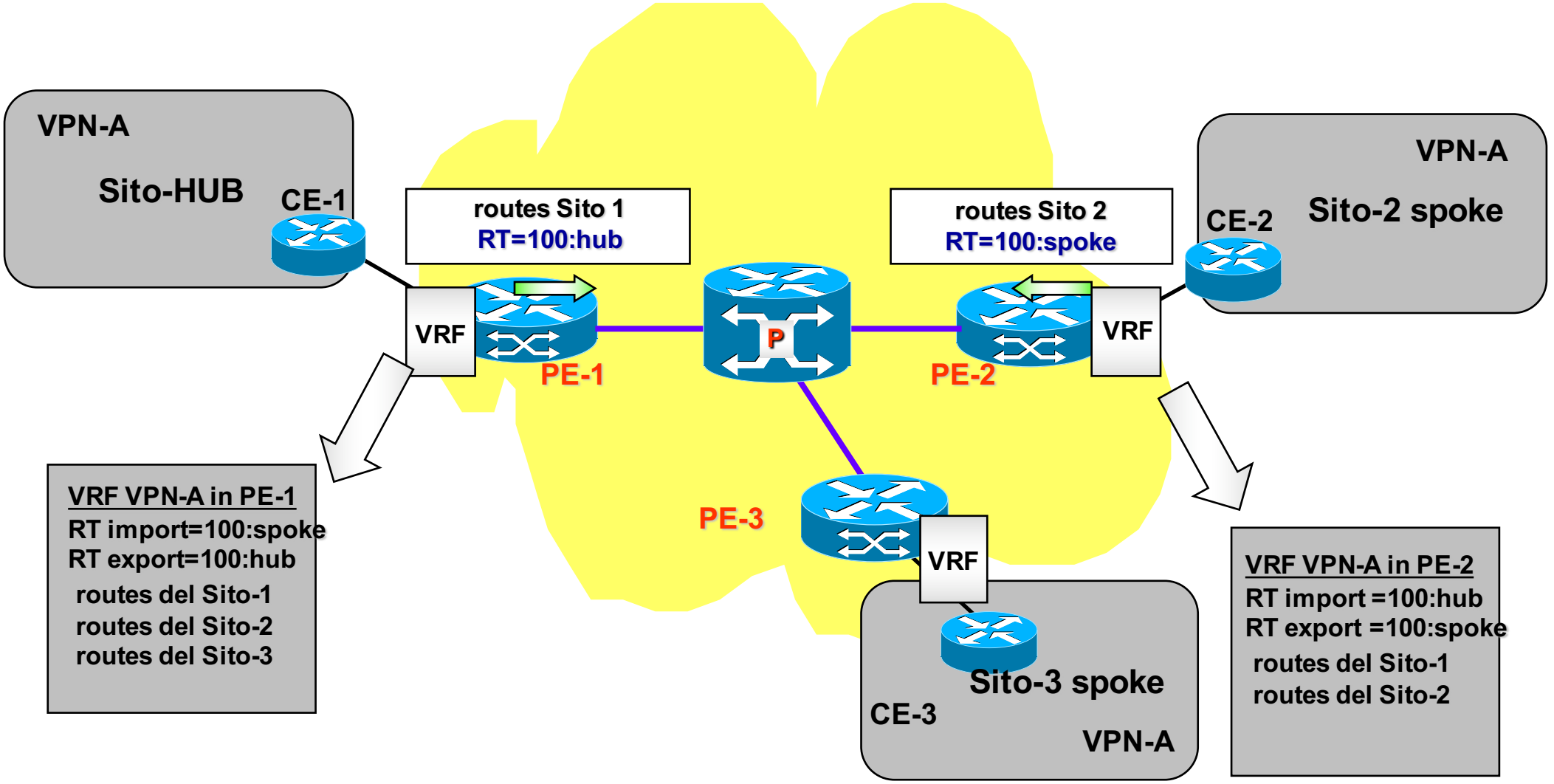
Utilizzo del “Route Target”: Esempio 1

- 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 Loopback0
- 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

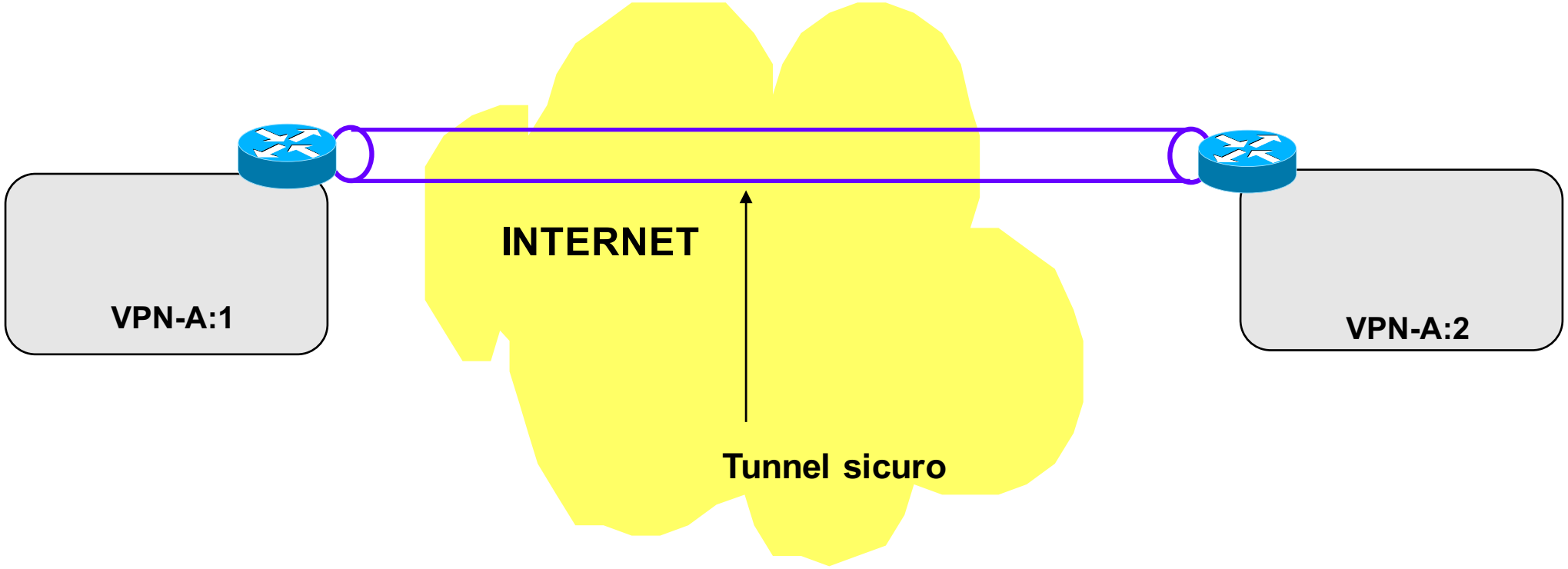
Cisco IOS configuration

- **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**

Overlay VPN

Concetti di base

- Sono VPN realizzate su rete pubblica INTERNET.
- La sicurezza delle comunicazioni deve essere realizzata ent-to-end, in quanto non ci si può fidare di una rete sicura di trasporto (e.s., MPLS)
- Il modello di riferimento prevede la creazione di Tunnel sicuri fra gli end-points della VPN



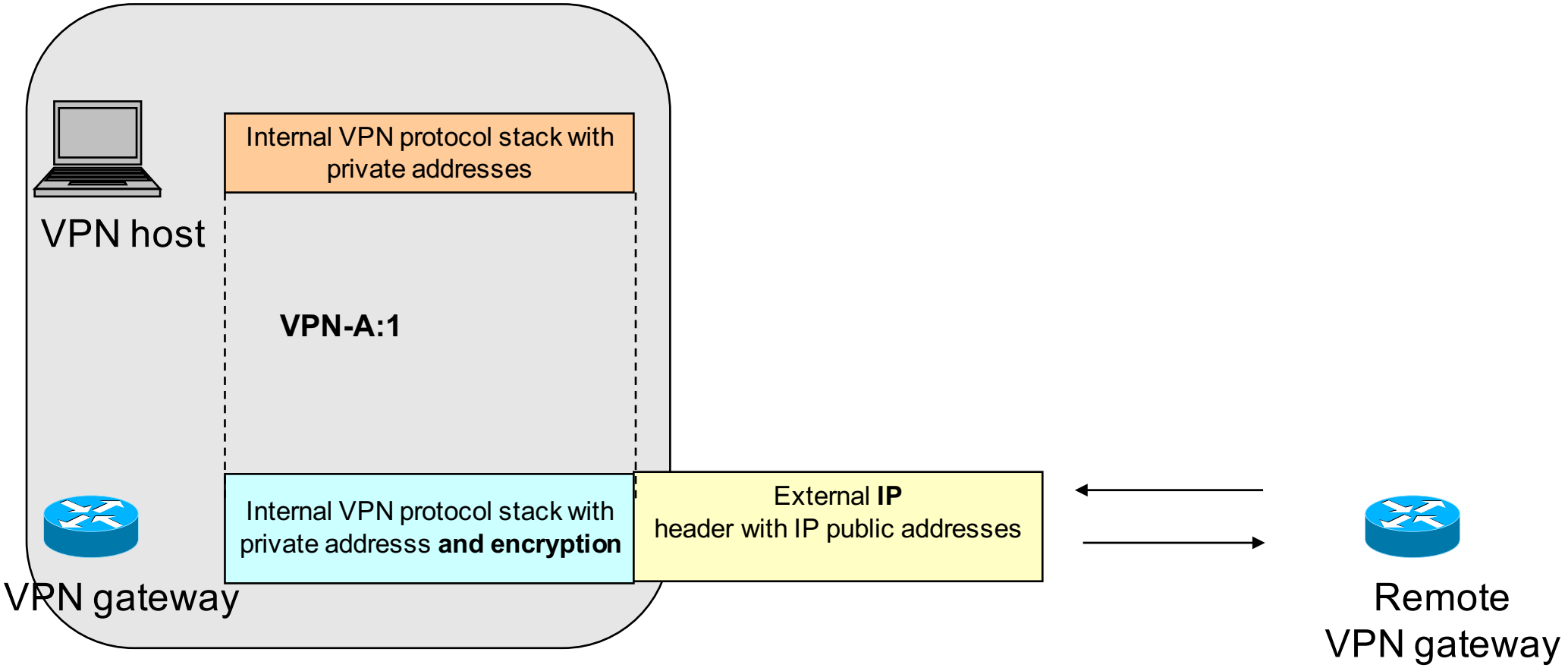
Tunneling

- Il termine tunneling si riferisce a un insieme di tecniche per cui un protocollo viene incapsulato in un protocollo dello stesso livello o di livello superiore per realizzare configurazioni particolari.

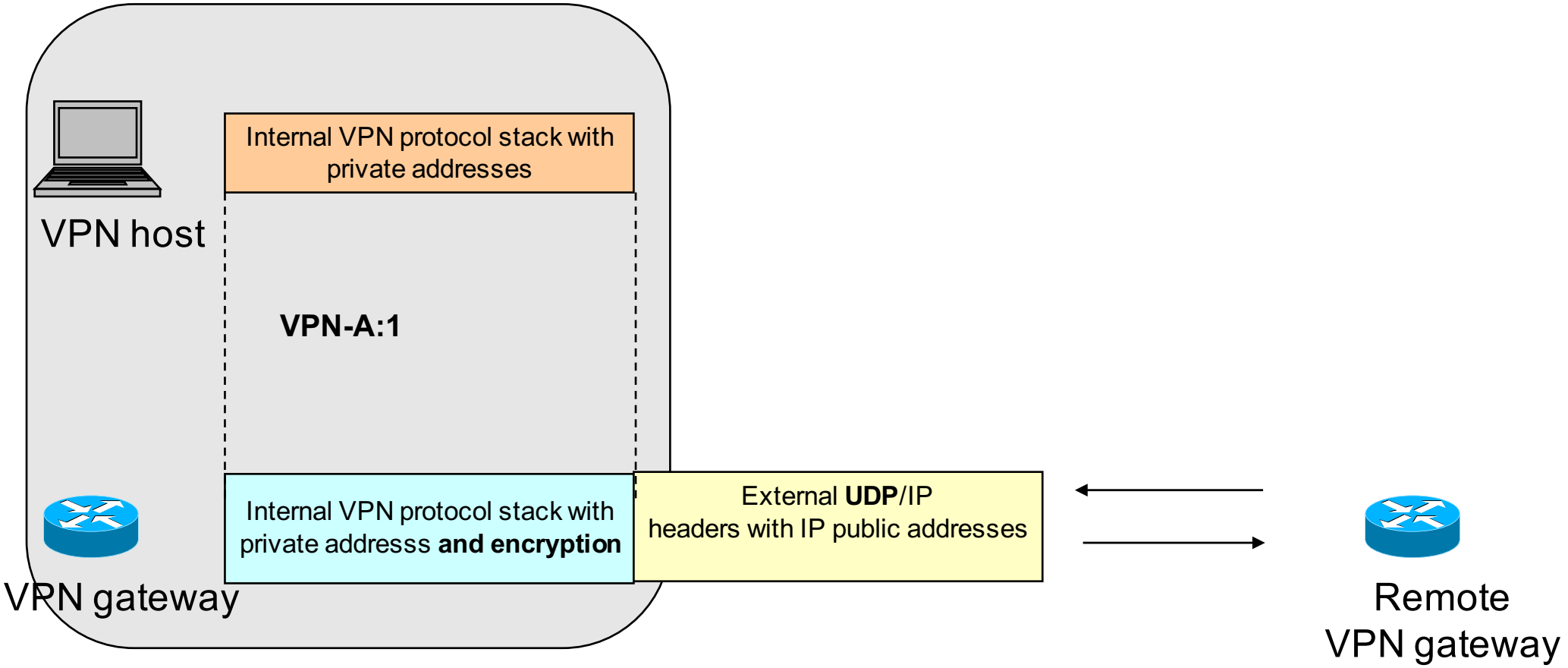
- Le due tipologie di tunnel più importanti sono
  - Tunnel IP
  - Tunnel UDP

- La sicurezza della comunicazione è ottenuta attraverso la cifratura dei dati che sono inseriti all'interno del Tunnel e la autenticazione degli end-point.
  - Sicurezza delle Reti (Prof. Giuseppe Bianchi)

IP tunnel


Internal VPN protocol stack with private addresses
VPN host
VPN-A:1
Internal VPN protocol stack with private addresss **and encryption**
External **IP** header with IP public addresses
VPN gateway
Remote VPN gateway

UDP tunnel

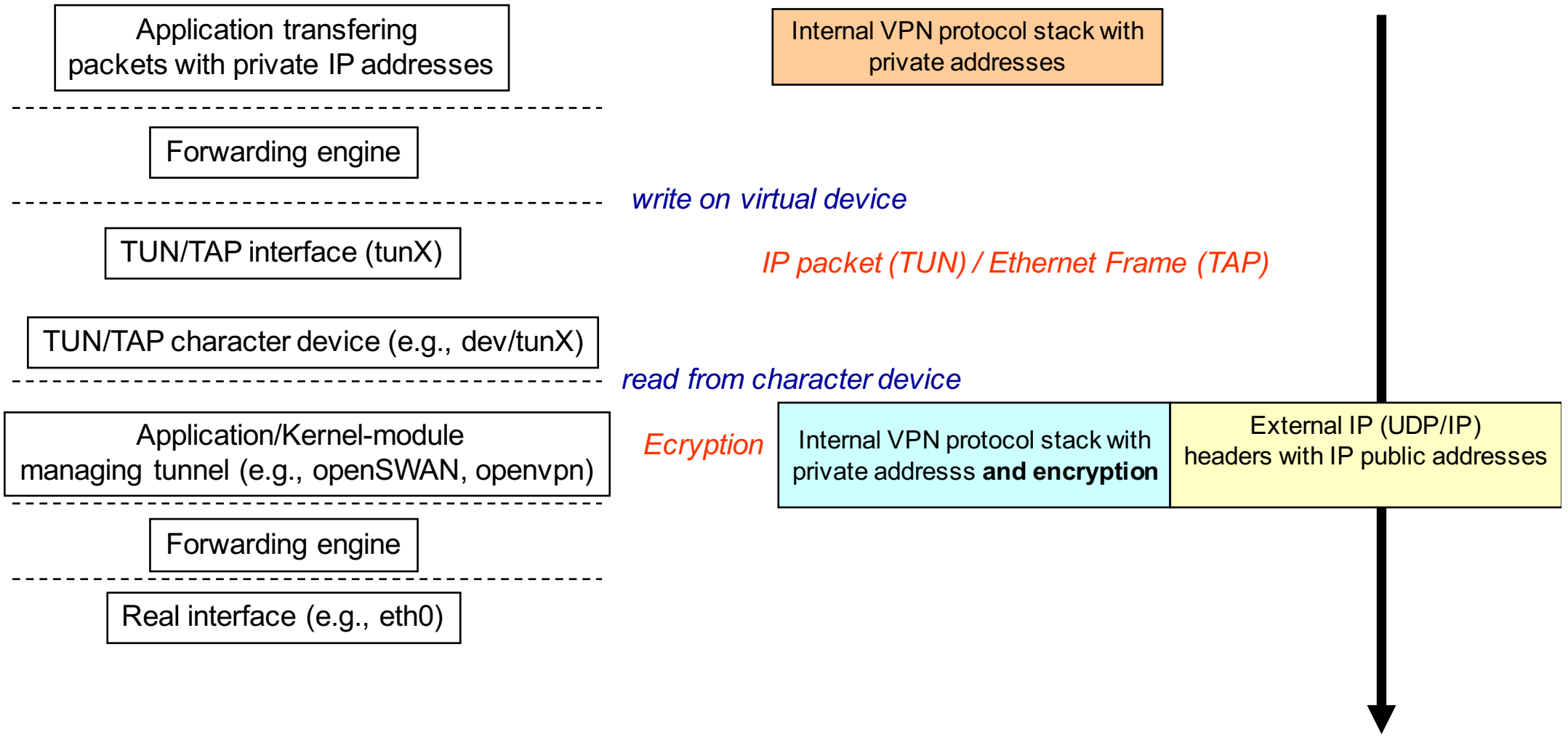

Internal VPN protocol stack with private addresses
VPN host
VPN-A:1
Internal VPN protocol stack with private addresss **and encryption**
External **UDP**/IP headers with IP public addresses
VPN gateway
Remote VPN gateway

Tunnel visibili dal livello applicativo: TUN / TAP driver

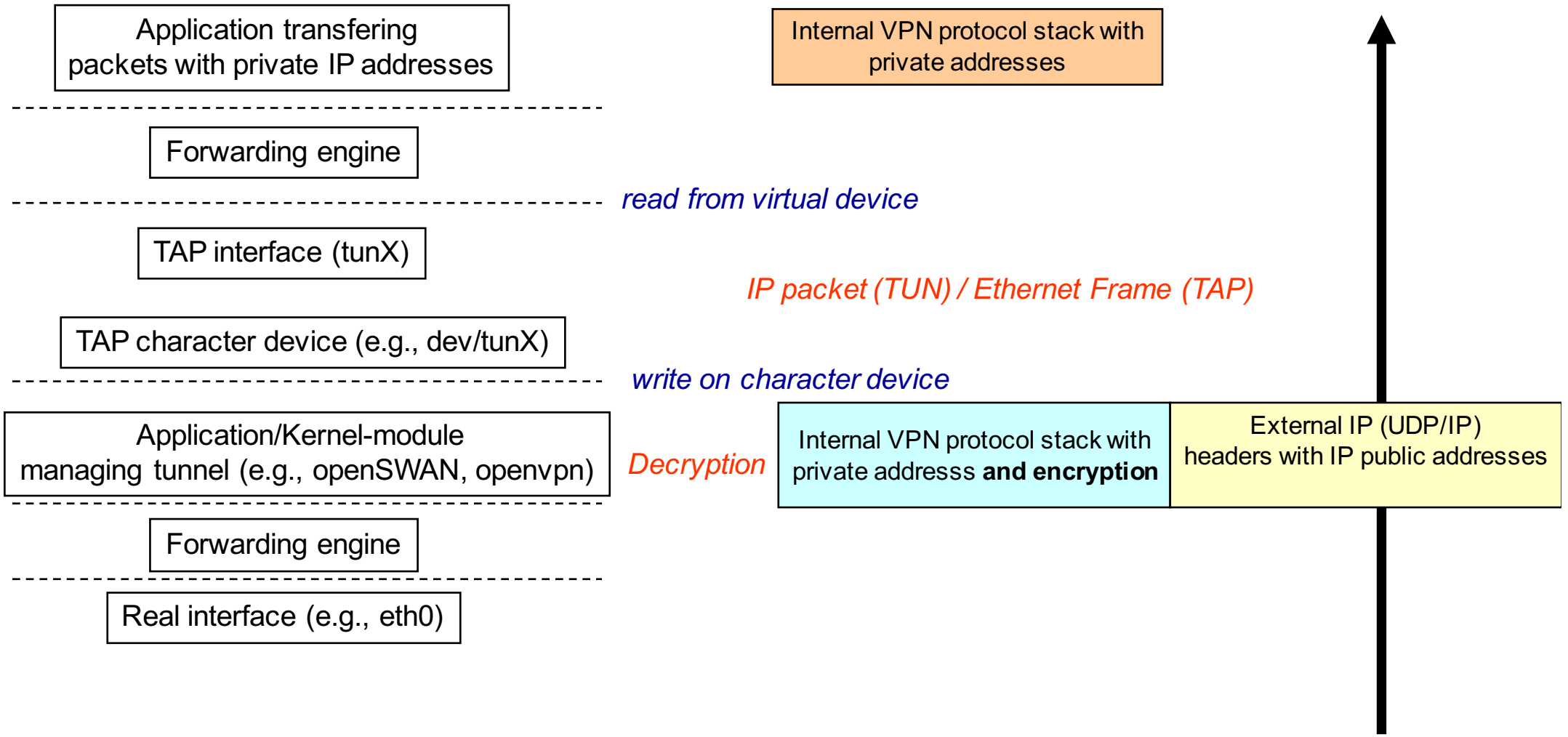
- Un tunnel può essere reso visibile o meno al livello applicativo
- Quando visibile, è spesso presentato come una scheda *virtuale* layer-3 che trasferisce/riceve pacchetti IP (TUN driver) o come una scheda *virtuale* layer-2 (TAP driver) che trasferisce/riceve trame Ethernet
- Con un TUN si trasferiscono pacchetti (Routed VPN)
- Con un TAP si trasferiscono trame Ethernet (Bridged VPN)

- Oltre alla scheda virtuale un TUN/TAP driver può ricevere/trasmettere pacchetti su una zona comune di memoria (*character device*)
- Una applicazione che scrive sul *character device* invoca una *ricezione* sul *device di rete virtuale*
- Una applicazione che scrive sul *device di rete virtuale* invoca una *ricezione* sul *character device*

Trasferimento di un pacchetto via TUN/TAP driver



Ricezione di un pacchetto via TUN/TAP driver



User-space VPN

Overlay VPN

User-space VPN

- Sono VPN i cui link sono dei tunnel UDP o TCP gestiti da uno specifico tool di livello applicativo
- La sicurezza su questi tunnel è garantita da (Datagram) Transport Layer Security TLS (DTLS)
- Si chiamano user-space VPN poichè sono basate sui socket che sono controllabili dallo user-space
- UDP vs TCP tunnel: UDP
  - Il tunnel deve transportare lo stack protocollare TCP-UDP/IP
  - questo stack è stato ottimizzato per un trasporto diretto su una rete non *reliable*, quale quella Internet. Pertanto, fare un tunnel UDP (i.e., unreliable) è preferibile in quanto il tunnel ha le stesse proprietà di un trasporto diretto su Internet, a parte un overhead addizionale.

User-space VPN – Packet handling

- I pacchetti IP (Ethernet) trasferiti dall'applicazione su una scheda virtuale TUN/TAP sono trattati dal tool che gestisce la "*user-space VPN*" (e.g., openvpn)
- Alla ricezione di un pacchetto proveniente da una applicazione locale, il tool *user-space VPN* controlla l'indirizzo IP di destinazione e decide su quale socket UDP (TCP) incapsulare il pachetto cifrato
- Pertanto il tool *user-space VPN* possiede una sua tabella di routing (overlay) svincolata dalla tabella di routing dell'OS

- Le entry di questa tabella *overlay* sono del tipo
  <netid, mask, public_ip_da, udp_port>

- Il tool *user-space VPN* remoto decifra, autentica e decapsula i pacchetti IP (Ethernet) entranti e li inietta (in su) sul TUN/TAP driver (i.e., scrive sul TUN/TAP character device)
- Il forwarding dello OS provvederà alle successive operazioni di forwarding intra-VPN

Routed o Bridged VPN ?

- **Quale stack protocollare è trasportato dal tunnel ?**
- ***Bridged VPN:* tap driver che trasporta trame ethernet**
  - » **Per gli host connessi alla VPN, la VPN è un dominio Ethernet, pertanto si può parlare di una *Virtual wide-area LAN***
  - » **Il traffico Broadcasts si trasmette sulla VPN – questo permette il funzionamento di software che dipendono da una LAN sottostante (e.s., Windows NetBIOS file sharing and network neighborhood browsing).**
  - » **Nessun routing da configurare**
  - » **Problema: su reti molto grandi, il trasferimento del Broadcast pone dei seri limiti alla scalabilità.**
- ***Routed VPN*: tun driver che trasporta pacchetti IP**
  - » **Ogni collegamento è una subnet ip diversa → no broadcast traversal**

Cenni di TLS

User-space VPN

Public Key Cryptography

Bob

Bob's Public Key

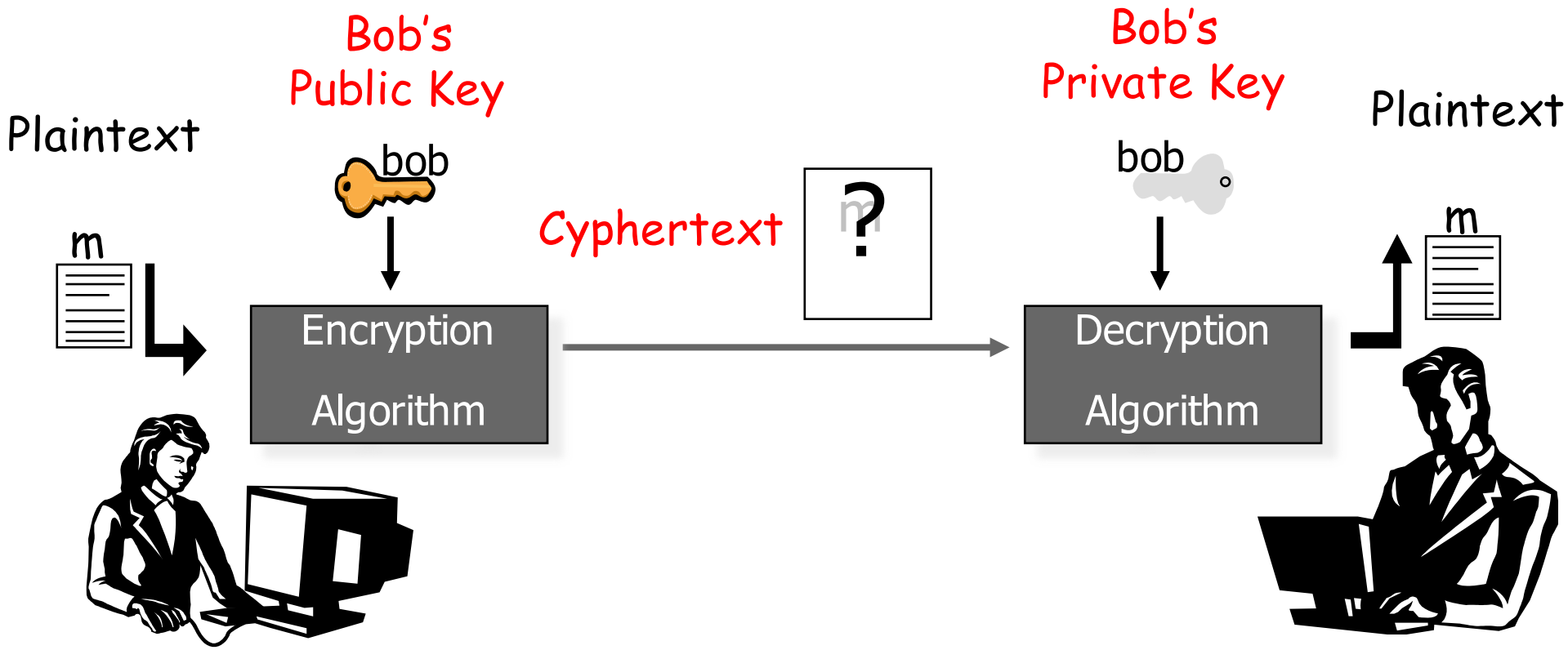
Bob's Private Key

Alice

Bob's Public Key

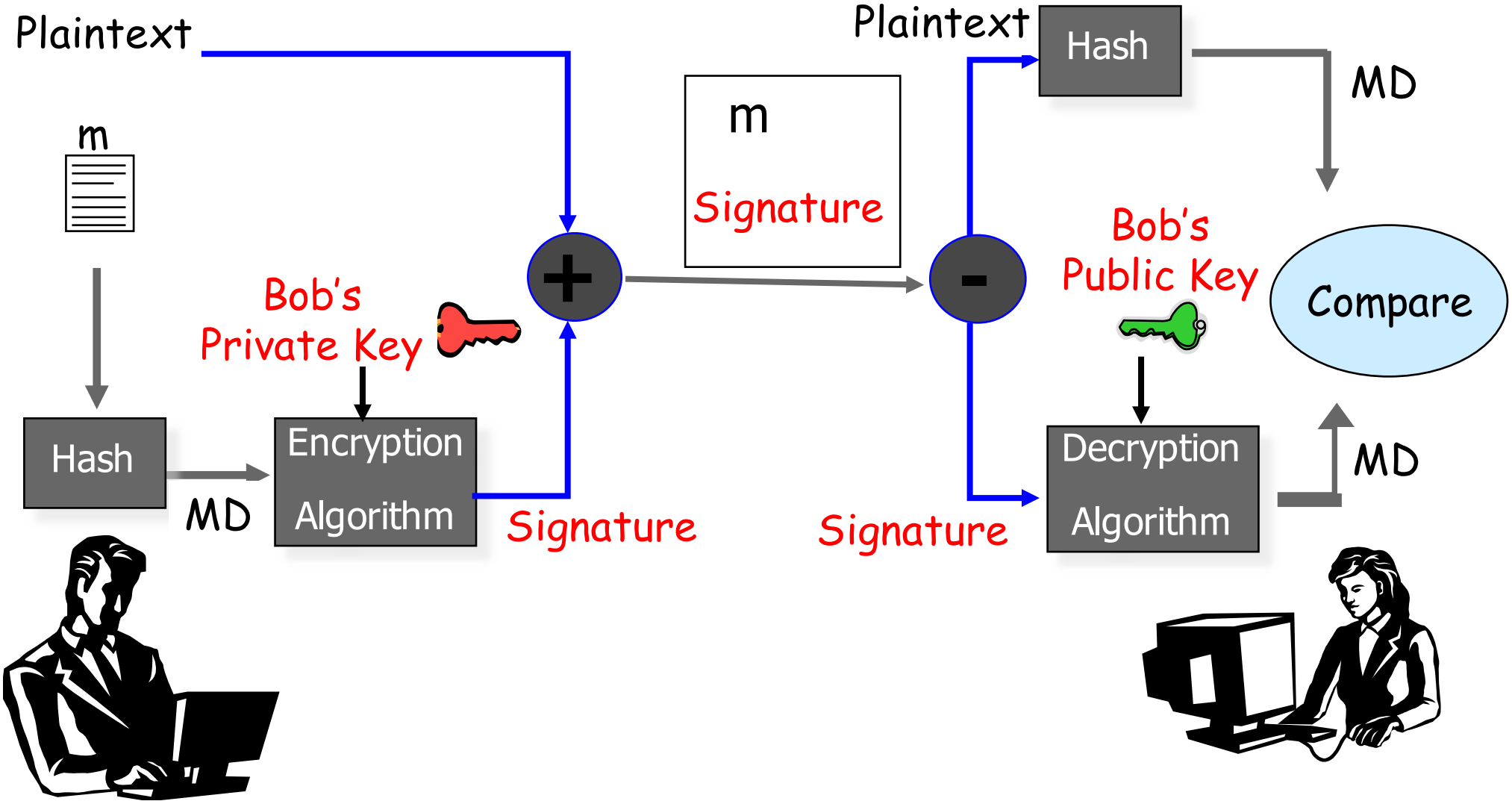
Public Key Cryptography

Confidentiality

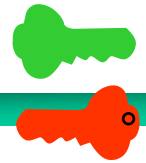


Public Key Cryptography

Authentication & Message Integrity Check



PK Cryptography: Digital Certificate



Come può Alice essere sicura che la Bob's public key è autentica?

Certificate Authority Center

Bob Info:

- Name
- Department
- Cubical Number

Certificate Info:

- Expiration Date
- Serial Number

Bob's Public Key

Sign data

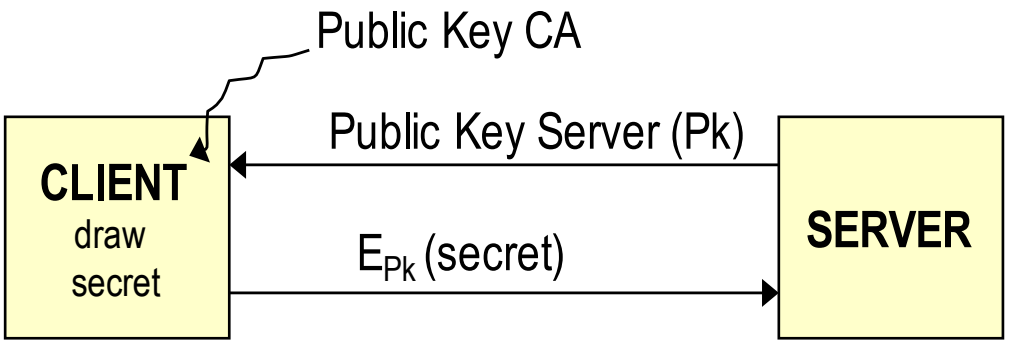
CA's Private Key

Transport Layer Security

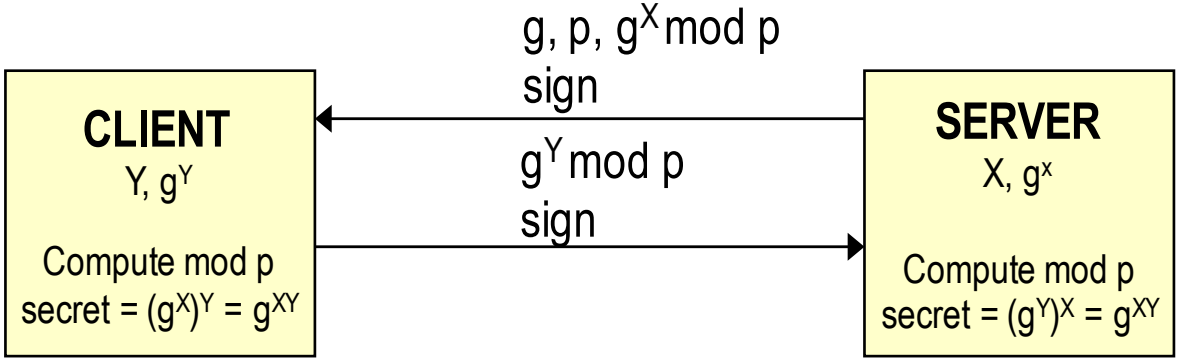
- Gestisce la comunicazione sicura tra un client ed un server
- Problema: l'uso di una chiave asimmetrica durante uno scambio informativo ad elevato bit/rate può creare un collo di bottiglia sul processing
- Approccio risolutivo utilizzo dei meccanismi a chiave asimmetrica per configurare una chiave simmetrica su entrambi i lati
  - » Key transport (e.g. RSA)
  - » Key agreement (e.g., Diffie-Hellman)

The two basic approaches to key management

- **Key transport (e.g., RSA)**
  - » **Il client genera una chiave random (Secret)**
  - » **La chiave è trasferita al server cifrandola con la chiave pubblica del server**



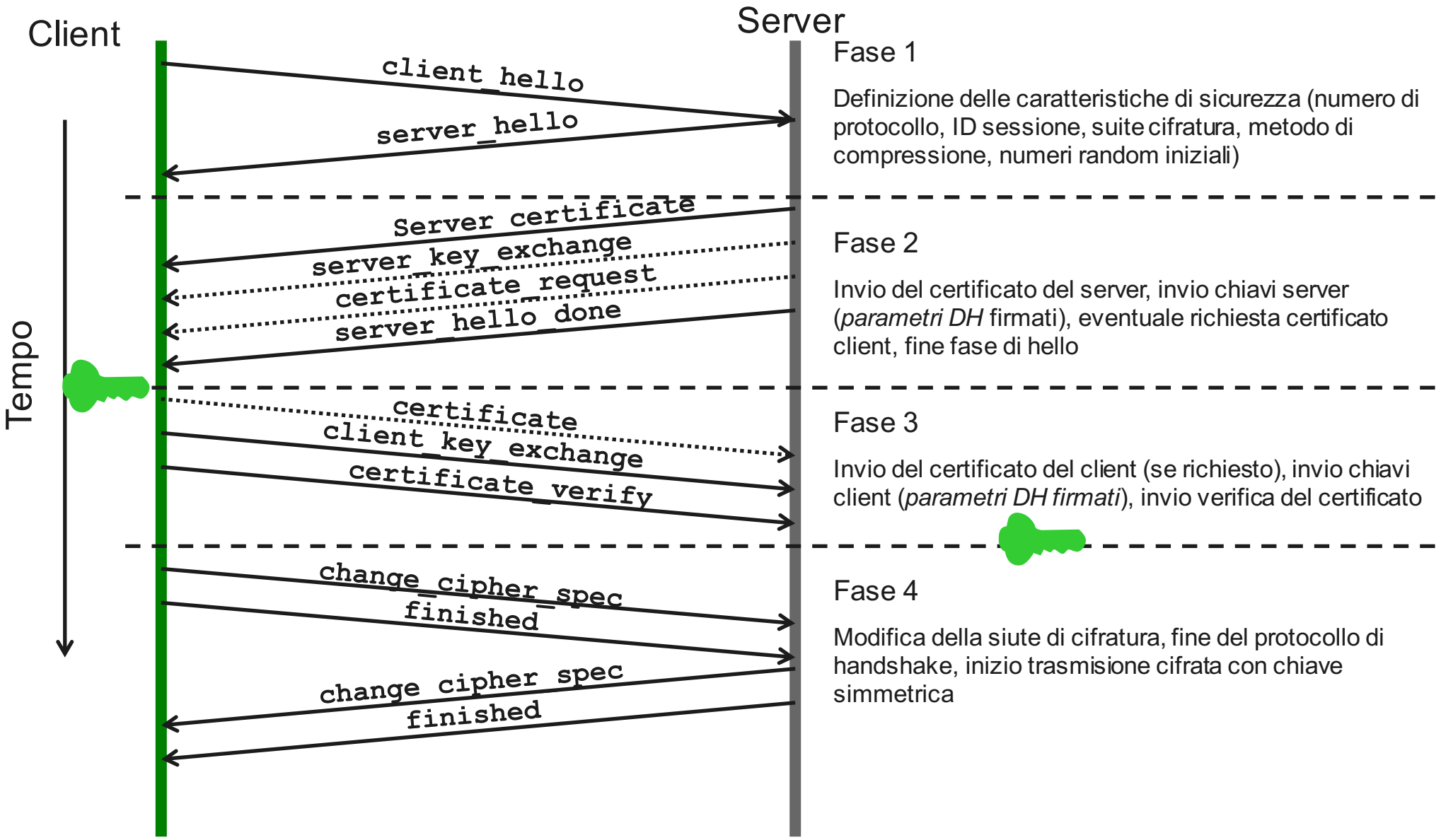
- **Key agreement (e.g., DH Ephermal)**
  - » **Segreto condiviso calcolato da entrambe le parti attraverso lo scambio opportuno di parametri crittografici**



Transport Layer Security (E-DH)

- **TLS / Ephermal Diffie-Hellman :**
  - **Si instaura una connessione sicura tra le parti**
  - **Nella fase di instaurazione, le parti si scambiano i loro certificati, firmati da una CA affidabile in modo che possano autenticarsi a vicenda**
  - **Inoltre, sempre nella fase di instaurazione, le parti si scambiano alcuni parametri (*firmati*) che permettono di decidere quale sia la chiave di cifratura simmetrica da utilizzare durante il successivo trasferimento dati (Ephermal Diffie-Hellman parameters)**
  - **L'intercettazione dei Diffie-Hellman parameters che transitano in rete non permette ad un ascoltatore intruso di capire quale sarà la chiave simmetrica che sarà adottata**
  - **La *firma* su questi Diffie-Hellman parameters assicura le parti che chi sta trasmettendo è effettivamente chi si dichiara di essere**

TLS Handshake (E-DH)



TLS cosa serve e dove (E-DH)

Client1

Certificato client1 firmato dalla CA: è la carta d'identità da trasferire per farsi riconoscere; contiene la chiave pubblica di *client1*

Certificato della CA: contiene la chiave pubblica della CA *con la quale posso validare i certificati che ricevo*

Chiave privata client1 (secret)

Server

Certificato server firmato dalla CA: è la carta d'identità da trasferire per farsi riconoscere; contiene la chiave pubblica del server

Certificato della CA: contiene la chiave pubblica della CA *con la quale posso validare i certificati che ricevo*

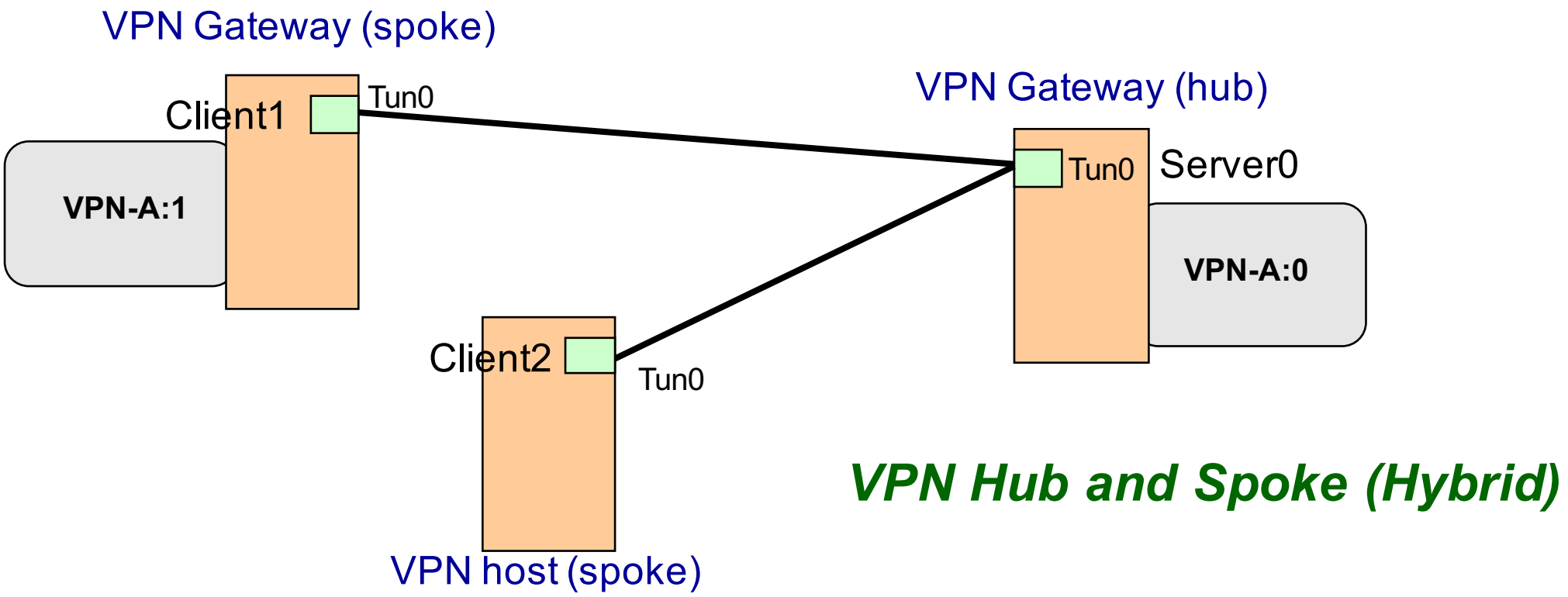
Chiave privata server (secret)

Parametri iniziali Diffie-Hellman

Nel caso in cui non si intende autenticare in client via TLS, il client ha solo bisogno del certificato della CA (*oppure accetta di non verificare la validità dei certificati del server*)

Topologie delle User-Space VPN

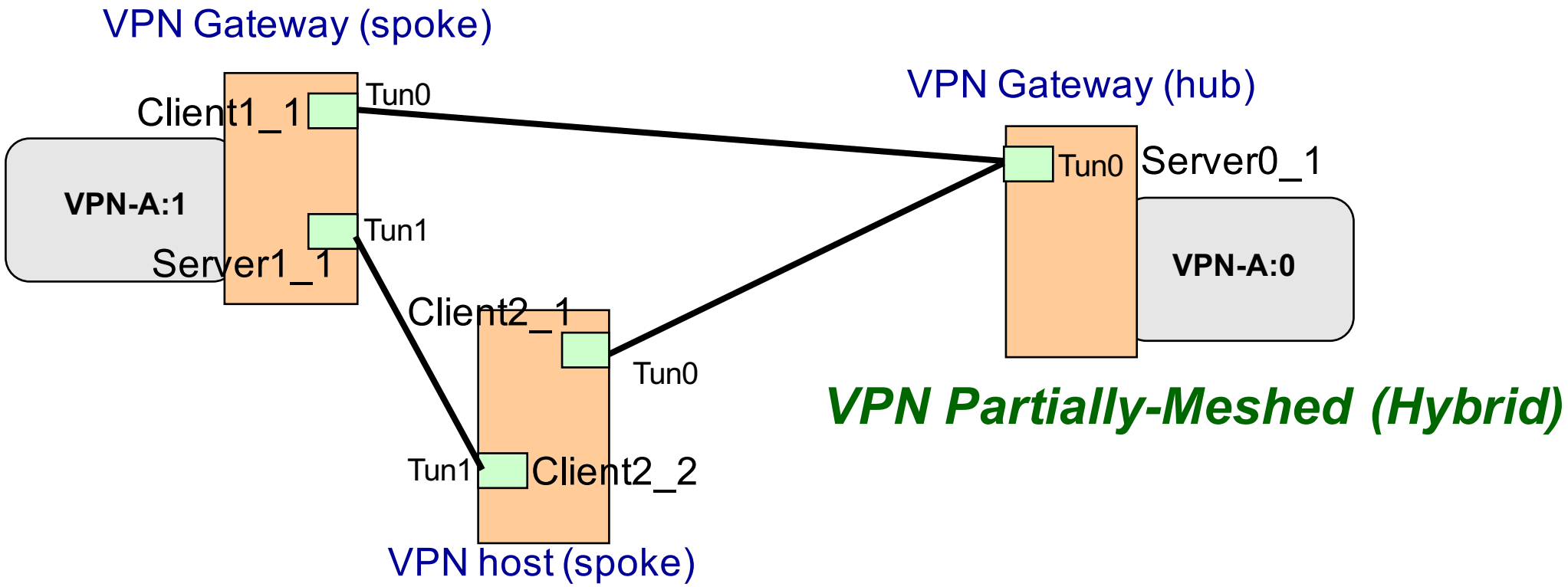
- **Essendo basate su socket, sono conformi al paradigma client-server.**
- **Pertanto, la topologia nativa di questo tipo di VPN è Hub-and-Spoke dove l'Hub è il server e gli spokes sono i client**
- **Il client ed il server possono girare sia host, che gateway**
  - » **Host-to-Host VPN: VPN overlay in cui i tunnel terminano su host**
  - » **Gateway-to-Gateway VPN overlay i cui tunnel terminano su gatevay di reti private (unica tipologia offerta da MPLS MB-iBGP)**
  - » **Hybrid: soluzione ibrida; e.s. host mobile che si connette alla LAN aziendale via VPN gaeway**



VPN Hub and Spoke (Hybrid)

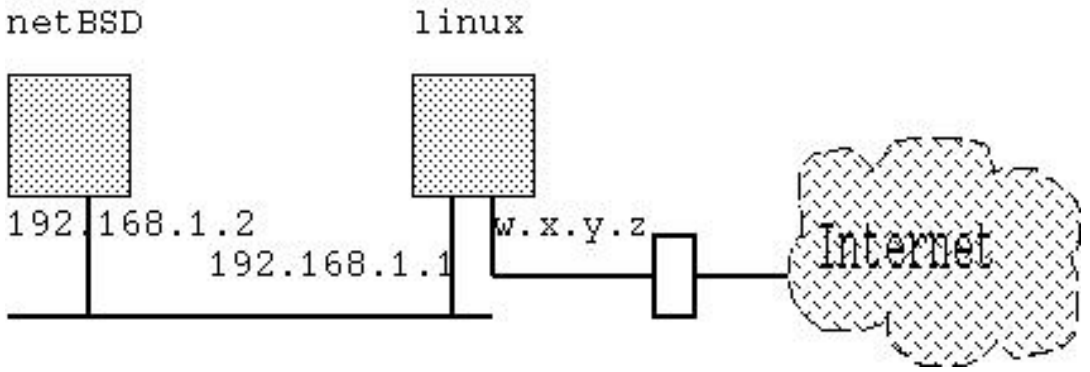
Topologie delle User-Space VPN

- **Topologie meshed richiedono combinazioni client-server e/o più clients sulla stessa macchina**
- **Inoltre, richiedono una buona cura della configurazione delle tabelle di instardamento IP / overlay**



User-space VPN vs NAT e Dynamic IP

- **Molto spesso un piccolo ufficio o una abitazione sono connessi ad Internet attraverso un gateway ADSL che ottiene un indirizzo pubblico IP dinamico, assegnato dall'ISP alla connessione fisica.**
- **Per far accedere ad Internet gli hosts interni dietro al gateway, sul gateway è abilitata la funzionalità di Network (and port) Address Translation (NAT o NAPT)**



- **Basic NAT**
  - » **192.168.1.2 → w.x.y.z**
- **NAPT**
  - » **192.168.1.2, Source Port A →w.x.y.z, Source Port B**

User-space VPN vs NAT e Dynamic IP

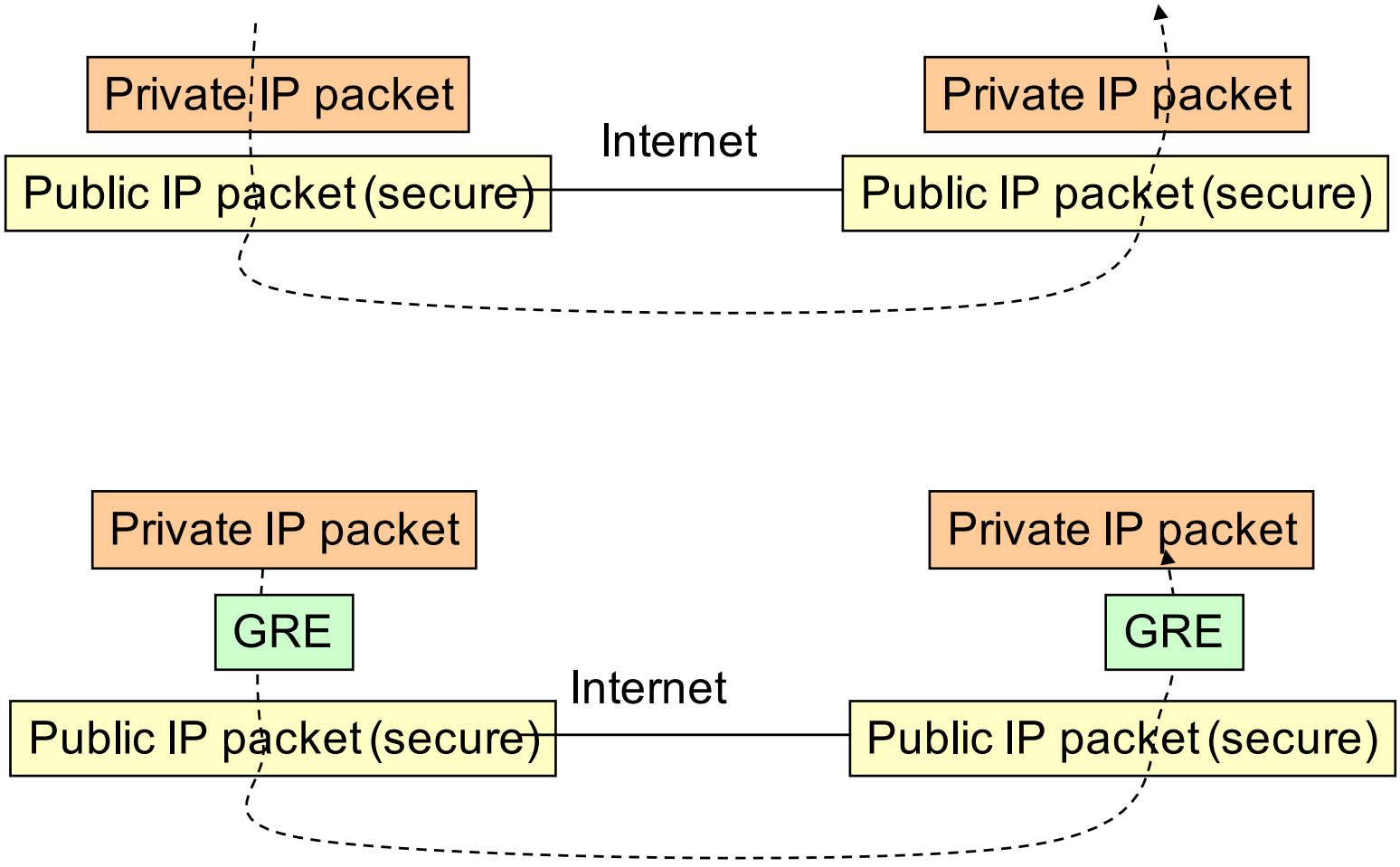
- **Client VPN dietro NAT: nessun problema poiché i tunnel sono basati su socket che interlavorano perfettamente con il NAT del gateway**
- **Server VPN dietro NAT:**
  - **I client VPN necessitano di raggiungere il server. Pertanto i server deve essere raggiungibile attraverso un indirizzo IP pubblico noto ai client**
  - **Per far ciò, il gateway ADSL deve avere anche un indirizzo mnemonico (e.s., srdserver.it) ottenibile da un gestore di *dynamic DNS address* (e.s., www.dyndns.com) e registra sul server DNS l'indirizzo IP pubblico associato all'indirizzo mnemonico ogni volta che l'IP address cambia**
  - **Il gateway del server deve essere configurato in modo da effettuare il port forwarding della porta TCP/UDP del server VPN sull'host che ospita il server VPN**
  - **Il client VPN, nella sua configurazione, ha come indirizzo del server l'indirizzo mnemonico piuttosto che quello IP.**

IPsec VPN

Overlay VPN

IPsec VPN

- **Sono VPN realizzate mediante tunnel i) IP over IP oppure ii) IP over GRE over IP**



IPsec VPN

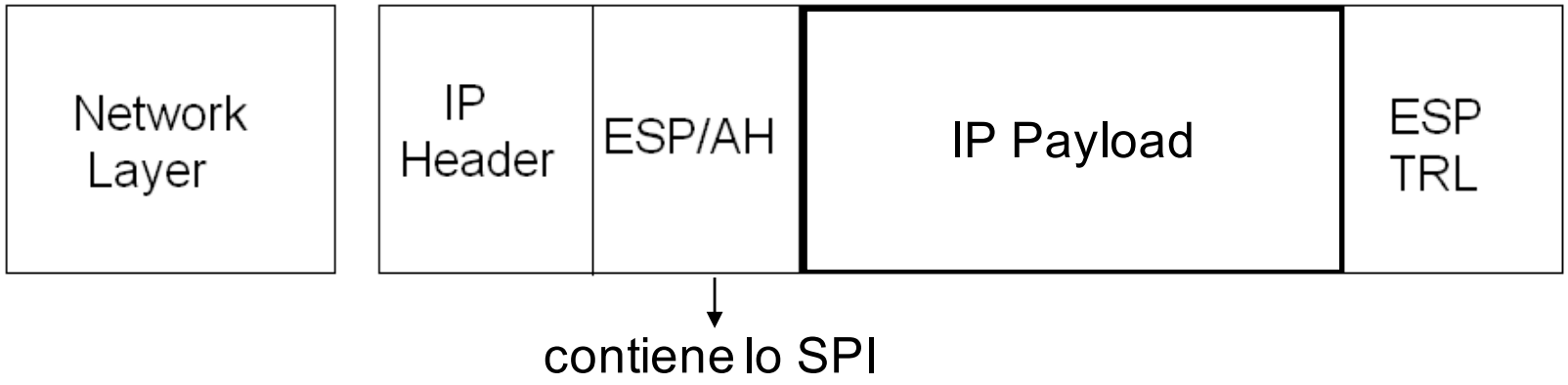
- La sicurezza è affidata ad IPsec: protocol suite che implementa la crittografia a livello di network layer per fornire servizi di autenticazione e confidenzialità tra host che comunicano attraverso una untrusted network consentendo la creazione di VPN

- Su Linux (Windows) è implementata a livello Kernel
  - » No tun/tap virtual interface
  - » Solitamente il modulo IP sec si interpone fra IP ed il driver della scheda: fisica,
    - » (senza IPSec) IP→Ethernet;
    - » (con IPSec) IP→IPSec→Ethernet
  - » VPN non visibile da livello utente

- Due modalità di incapsulamento dati: Transport mode , Tunnel mode

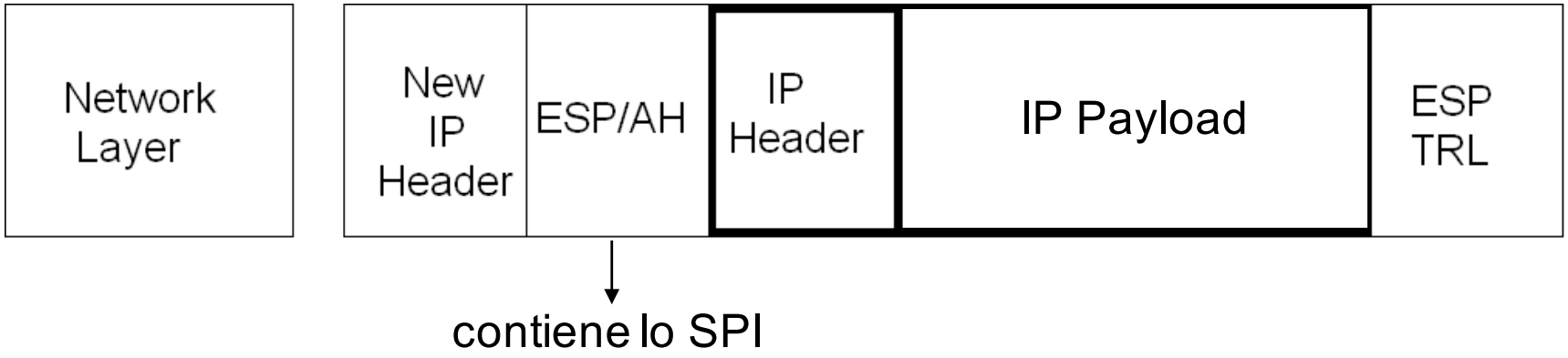
Transport mode

- **E' messo in sicurezza solo il payload del pacchetto**
- **Due protocolli di sicurezza:**
  - **Authentication Header (AH): garantisce autenticità ed integrità di tutto il messaggio**
  - **Encapsulating Security Payload (ESP): garantisce autenticità, integrità e confidenzialità (encryption) solo del payload del messaggio**
  - Solitamente si usa ESP e raramente ESP ed AH possono essere utilizzati insieme
- **Attraversando lo stack TCP/IP verso il basso a livello di network layer IPsec rimuove l'header IP originale, cripta (solo con ESP) i dati realtivi ai layer OSI più alti, aggiunge in testa il security header selezionato (ESP/AH) e riapplica l'header IP originale.**
- **Tipica soluzione per una comunicazione sicura fra due host (*host-to-host VPN*) che hanno indirizzo IP pubblico, infatti non si crea un tunnel su cui poter trasferire pacchetti IP con indirizzi privati**
- **Utilizzando GRE, invece, può essere anche utilizzato per creare una VPN…**

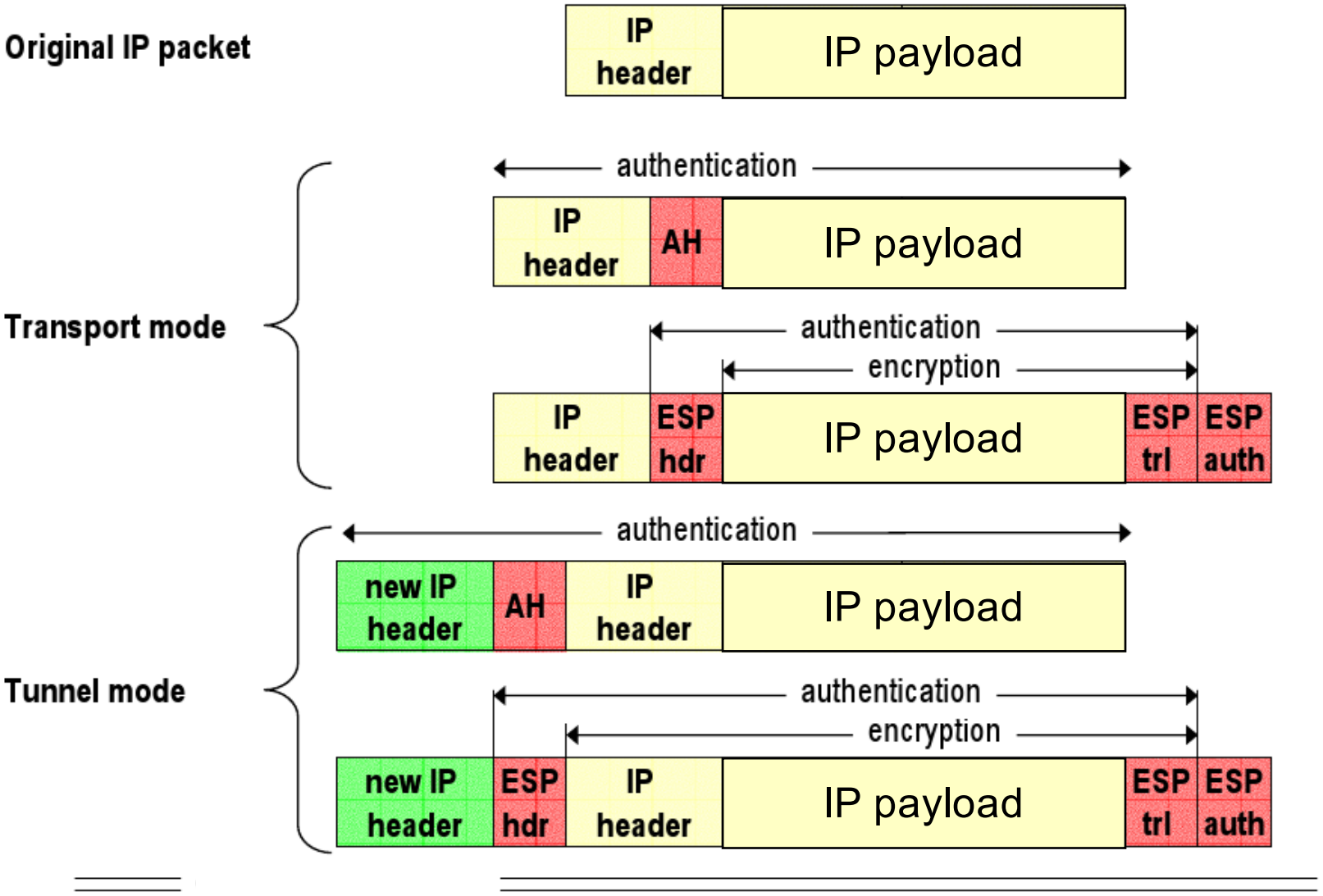


Tunnel mode

- **E' messo in sicurezza tutto il pacchetto IP**
- **L'intero pacchetto originario viene incapsulato e criptato (solo ESP) e vengono aggiunti in testa un nuovo Header IP e l'authentication protocol header (ESP/AH).**
- **Tipica soluzione per una comunicazione sicura fra Reti Private (i.e., gateway-to-gateway VPN) che hanno gateway pubblici, infatti si crea un tunnel fra i gateway su cui poter trasferire pacchetti IP privati**



Transport vs Tunnel – AH and ESP



Elementi fondamentali di IPsec

- **SA: Security Association. Sta alla base di una VPN IPsec. È un set di proprietà relative alla connessione tra 2 host, è una sorta di tabella che descrive le proprietà specifiche di una VPN IPsec. In altre parole definisce il "come" realizzare una comunicazione sicura tra due devices**
  - **SPI: Security Parameter Index. Numero che identifica la SA in modo univoco su entrambe gli end-devices**
  - **AH parameters**
  - **ESP parameters**
  - **Indirizzo IP pubblico sorgente (local device)**
  - **Indirizzo IP pubblico destinazione (remote device)**
  - **Modalità di incapsulamento (transport/tunnel)**
- **SAD: Security Association Database. Database delle SA attive su un device.**

Elementi fondamentali di IPsec

- **SP: Security Policy. è una regola che dice al modulo/driver IPsec "chi" (i.e., quali flussi di dati) deve essere trattato da una specifica SA**
  - **Net_id/mask sorgente (in transport mode è solo un indirizzo IP sorgente)**
  - **Net_id/mask destinazione (in tunnel mode è solo un indirizzo IP destinazione)**
  - **Porta sorgente / destinazione**
  - **Direzione (in out)**
  - **Azione da intraprendere (ipsec/discard/none)**
  - **Protocollo di sicurezza (ah/esp/ipcomp)**
  - **Modalità di incapsulamento (transport/tunnel)**
  - **IP sorgente e destinazione del tunnel (solo tunnel mode)**

- **Le SP/SA hanno attualmente dei problemi con indirizzi Multicast/Broadcast, ovvero IPSec non gestisce nativamente il routing multicast**

- **SPD: Security Policy Database. Database delle SP attive su un device.**

Processing IPSec

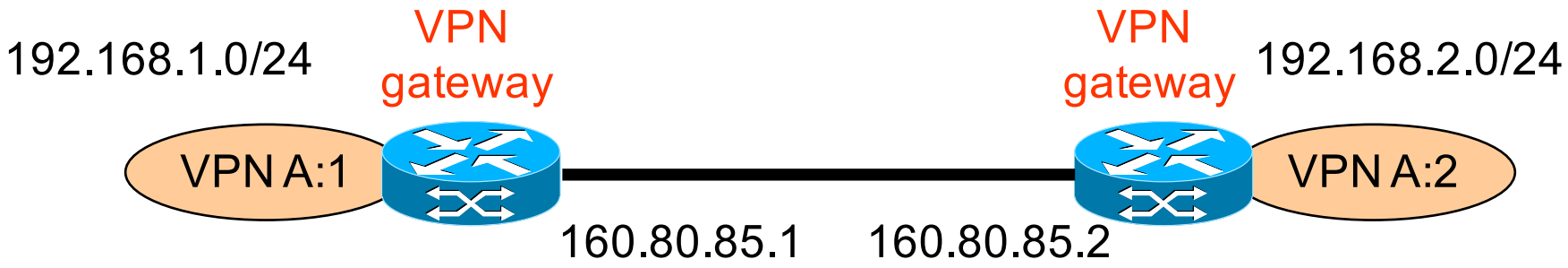
- Alla ricezione di un pacchetto in uscita, il gateway controlla se questo verifica qualche SP all'interno dello SPD
- Se un SP è verificata, allora il gateway esegue le operazioni di sicurezza definite dalla SP (e.s., tunnel mode con ESP) in accordo ai parametri definiti dalla SA (e.s., chiave di cifratura ESP, SPI, etc)

- Alla ricezione del pacchetto in entrata, si usa SPI per identificare la SA e si ottinene il pacchetto «in chiaro»
- Quindi il gateway controlla se questo è associato qualche SP all'interno dello SPD
- Se una SP è trovata, verifica che le condizioni di sicurezza definite dalla SP (e.s., tunnel mode con ESP) siano utilizzate e quindi accetta il pacchetto.

Configurazione delle SA e delle SP

- Le Security Policies sono definite manualmente
- Le SA possono essere
  - » Definite manualmente
  - » Definite in modo automatico attraverso l'uso del protocollo IKEv2
    - » IKE è solitamente invocato quando una SP è verificata ma non vi è la relativa SA all'interno del SAD
    - » È composto da due fasi:
    - » Phase 1: si contratta una IKE SA, ovvero una Security Association IPsec per la sola segnalazione IKE. Per rendere sicura la negoziazione (che include un accordo sulle chiavi di cifratura della IKE SA) si usano approcci basati sullo scambio di cetificati (tipo TLS) o su un segreto condiviso a priori
    - » Phase 2: si usa il canale sicuro della segnalazione IKE per negoziare la IPSEC SA
    - » Una volta configurata IKE SA può essere utilizzata per contrattare più IPSEC SA. La IKE SA è long-term rispetto alla IPSEC SA

VPN IPSEC Tunnel Mode (G2G)- (No IKE)



SA:

- »**SPI: 0x01**
- »**ESP Key:** 0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df
- »**Src IP: 160.80.85.1**
- »**Dst IP: 160.80.85.2**
- »**Mode: Tunnel**

SP:

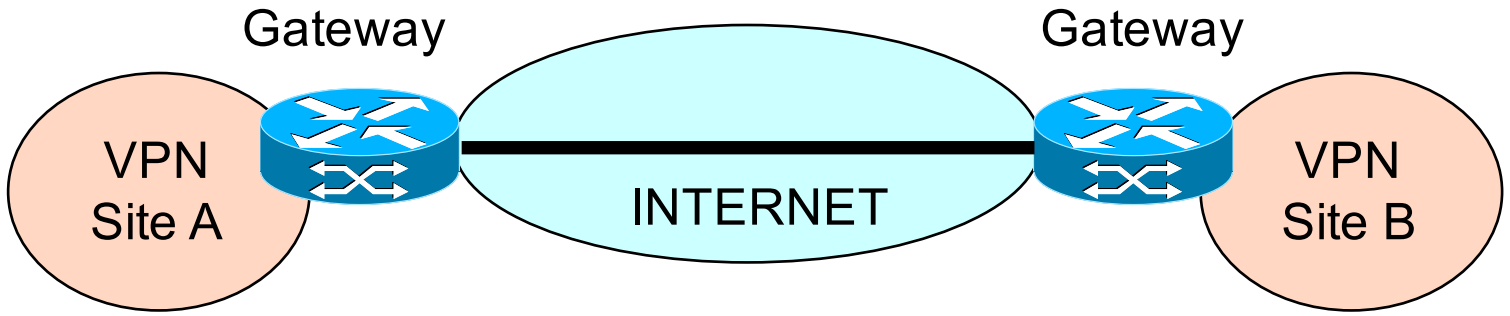
- »**Net_id/mask sorgente 192.168.1.0/24**
- »**Net_id/mask 192.168.2.0/24**
- »**Porta sorgente / destinazione: any**
- »**Direzione (in/out): out**
- »**Azione da intraprendere (ipsec/discard/none): ipsec**
- »**Protocollo di sicurezza (ah/esp/ipcomp): esp**
- »**Modalità di incapsulamento (transport/tunnel): tunnel**
- »**IP sorgente e destinazione del tunnel (solo tunnel mode): 160.80.85.1-160.80.85.2**

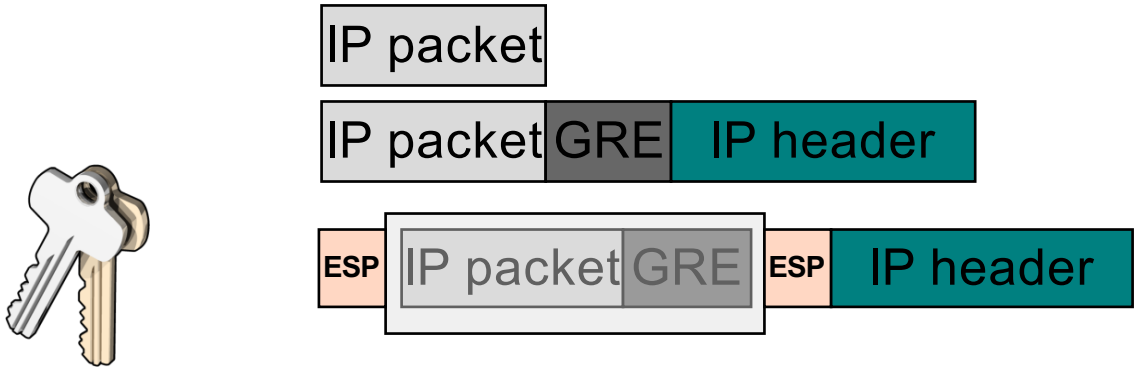
Problema: come faccio a trasferire anche il traffico broadcast/multicast ?

IP over GRE over IPsec (transport)

IP over GRE over IPsec (transport)

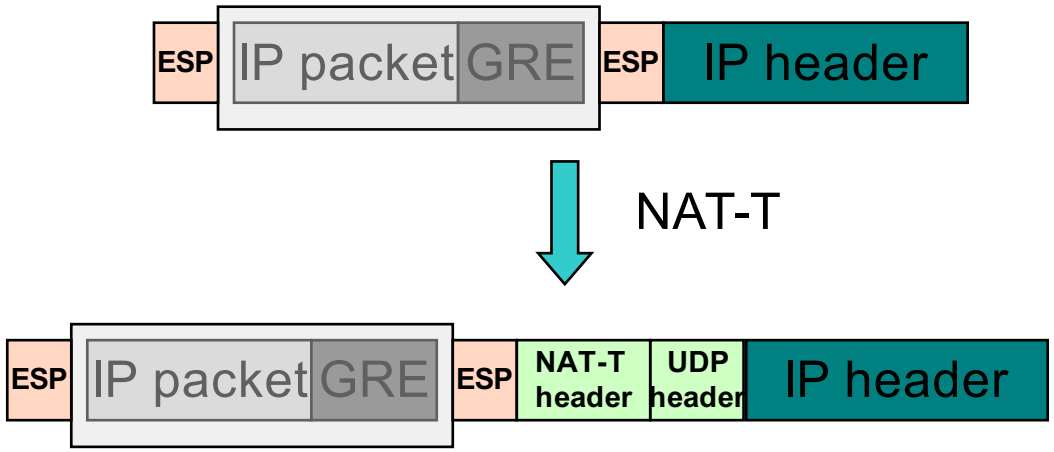
- GRE è un protocollo che principalmente definisce solo un formato di incapsulamento; l'header GRE ha un campo protocol_type da due byte che permette anche l'incapsulamento di pacchetti IP, MPLS, etc.
- È utilizzato per fare dei tunnel IP
- Il tunnel è visibile all'utente come una scheda virtuale tun gestita dal modulo GRE del kernel
- Nel nostro caso,
  - GRE incapsula un pacchetto IP (anche multicast) da mandare sulla VPN remota
  - GRE genera un pacchetto IP esterno con indirizzi ip pubblici di sorgente e destinazione
  - Questo pacchetto IP è unicast e con indirizzi pubblici quindi trattabile da IPSec in transport mode
- Infine la soluzione GRE over IPSec è anche utilizzabile per supportare il dynamic routing. Pertanto offre più servizi rispetto a IPSec tunnel mode, sebbene aumenti l'overhead



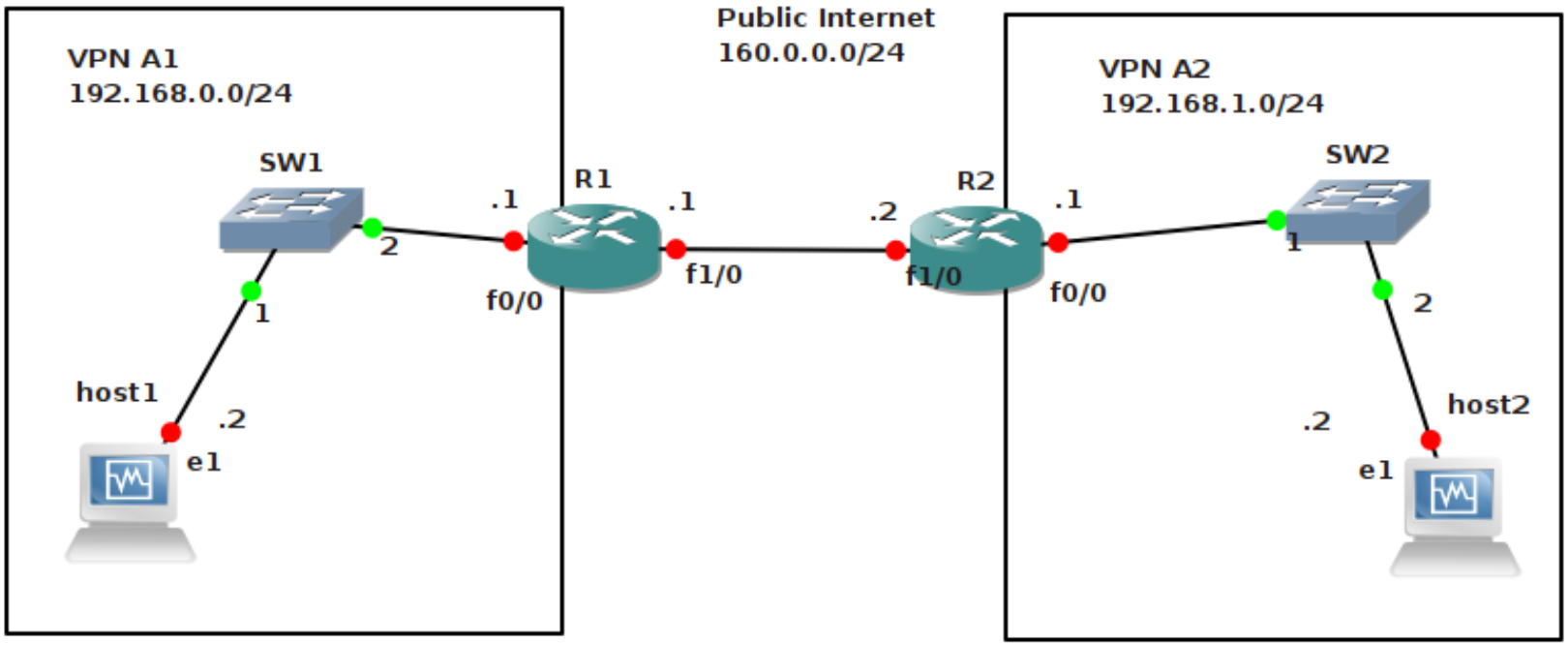


IPSec VPN vs NAT e Dynamic IP

- Stesso scenario del caso user-space VPN
- IPSec assicura l'integrità informativa di tutto il pacchetto (con AH) o della sola parte di payload (con ESP)
- Nel caso di impiego di AH, la modifica dell'header IP apportata dal NAT è vista come una alterazione dell'integrità e quindi in ricezione il pacchetto è scartato
- Con ESP questo problema non sussiste, tuttavia normalmente il NAT è un NPAT (network and port address translation) e se ESP cifra il payload, l'informazione di porta è inaccessibile ed il NPAT non inoltra il pacchetto
- Soluzione NAT-T (NAT Traversal) : il payload IP del pacchetto IPSec ESP è incapsulato in datagramma UDP con header in chiaro
- Su questo datagramma il NAT riesce ad operare
- È richesto un accordo a priori fra le parti e la disponibilità della funzione di NAT-T su entrambe le parti



GRE/IPSEC Cisco LAB with static SAs



GRE/IPSEC Cisco LAB with static SAs

R1 configuration

```
!Phase A: send all packets toward LAN B within the GRE tunnel
! Step 1: configure IP addresses
! IP address configuration
interface FastEthernet1/0
          ip address 160.0.0.1 255.255.255.0
          no shut

interface FastEthernet2/0
          ip address 192.168.0.1 255.255.255.0
          no shut

! Step 2: configure GRE tunnel interface
interface Tunnel0
          ip address 10.0.12.1 255.255.255.0
          tunnel source 160.0.0.1
          tunnel destination 160.0.0.2

! Step 3: configure a route via Tunnel0
ip route 192.168.1.0 255.255.255.0 Tunnel0
```

GRE/IPSEC LAB with static SAs

R1 configuration

```
!Phase B: configure IP SEC
!step 1: create an ACL for the IPSEC outbound policy
access-list 100 permit ip host 160.0.0.1 host 160.0.0.2

!step 2: create a transform set
crypto ipsec transform-set myts esp-aes

!step 3: create a crypto map (XXX for r2 swap SPI_inbound and SPI_outbound)
crypto map mycmap 1 ipsec-manual
          set peer 160.0.0.2
          set session-key inbound esp 1000 cipher 7a8ec0d7f95b01d46758830ba0de280f
          set session-key outbound esp 1001 cipher 7a8ec0d7f95b01d46758830ba0de280f
          set transform-set myts
          match address 100

!step 4: attach my new crypto map to F1/0 (the out interface)
interface FastEthernet1/0
          crypto map mycmap
```

IPSEC configuration with IKE

- IKE automatically negotiates IPsec security associations (SAs) and enables IPsec secure communications without costly manual preconfiguration
- Benefits
  - » Eliminates the need to manually specify all the IPsec security parameters in the crypto maps at both peers
  - » Allows you to specify a lifetime for the IPsec SA
  - » Allows encryption keys to change during IPsec sessions
  - » Allows IPsec to provide antireplay services
  - » Permits certification authority (CA) support for a manageable, scalable IPsec implementation
  - » Allows dynamic authentication of peers

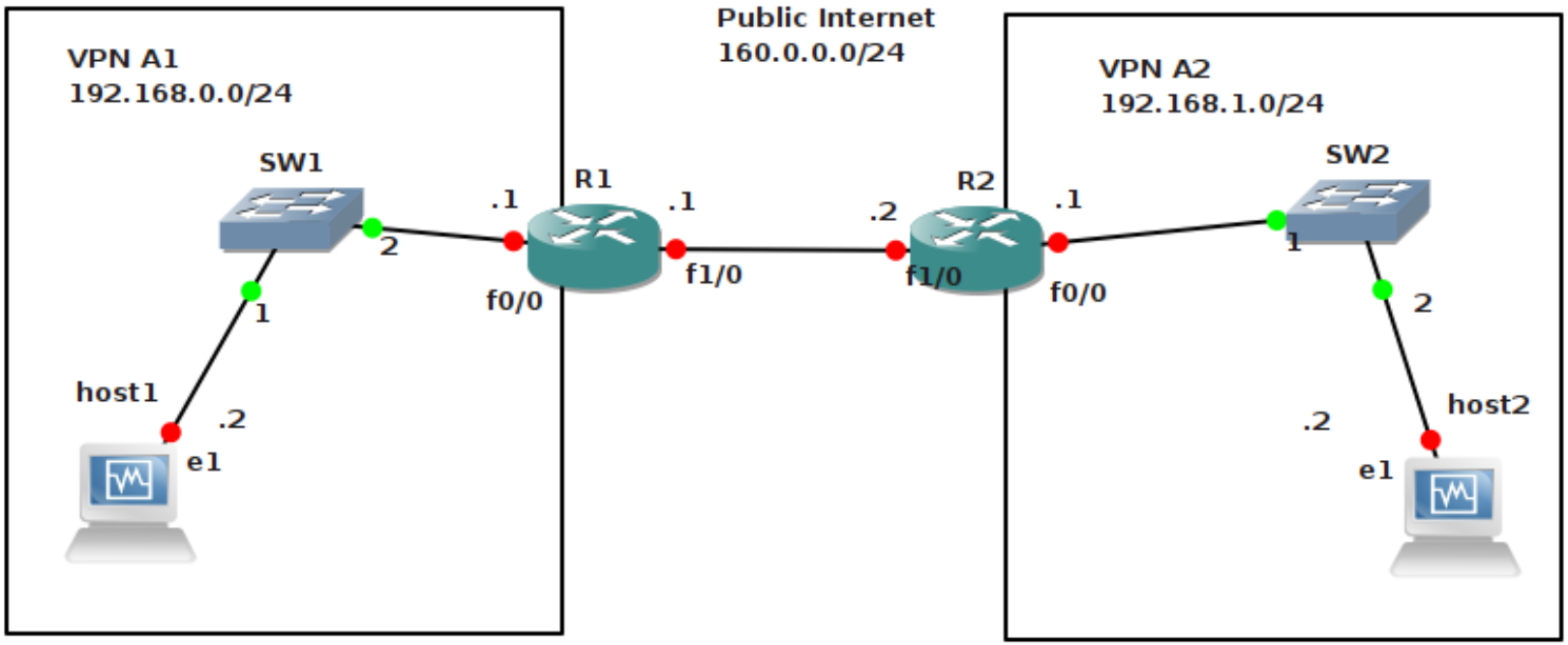
IPSEC configuration with IKE

- Each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy.
  - » This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated.
- After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these SAs apply to all subsequent IKE traffic during the negotiation
- When the IKE negotiation begins, IKE searches for an IKE policy that is the same on both peers
  - » The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match.
  - » The remote peer looks for a match by comparing its own highest priority policy against the policies received from the other peer.
  - » The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.
  - » A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values.

IPSEC IKE

- If a match is found, IKE will complete negotiation, and IPsec security associations will be created.
- If no acceptable match is found, IKE refuses negotiation and IPsec will not be established.
- IKE authentication type can be one of the following:
  - » RSA Signatures
  - » RSA Encrypted Nonces
  - » Preshared Keys

IKE LAB: pre-shared secret



Same LAB, same IP/GRE configuration!

IPSEC/IKE LAB: pre-shared keys

R1 configuration

```
!configure IKE policy
crypto isakmp policy 10
         encryption aes 256
         hash sha
         authentication pre-share
         group 5
         lifetime 180

!configure IKE identity identità ike
crypto isakmp key "blablabla1234" address 160.0.0.2

!configure a transform set
crypto ipsec transform-set myts2 esp-3des esp-md5-hmac

!configure a crypto map and reference the ike policy
crypto map mycmap2 10 ipsec-isakmp
         set peer 160.0.0.2
         set transform-set myts2
         match address 100

!attach crypto map to out interface
fastEthernet 1/0
         crypto map mycmap2
```

L2TP VPN

Overlay VPN

L2TP

- Sono VPN di tipo client-to-host utilizzabili in ambiente “Road-Warrior”, i.e. un utente viaggiatore che si connette alla rete *home* attraverso un laptop.
- Nessuna necessità di software aggiuntivi su terminali di tipo MS Windows
- L2TP è utilizzato per il tunnelling di trame PPP (Layer 2); quindi permette a PPP di lavorare anche fra dispositivi non direttamente connessi da un mezzo fisico
- L2TP si serve di un socket UDP su porta server 1701
- Dal punto di vista dell’utente, l’accesso alla rete home avviene come un classico accesso PPP dial-up basato su user-name e password; le funzionalità di PPP provvedono a configurare in modo automatico lo stack di networking dell’utente
- A differenza di PPP su un accesso fisico (e.s., modem), utilizzando PPP su L2TP l’accesso al servizio è svincolato dal set-up di una connessione modem. Basta che l’utente è connesso ad Internet ed L2TP farà apparire un tunnel a PPP, come se PPP fosse su un linea dial-up.
- Per incrementare la sicurezza della comunicazione, in aggiunta alla cifratura di PPP, L2TP è spesso incapsulato in IPSec (con o senza IKE) modalità transport