# Retele VPN bazate pe MPLS

MPLS VPN

# Agenda

- Conceptul MPLS
- MPLS-VPN
- Terminologie MPLS-VPN
- Modelul MPLS-VPN
- Mecanismul de forward
- Pasii construirii MPLS-VPN
- Concluzii

# Agenda

- Conceptul MPLS
- MPLS-VPN
- Terminologie MPLS-VPN
- Modelul MPLS-VPN
- Mecanismul de forward
- Pasii construirii MPLS-VPN
- Concluzii

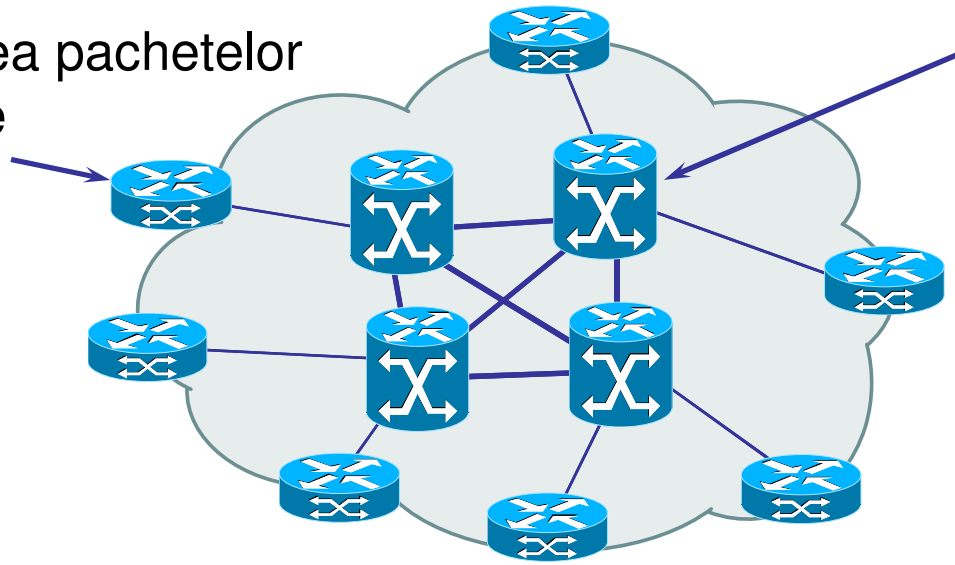
# Conceptul MPLS

- combina ce e mai bun din cele doua lumi:
  - securitate si QoS din ATM, Frame Relay
  - flexibilitate si scalabilitate din IP
- retea IP neorientat pe conexiune + mecanism de comutare orientat pe conexiune

# Conceptul MPLS

La intrare:
- clasificarea pachetelor
- etichetare

In retea:
- comutare cu etichete
- eticheta indica serviciul si destinatia

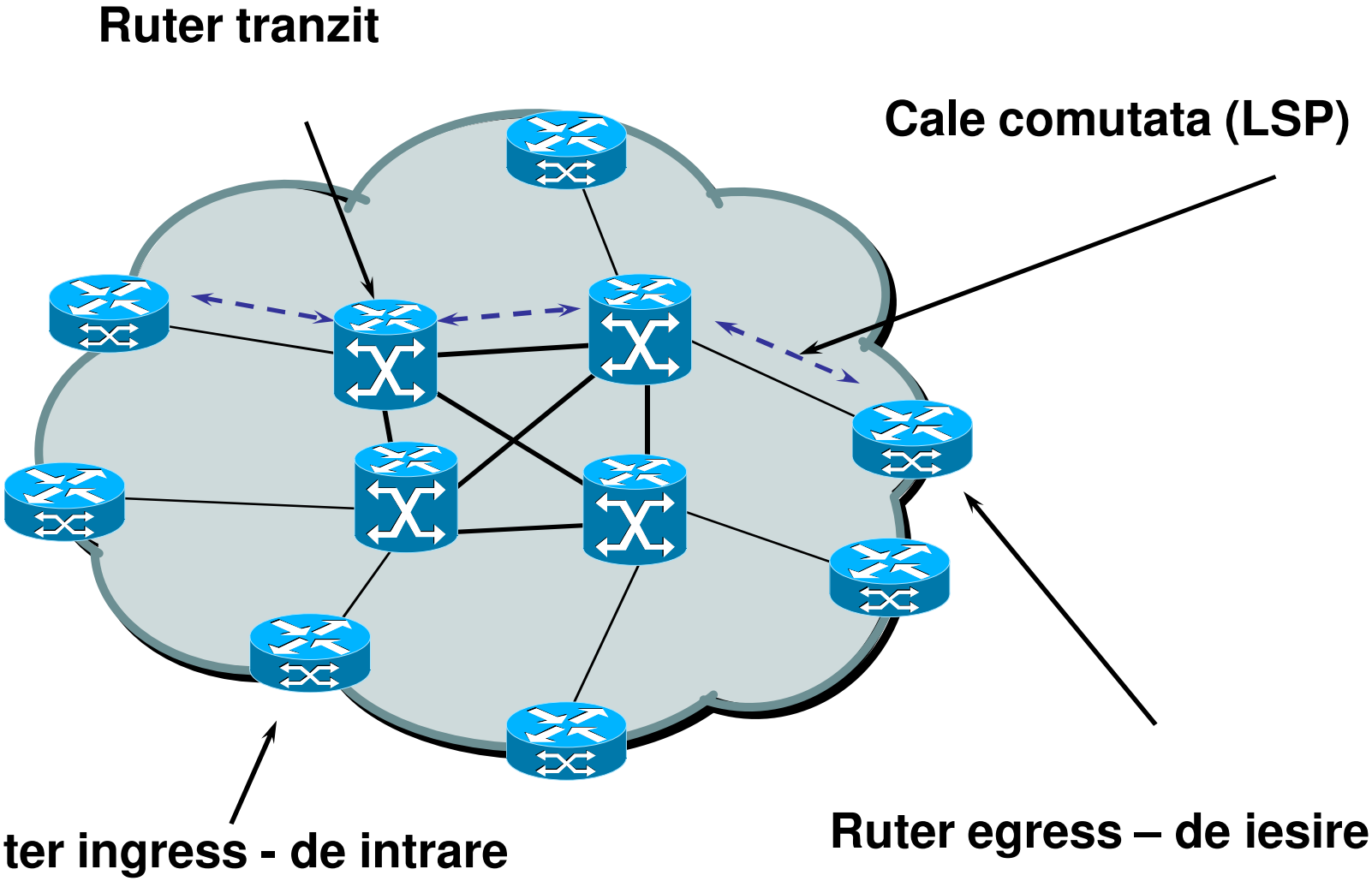


- comutarea cu etichete
- protocoale de nivel retea: IP, IPX, AppleTalk
- eticheta: unde si cum sa transmit pachetul

# Conceptul MPLS

- etichete MPLS
- clase de echivalenta
- rutere MPLS
- cai comutate
- penultimate/ultimate hop popping
- protocoale de semnalizare

# Conceptul MPLS

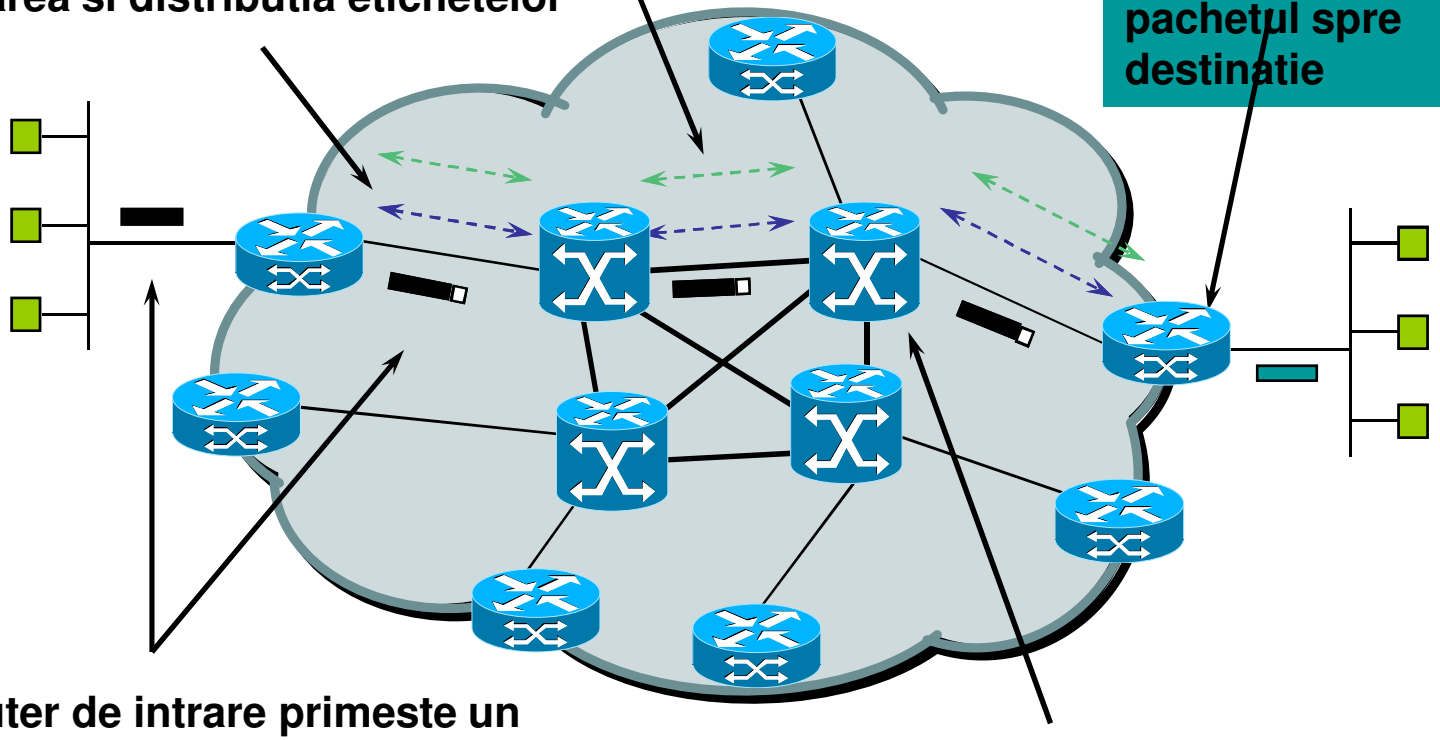


# Conceptul MPLS

**1a. Protocoale de rutare (OSPF,IS-IS) stabilesc topologia retelei**

**1b. Protocoale de semnalizare pentru asignarea si distributia etichetelor**

**4. Ruterele de iesire sterg eticheta si ruteaza pachetul spre destinatie**



**2. Un ruter de intrare primeste un pachet, evalueaza serviciile de care are nevoie, asigneaza unui FEC, eticheteaza pachetul**

**3. Ruterele tranzit comuta pachetele pe baza etichetelor**

# Agenda

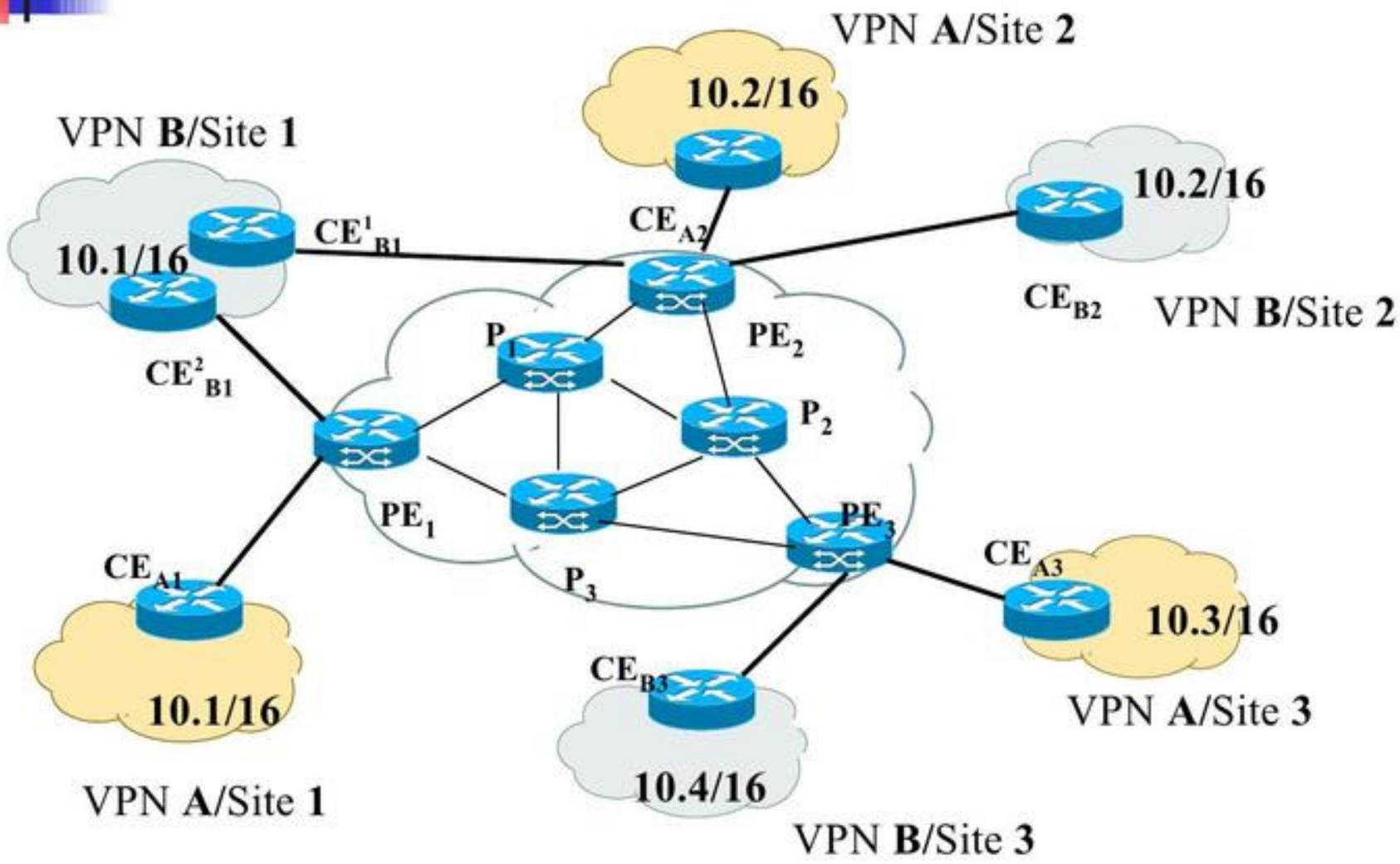
- Conceptul MPLS
- MPLS-VPN
- Terminologie MPLS-VPN
- Modelul MPLS-VPN
- Mecanismul de forward
- Pasii construirii MPLS-VPN
- Concluzii

# De ce MPLS-VPN

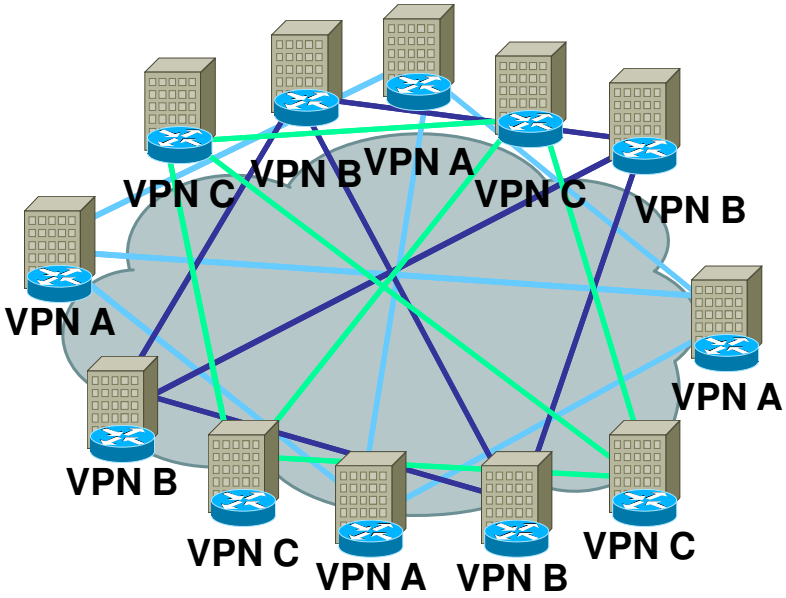
- VPN = servicii private intr-o infrastructura publica
- VPN = Set de site-uri carora li se permite sa comunice impreuna
- VPN definit ca un set de politici administrative:
  - Determina conectivitatea si servicii QoS intre site-uri
  - Politicile stabilite de utilizatori
  - Politicile implementate de VPN service provider prin mecanisme BGP/MPLS VPN

- Modele de VPN
    - model overlay: VPN de nivel 2
    - model peer: VPN de nivel 3

# BGP/MPLS VPN - example



# Modelul overlay



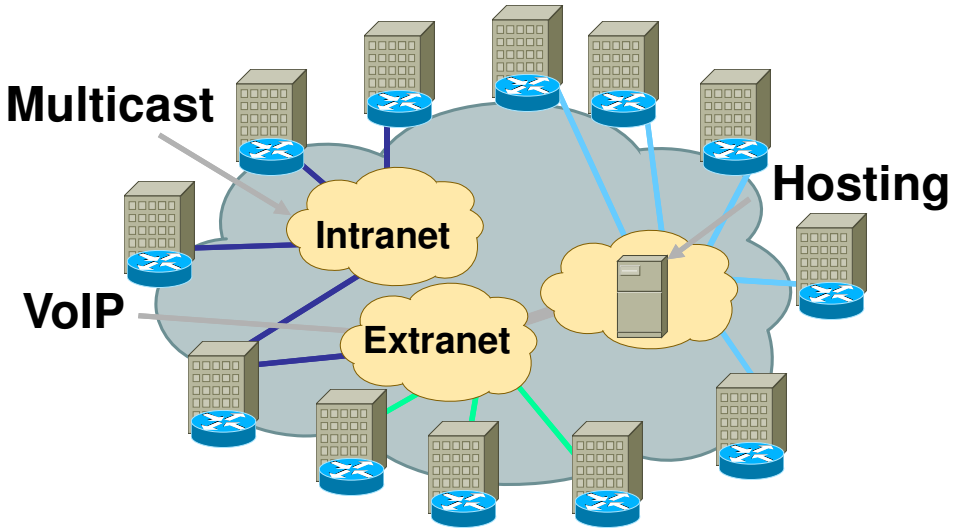

- protocol de nivel 2 orientat pe conexiune (Frame Relay/ATM)
- site legat la retea P (provider) prin CV (circuit virtual): Private Virtual Circuit
- PVC comutate in retea provider pt conectivitate cu alte site-uri
- topologie de rutare invizibila pentru provider
- inteligenta la utilizator
- problema scalabilitatii
- actualizarea matricii de trafic
- recalculare mesh de PVC
- reconfigurare echipamente pentru noua topologie

# Modelul peer

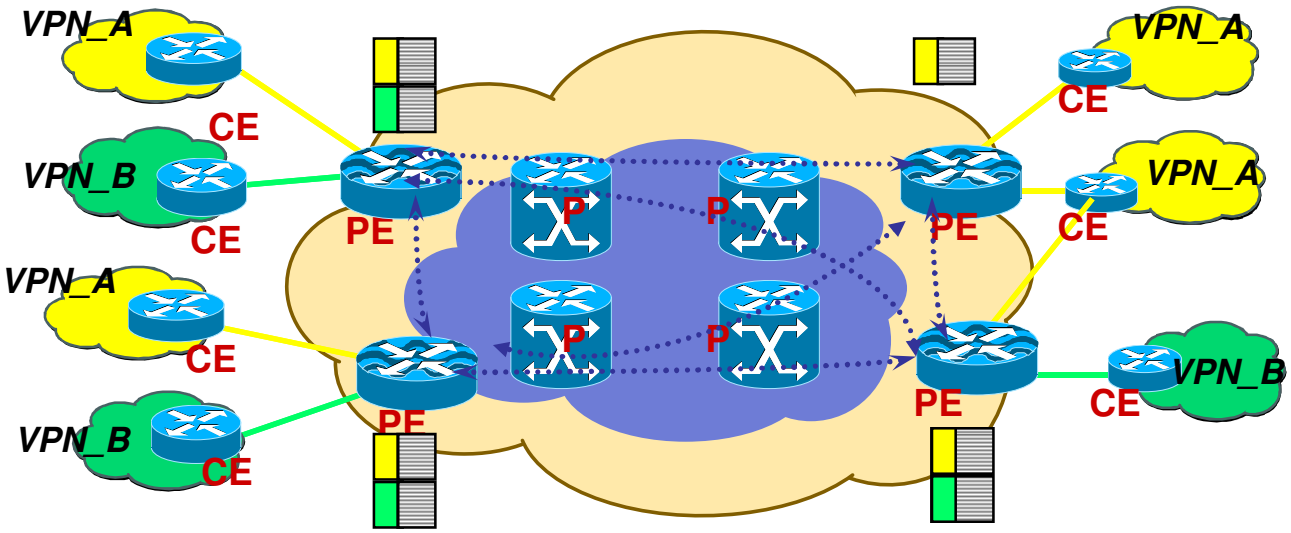
- protocoale de rutare – retea utlizator si retea provider
- ruterele utilizator mentin adiacenta de rutare cu ruterele provider
- inteligenta la utilizator si backbone
- problema: nu e permisa utilizarea adreselor private

# Adevaratul model peer: MPLS-VPN

- la fel ca peer DAR!!!
- ruterele provider mentin informatie doar despre VPN conectate
- MPLS in backbone
- independent de tehnologie
- neorientare pe conexiune + servicii IP



# Terminologie MPLS-VPN



# Terminologie MPLS-VPN

- retea provider (P net)

  backbone sub control Service Provider
- retea utilizator (C net)

  retea sub control utilizator
- ruter CE (Customer Edge Router)

  ruter utilizator care are o interfata spre ruter PE

# Terminologie MPLS-VPN

- ruter PE (Provider Edge Router)
  - ruter provider care are interfata spre un ruter CE
  - noduri ingress/egress in domeniul MPLS
- ruter P
  - ruter din backbone provider
  - nod tranzit in domeniul MPLS
  - nu are informatii despre VPN

# Terminologie MPLS-VPN

- legatura PE-CE
  - link intre PE-CE
  - ATM, Frame Relay, Ethernet, PPP
- Site
  - (sub)retele in aceeasi locatie (acelasi site)
  - conectare la backbone prin link PE-CE

# Terminologie MPLS-VPN

- VRF (VPN Routing and Forwarding Instance)
  - nivel ruter PE
  - asociat unei/unor interfete PE
  - accesibil doar membrilor unui anumit VPN
  - informatia de rutare dintr-un VPN
  - avantaj: spatii de adresare comune

# Terminologie MPLS-VPN

- **RD (Route Distinguisher)**
  - atribut al unei rute; 64 biti
  - identifica unic VPN-ul
  - nivel ruter PE, pentru fiecare VRF (fiecare VPN direct atasat)

  RD = Type + Provider's Autonomous System Number + Assigned Number

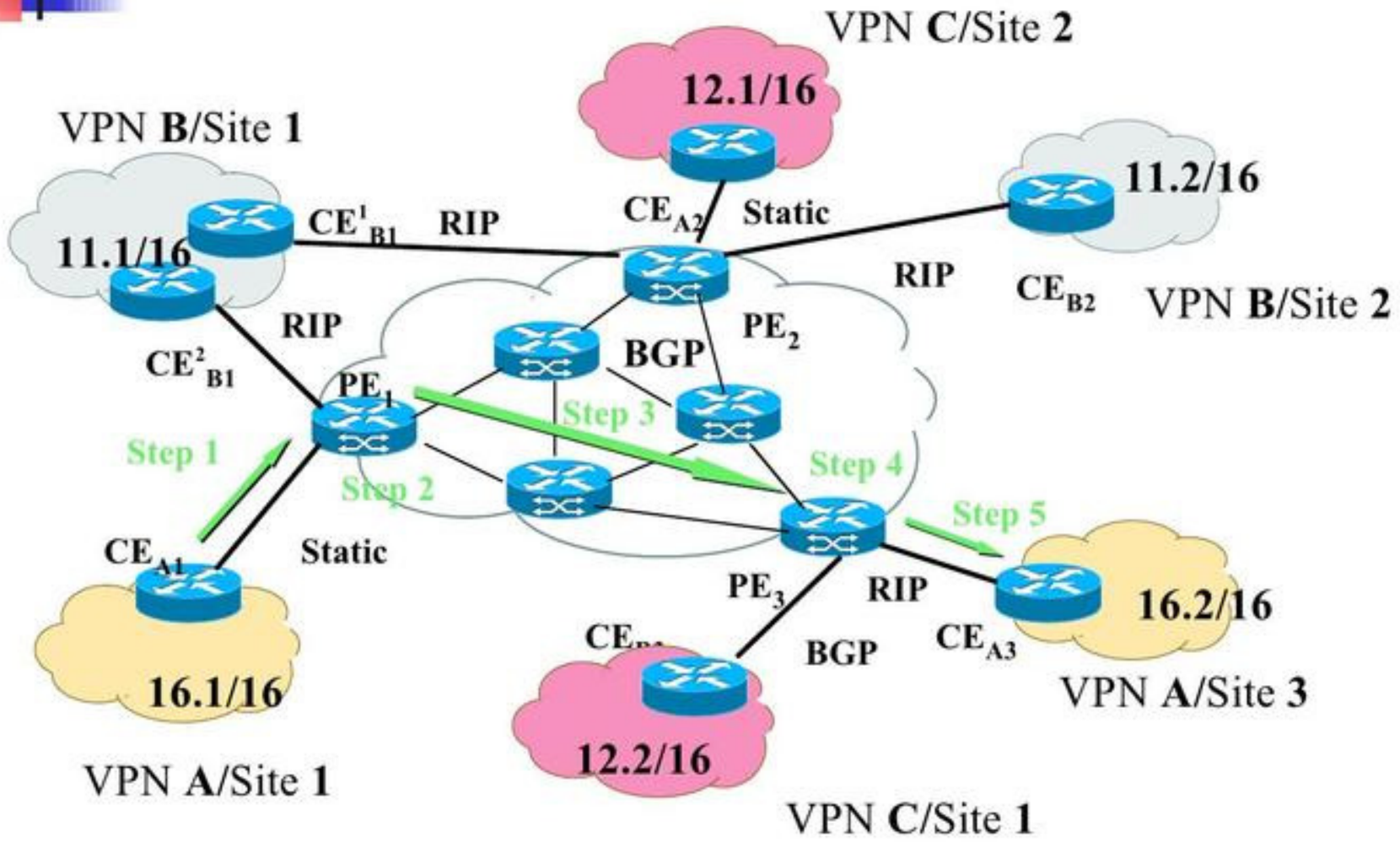
  - realizare unicitate adresa (VPN diferite = RT diferite)

- **adresa VPN-IPv4**
  - concatenare RD si adresa IPv4; 96 biti
  - Folosita in transport info rutare in backbone (prin extensii multiprotocol ale BGPv4 i.e. MP-iBGP); nu pentru transport trafic VPN!
  - utilizatorii nu cunosc VPN-IPv4

# Terminologie MPLS-VPN

- **Route Target (RT)**
  - identifica ruterele care trebuie sa primeasca informatie de rutare
  - atribut in mesajele MP-iBGP de actualizare
  - ruterele PE importa/exporta msg de actualizare
  - actualizarea VPN-IPv4 marcata cu atributul RT

# Routing Information Distribution - example



**Distribuirea informatiei de rutare:**

Distribuire constransa a informatiei de rutare ( conectivitatea site-uri determinata de distribuirea informatie rutare)

Step 1 : de la site (de la CE asociat) la service provider (la interfata PE corespunzatoare)

Prin RIP, static routing, BGP, sau OSPF

Step 2 : pentru PE ingress: export informatie de rutare (bazata pe IP) la protocolul MP-iBGP rulat in retea provider (intre rutere PE), prin formare adresa VPN-IP;

Step 3 : transmisie in cadrul/intre domenii providerilor (intre PEs) – de obicei in backbone (aici MPLS backbone)

Step 4 : informatia de rutare (VPN-IP) importata de la MP-iBGP provider si transmisa catre egress PE (adresa IP folosita in tabela de inaintare (VRF) corespunzatoare)

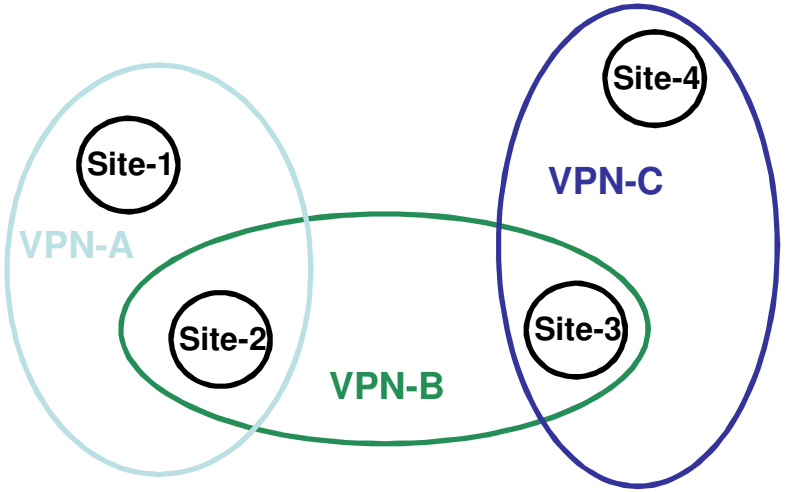
Step 5 : de la provider (PE) la site (CE)

e.g., via RIP, static routing, BGP, sau OSPF

# Modelul MPLS-VPN

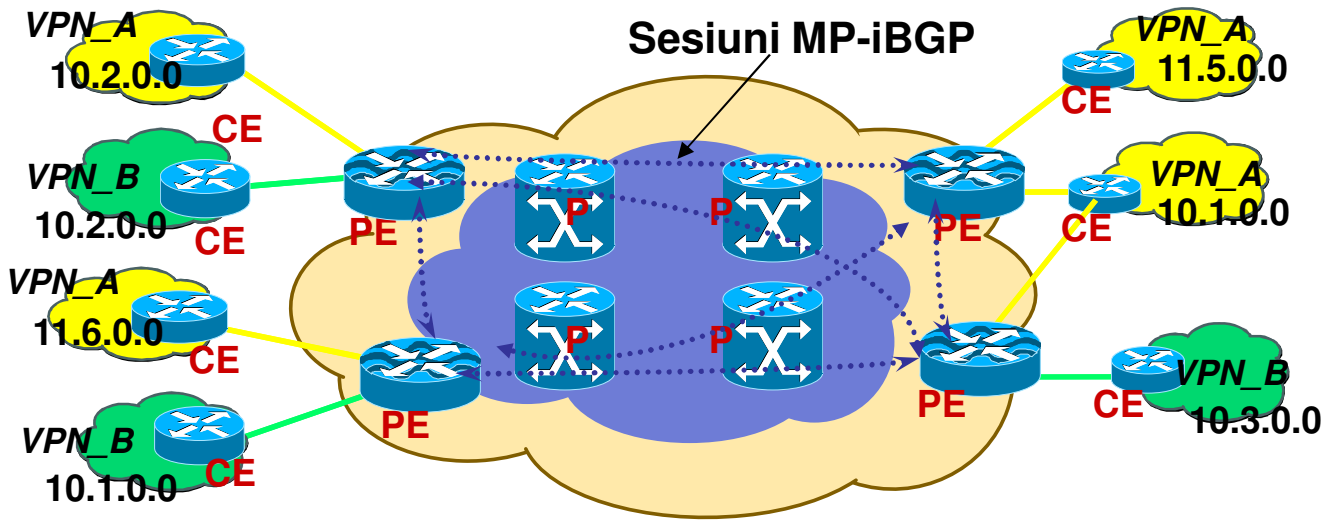
- VPN = set de site-uri care impart aceeasi informatie de rutare
- VPN – comunitate de interese
- multiple VRF la nivelul ruterelor PE

# Modelul MPLS-VPN




- un site poate sa apartina mai multor VPN-uri
- daca doua sau mai multe VPN-uri au un site comun, spatiul de adresare trebuie sa fie unic intre aceste VPN-uri

# Modelul MPLS-VPN

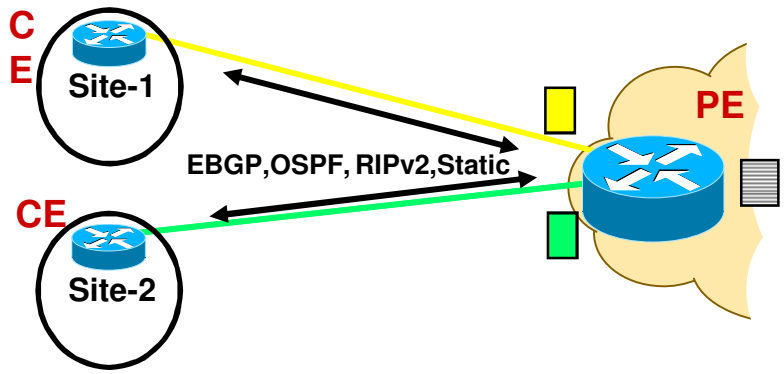



- backbone cu noduri MPLS
  - rutere PE – noduri intrare/iesire backbone
  - rutere P – noduri tranzit

# Modelul MPLS-VPN

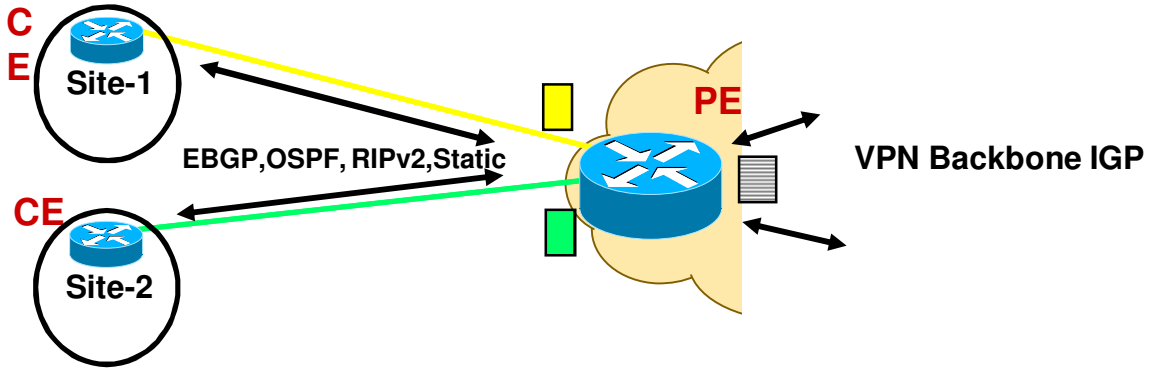
- rutere PE legate de rutere CE
- rutere PE distribuie informatie de rutare VPN prin sesiuni MP-iBGP
- rutere PE utilizeaza MPLS in backbone (cu rutere P) si IP routing cu rutere CE
- rutere PE si P utilizeaza aceleasi protocoale interioare de rutare
- Se realizeaza full mesh intre rutere PE

# Modelul MPLS-VPN



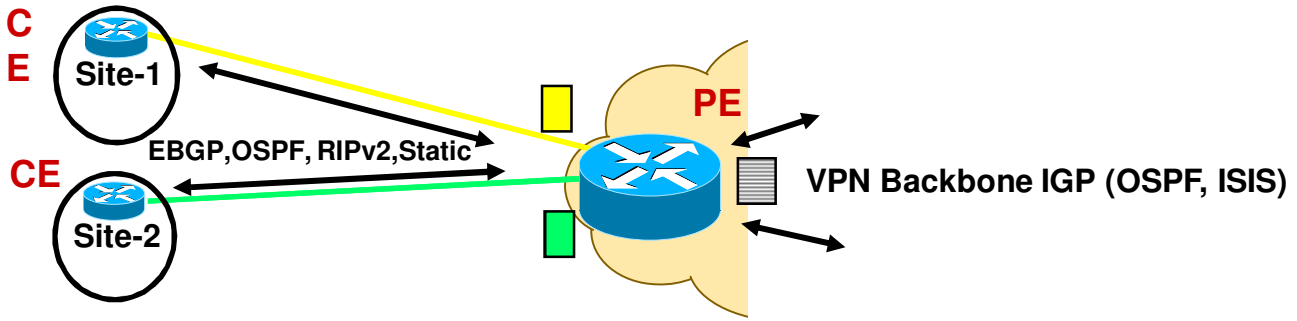

- ruterele PE si CE schimba informatie de rutare prin:
  - eBGP, OSPF, RIPv2, rutare statica

# Modelul MPLS-VPN



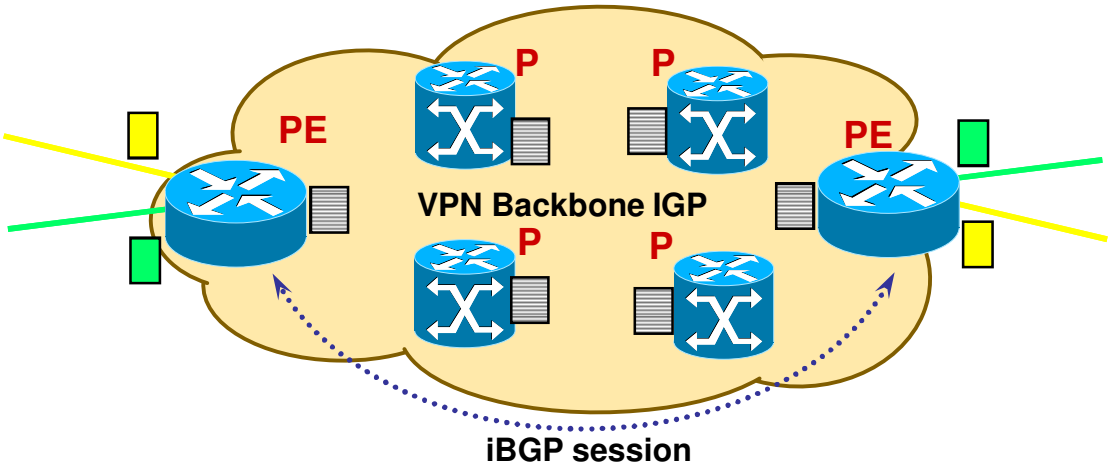

- pentru un PE: rutele primite de la CE se mentin in VRF (aici in tabele verde sau galben: VPN diferite - culori diferite!)
- rutele primite prin IGP se mentin in tabela globala de rutare (aferenta MPLS backbone la care apartine acel PE)

# Modelul MPLS-VPN




- ruterele PE mentin
  - tabela globala de rutare
    - rutele spre PE si P
    - populata de protocoale de rutare IGP
  - VRF (VPN Routing and Forwarding)
    - VRF asociat cu unul sau mai multe site-uri (CE)
    - VRF asociat (sub)interfetelor ce leaga PE de CE

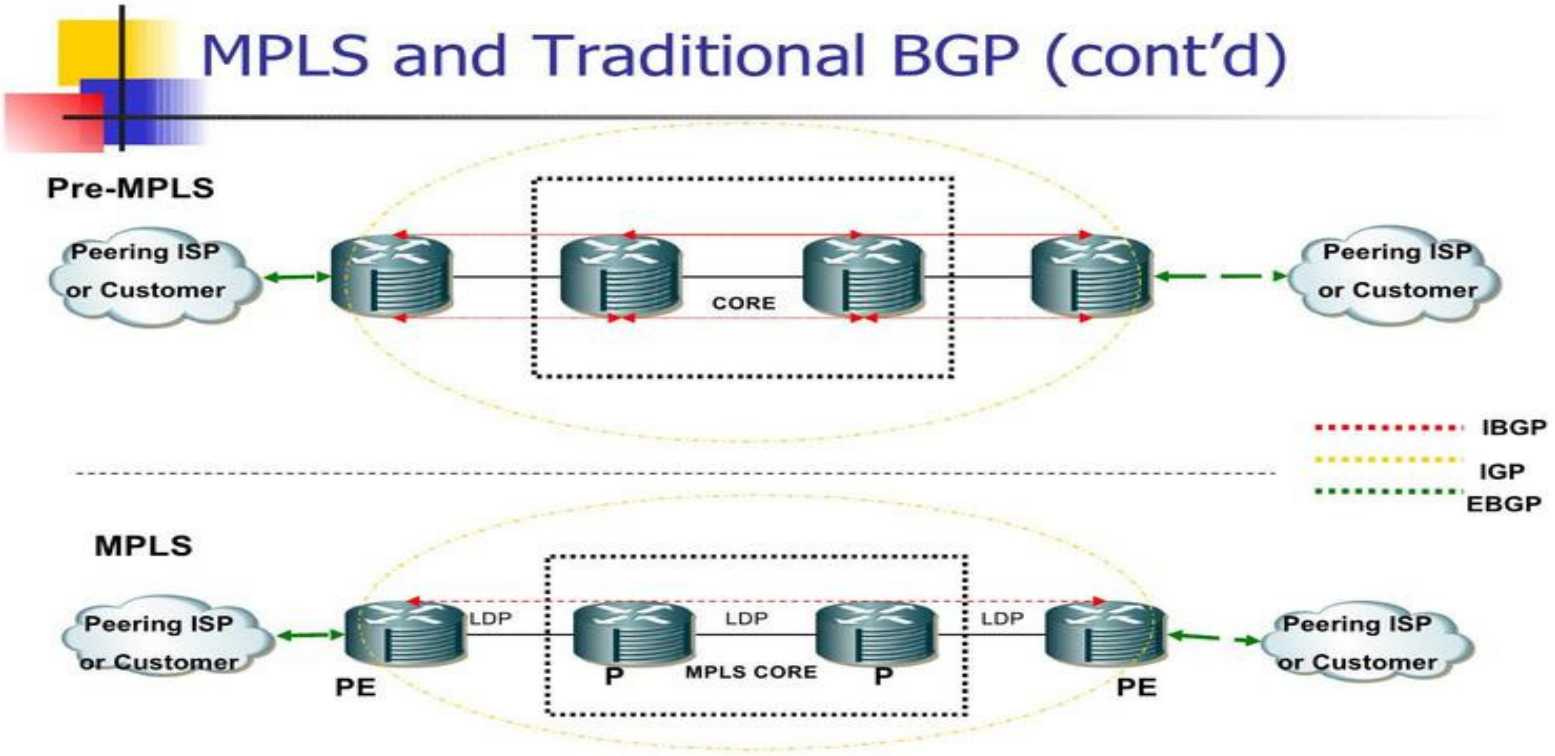
# Modelul MPLS-VPN




- ruterele PE si P utilizeaza acelasi IGP (OSPF, IS-IS)
- ruterele PE stabilesc sesiuni MP-iBGP
- ruterele PE utilizeaza MP-iBGP pt schimbul de informatie de rutare (despre diferite sites, VPNs)

# MPLS si BGP

-MPLS simplifica inaintarea pachetelor catre destinatii BGP
-Traditional fiecare ruter din backbone ISP provider trebuia sa ruleze BGP
-MPLS permite inaintarea pachete catre destinatii BGP (BGP next hop) prin simpla comutare bazata pe etichete MPLS
-Ruterele ISP core (ruterele P) necesar sa ruleze doar IGP, doar ruterele PE necesar sa ruleze si BGP

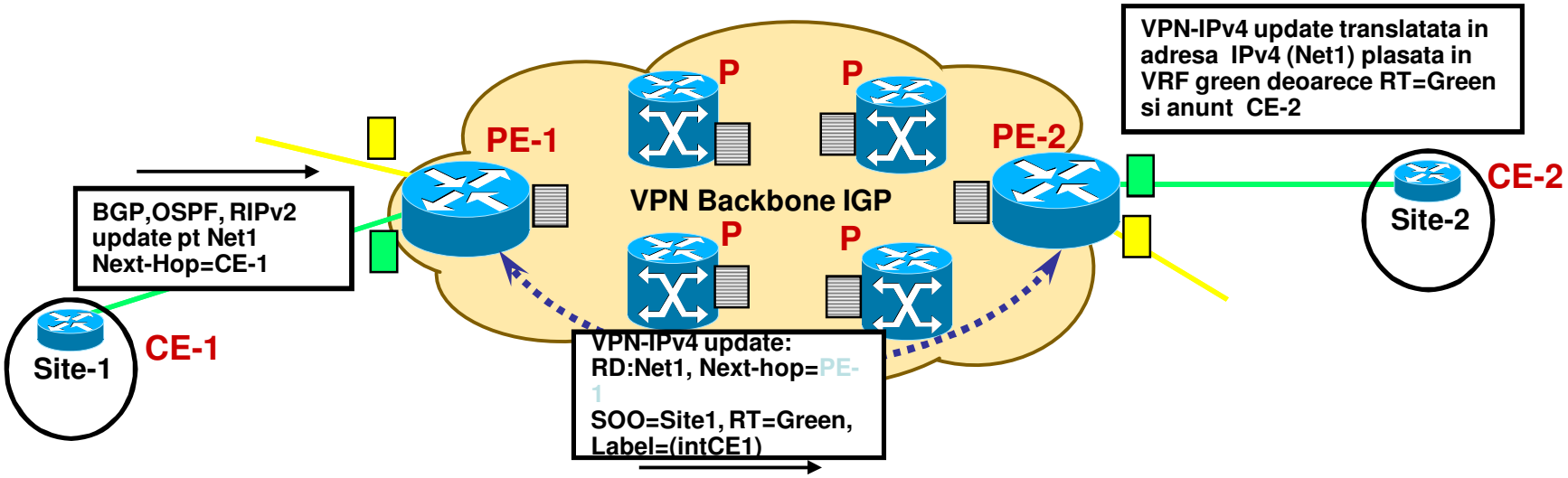


## Modelul MPLS-VPN

- actualizari MP-iBGP
  - adresa VPN-IPv4
  - atribute: RT (route target)
  - eticheta: identifica interfata de iesire (un ruter PE asociaza o eticheta rutelor pe care le invata de la un site)

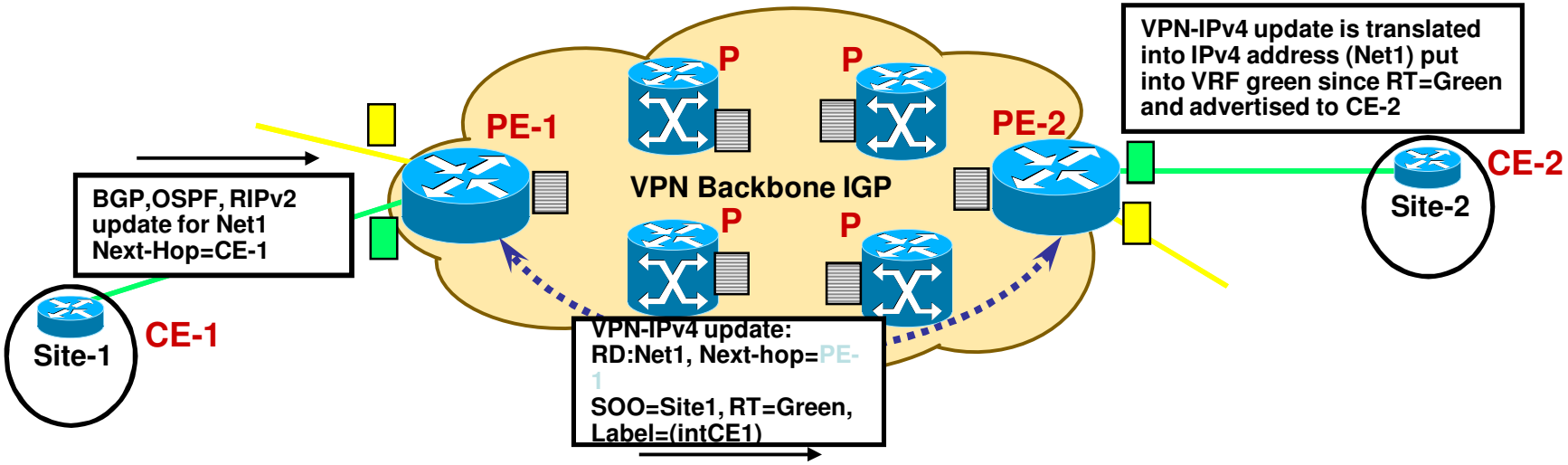
- In updates pentru VPN-IP, fiecare PE trece ca adresa next-hop propria adresa (vezi slide urmator)

# Modelul MPLS-VPN




- PE primeste msg de actualizare de la CE, bazat pe adrese IPv4
    - translateaza in VPN-IP, asigneaza RT
    - rescrie next-hop cu propria adresa
    - asigneaza eticheta (interfata)
    - mesaj de actualizare celorlalte rutere PE

# Modelul MPLS-VPN

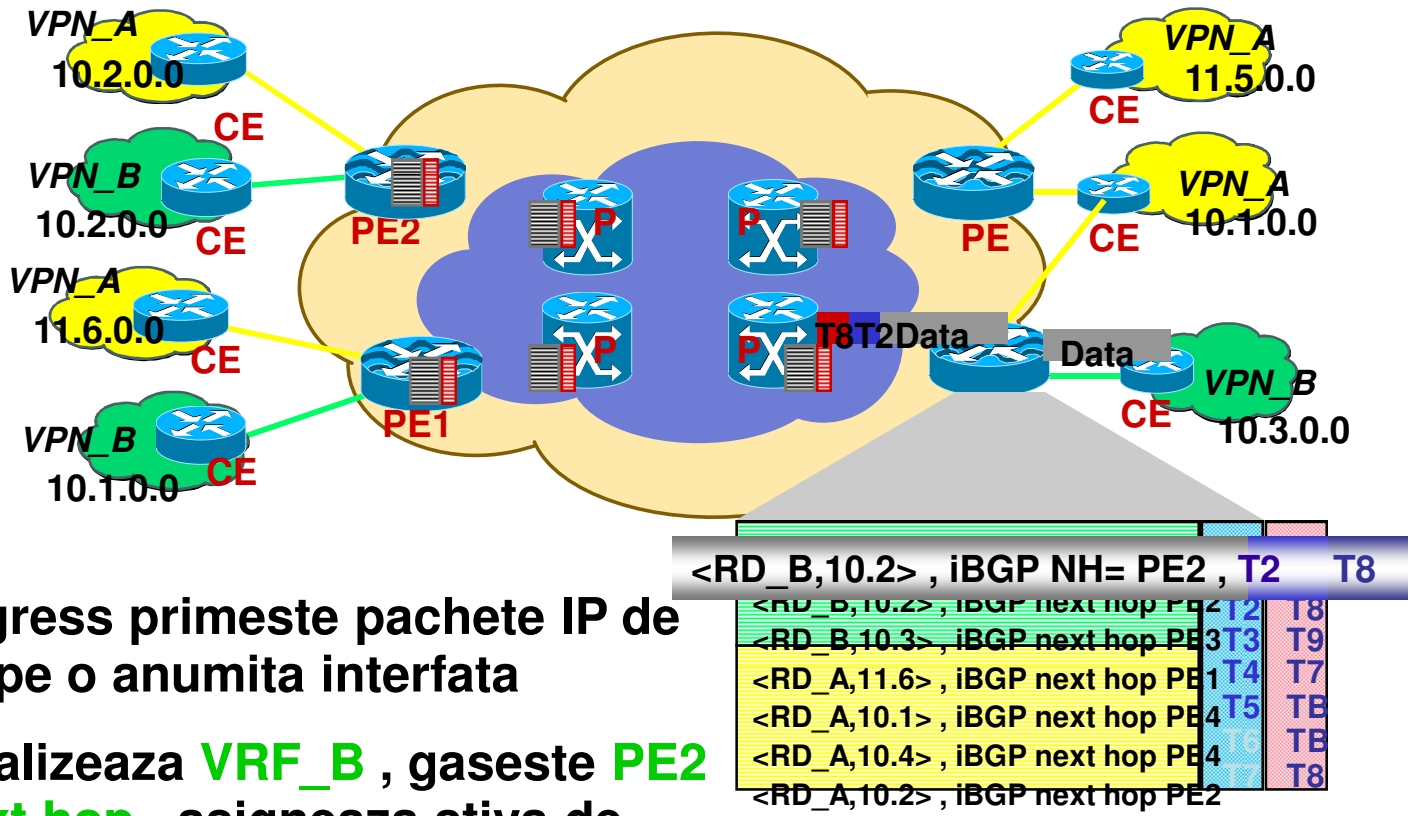



- ruterele PE care primesc msg de actualizare insereaza ruta in VRF identificat prin RT
- eticheta e transmisa in headerul MPLS al pachetului

# Mecanismul de forward

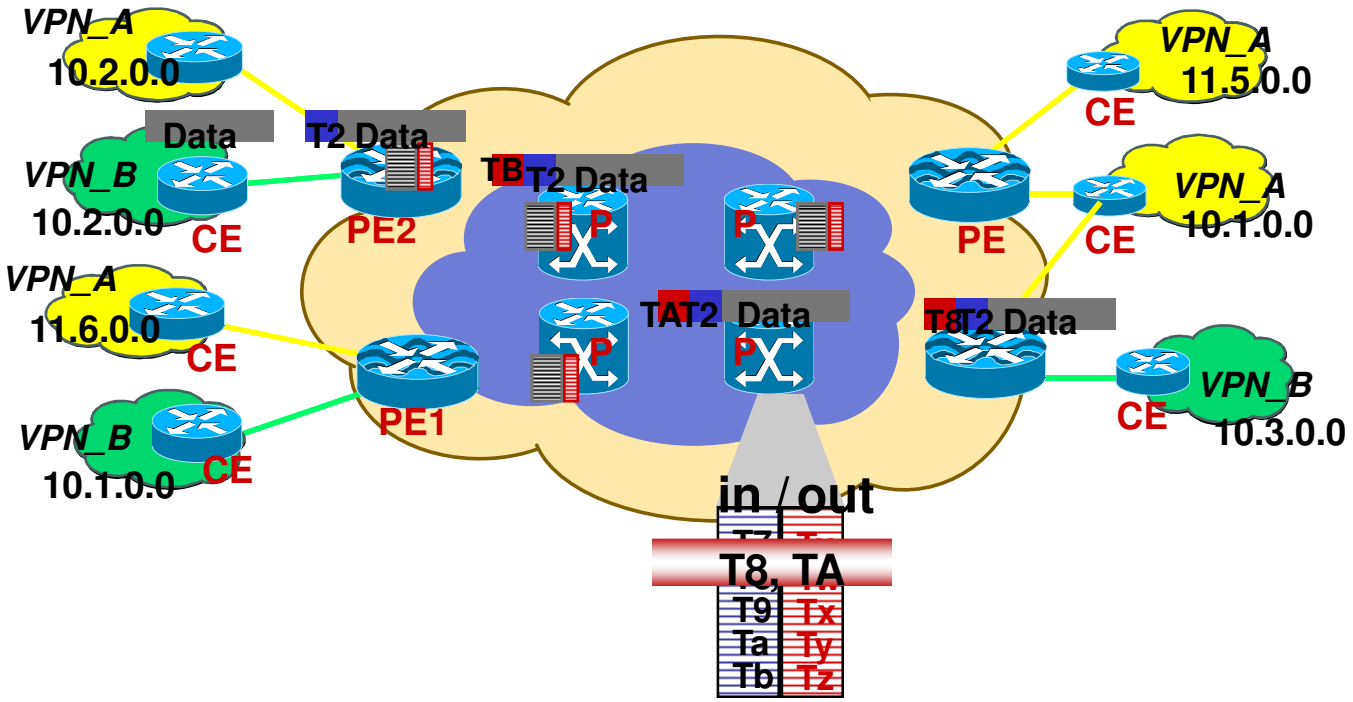
- PE si P utilizeaza protocoale IGP
- In backbone: MPLS
- comutare cu etichete asignate si distribuite prin LDP
- stiva de etichete
  - top label (interior): comutare in interior backbone (folosite de ruterele P- pentru rutele interne)
  - bottom label (exterior): transmitere pachete de la egress PE la CE corespunzator (la VPN direct conectat corespunzator)
- nodurile MPLS comuta pe baza top label

# Mecanismul de forward




- **PE ingress primeste pachete IP de la CE pe o anumita interfata**
- **PE analizeaza VRF_B , gaseste PE2 ca next hop, asigneaza stiva de etichete:**
  **eticheta exterior T2 + eticheta interior T8**

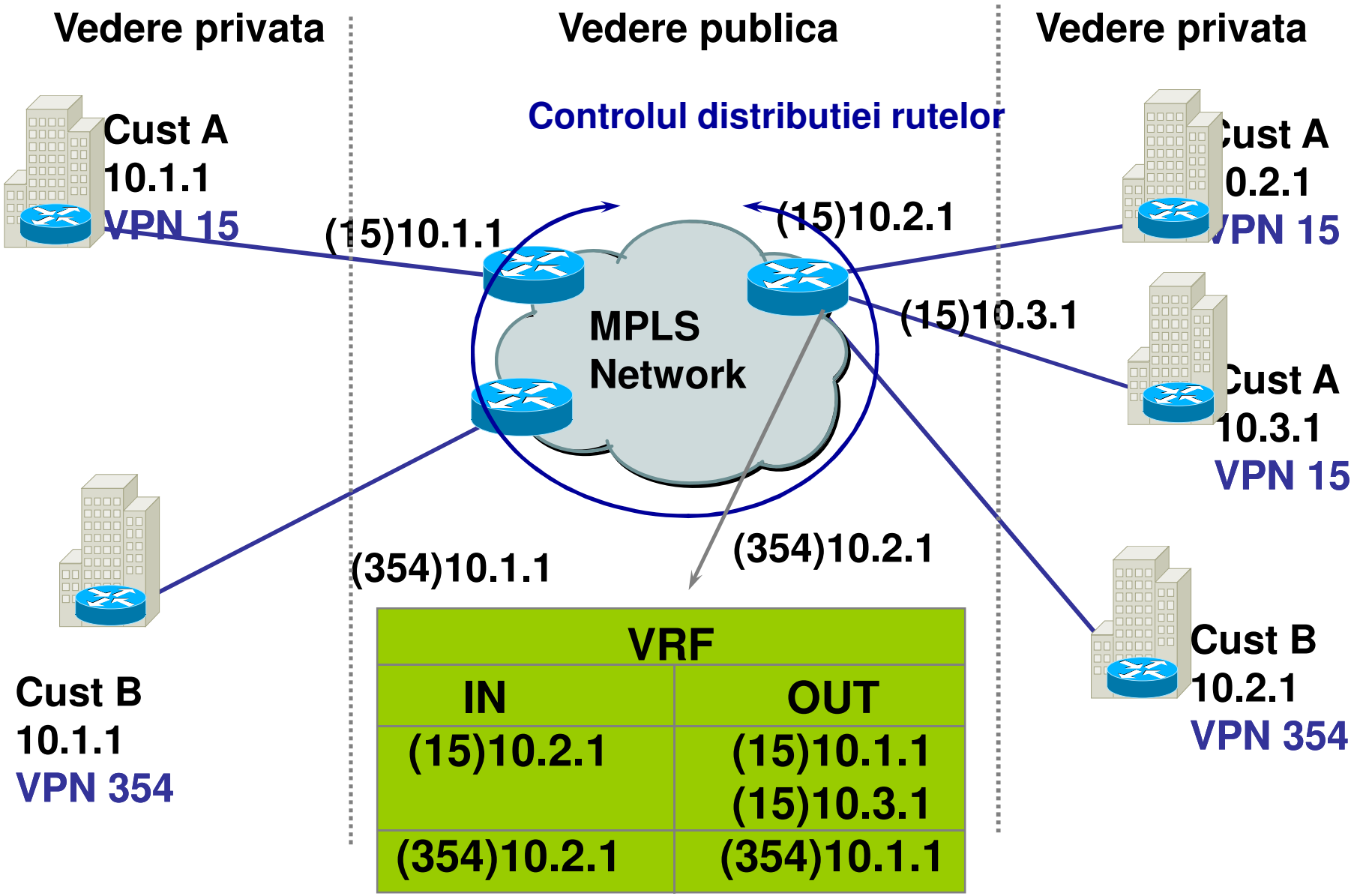
# Mecanismul de forward




- **ruterele P comuta pe baza etichetei interioare**
- **PE egress sterge eticheta interioara**
- **PE utilizeaza eticheta exteriora pentru a decide VPN/CE destinatie**

# Construire MPLS-VPN

- tabele de rutare din retea
- utilizare LDP pentru asignare etichete
- configurare generica rutere PE
- invatare adresa de la rutere CE
- actualizari MP-iBGP
- decizia completarii tabelelor VRF
- comutare pachet in backbone prin MPLS


Vedere privata
Vedere publica
Vedere privata
Controlul distributiei rutelor
Cust A
10.1.1
VPN 15
(15)10.1.1
(15)10.2.1
MPLS
Network
(15)10.3.1
Cust A
0.2.1
VPN 15
Cust A
10.3.1
VPN 15
(354)10.1.1
(354)10.2.1
Cust B
10.1.1
VPN 354
Cust B
10.2.1
VPN 354
VRF
IN
OUT
(15)10.2.1
(15)10.1.1
(15)10.3.1
(354)10.2.1
(354)10.1.1

# Concluzii

- neorientare pe conexiune
- scalabilitate
- securitate
- adresare flexibila
- suport pentru orice tehnologie de acces si backbone
- clase de servicii
- standardizare

# Concluzii

- site nou => configurare PE
- ruterele P nu mentin informatie VPN
- management usor pentru provider