Temă de curs RCI

MPLS (Multiprotocol Label Switching)

Student

Jircu Andrei

Master IISC – anul II

Îndrumător

Conf. Dr. Ing Ştefan Stăncescu

Cuprins

1. Introducere 3

2. MPLS (Multiprotocol Label Switching) 3

2.1. Beneficiile protocolului MPLS în reţea 4

2.2. Concepte de bază MPLS 4

2.3. Cale comutată după etichetă (Label Switched Path – LSP) 5

2.4. LDP (Label Distribution Protocol) 6

2.5. RSVP (Resource Reservation Protocol) 7

2.6. RSVP-TE şi ingineria de trafic 7

3. Algoritmul DORA (Dynamic Online Routing Algorithm) pentru ingineria de trafic MPLS 8

4. MPLS VPN 13

4.1. Reţeaua MPLS VPN folosind IPv6 peste tunelele de IPv4 pe rutere Customer Edge (CE) 15

4.2. Rutarea VPN/instanţa de forward (VRF – Virtual RoutingForwarding) 16

4.3. Crearea unui VRF 18

5. Concluzii 19

6. Bibliografie 20

1. Introducere

În prezent, tehnologiile de transport a informaţiei dezvoltate până acum sunt Frame Relay, PDH (Plesiochronous Digital Hierarchy), SDH (Synchronous Digital Hierarchy), ATM (Asynchronous Transfer Mode), MPLS + IP (Multiprotocol Label Switching + Internet Protocol).

Utilizatorii de reţele locale LAN (Local Area Network) sunt obişnuiţi cu viteza şi fiabilitatea acestor reţele proprii. A existat însă nevoia de a extinde aceste reţele locale peste limitele lor prin servicii precum linii închiriate, ISDN şi Frame Relay pentru a interconecta aceste reţele LAN. Dar utilizatorii se aşteaptă la aceeaşi viteză şi fiabilitate a traficului transmis peste reţelele metropolitane MAN (Metropolitan Area Network) şi WAN (Wide Area Network). Aceste aşteptări pun o presiune foarte mare asupra furnizorilor de servicii şi echipamente pentru a crea dispozitive care leagă aceste tehnologii de comunicaţie într-o reţea fără întreruperi. Nevoia de viteză a reprezentat principala motivaţie pentru dezvoltarea primelor aplicaţii ATM.

2. MPLS (Multiprotocol Label Switching)

Comutarea multiprotocol cu etichete este o tehnologie prin care nodurile terminale adaugă o etichetă la un pachet IP. Etichetele MPLS sunt anunţate între routere, astfel încât acestea să poată construi o tabelă a etichetelor. Aceste etichete sunt ataşate la pachetele IP pentru a permite routerelor să transmită traficul uitându-se doar la etichetă, fără a mai fi necesară adresa de destinaţie. Aceste pachete sunt trimise prin intermediul comutării de etichete şi nu prin comutarea IP.

Această tehnică de comutare a etichetelor nu este nouă. Frame Relay şi ATM folosesc această tehnică pentru a transmite cadrele sau celulele. La Frame Relay, cadrul poate avea orice lungime, pe când la ATM celula are o capacitate maximă de 53 de octeţi (5 octeţi antetul şi 48 de octeţi capacitatea utilă). Asemănarea cu Frame Relay şi ATM este că la fiecare pas prin reţea, valoarea etichetei din antet se schimbă. Acest lucru este diferit faţă de transmisia pachetelor IP. Când un router transmite un pachet IP, acesta nu îşi schimbă adresa IP de destinaţie.

Înainte de MPLS, cele mai populare protocoale WAN (Wide Area Network) erau ATM şi Frame Relay. Pentru că Internetul s-a dezvoltat foarte repede, IP-ul a devenit cel mai folosit protocol, deoarece era pretutindeni. Putem spune că MPLS este un protocol de nivel 2.5, deoarece integrează controlul rutării IP (nivelul 3 OSI), precum şi comutarea la nivelul legăturii de date (nivelul 2 OSI).

2.1. Beneficiile protocolului MPLS în reţea

- Integrare mai bună cu IP decât cu ATM ;
- Reduce complexitatea operaţiilor din reţea ;
- Ingineria traficului ;
- Reduce complexitatea operaţiilor din reţea ;
- Facilitează apariţia de noi posibilităţi de rutare, care îmbunătăţesc tehnicile de rutare existente;

Unul dintre motivele apariţiei unui protocol bazat pe schimbul de etichete a fost nevoia de viteză. Comutarea pachetelor IP pe procesor a fost considerat a fi mai lentă decât comutarea pachetelor etichetate. Un router transmite un pachet IP prin căutarea adresei de destinaţie din antetul IP-ului şi încearcă să găsească cea mai bună potrivire în tabela de dirijare. Cu toate acestea, pentru că adresele IP pot fi unicast, multicast şi au 4 octeţi căutarea poate fi complexă. Prin folosirea protocolului MPLS cu IP putem avea mai multe posibilităţi de a transmite date. Adăugarea etichetelor la pachete permite transmiterea informaţiei şi cu ajutorul altor protocoale precum : IPv4, IPv6, Ethernet, HDLC (High-Level Data Link Control), PPP (Point-to-Point Protocol) şi alte tehnologii ale nivelului 2 OSI.

2.2. Concepte de bază MPLS

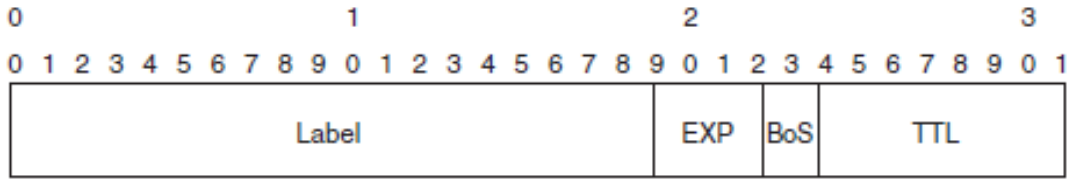

Figura 1 : Structura antetului MPLS

Eticheta (label) este un identificator scurt cu o lungime fixă, care poate fi folosită în asistarea procesului de forwarding (trecerea pachetelor dintr-o reţea în alta). O etichetă MPLS are 32 de octeţi. Primii 20 de octeţi reprezintă valoarea etichetei. Biţii de la 20 la 22 sunt trei biţi experimentali (EXP). Aceşti biţi sunt utilizaţi exclusiv pentru calitatea de serviciu (QoS). Bitul 23 este bitul de stivă (BoS). Stiva reprezintă o colecţie de etichete care se găsesc în partea superioară a pachetului. Stiva poate avea o singură etichetă sau mai multe. Cei 8 biţi rămaşi reprezintă câmpul TTL (Time-To-Live). Acest câmp are aceeaşi semnificaţie care se găseşte şi în antetul IP-ului. Valoarea acestui câmp se decrementează cu 1 la fiecare hop întâlnit în reţea, iar funcţia sa principală este de a evita ca un pachet să rămână blocat într-o buclă de circuit. Dacă o buclă de circuit apare şi acest câmp nu este prezent, atunci pachetul se rutează la infinit ceea ce duce la congestie în reţea. În momentul în care valoarea câmpului TTL ajunge la 0, atunci pachetul este

eliminat din reţea.

Un router de comutare a etichetelor (LSR – label switch router) este un router ce suportă MPLS. Este capabil să înţeleagă etichetele MPLS şi să primească sau să transmită pachete etichetate pe o legătură de date. Există trei tipuri de LSR într-o reţea MPLS :

- LSR de intrare (ingress LSR) – este routerul care are rolul de a încapsula prima dată un pachet şi de a trimite pachetul pe legătura de date.
- LSR de ieşire (egress LSR) - este routerul care primeşte pachetele etichetate, elimină eticheta şi trimite pachetul mai departe pe legătura de date. Routerele LSR de intrare şi ieşire reprezintă routerele de margine ale reţelei.
- LSR intermediar – acest router efectuează doar comutare MPLS pe baza etichetei.[1]

2.3. Cale comutată după etichetă (Label Switched Path – LSP)

Este unul dintre cele mai importante concepte folosite în practică. LSP reprezintă un tunel unidirecţional între două sau mai multe routere, care este dirijat în interiorul unei reţele MPLS. În cazul în care nu există LSP atunci nu putem să avem trafic.

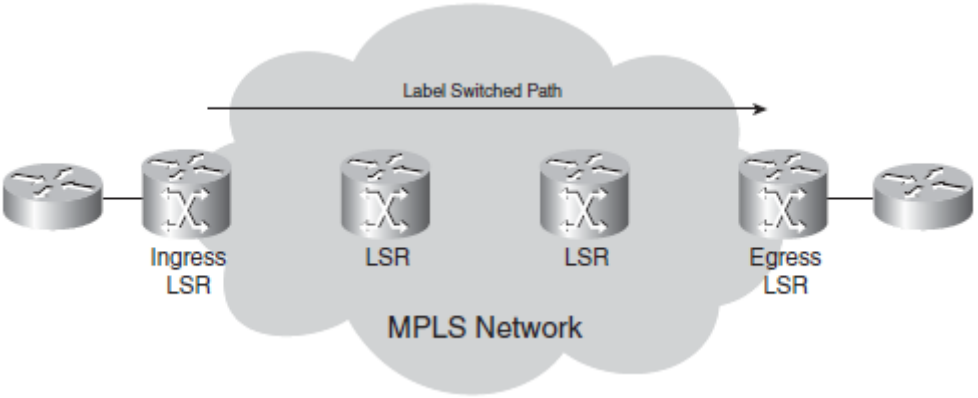

Figura 2 : LSP prin reţeaua MPLS

În figura 2, săgeata reprezintă direcţia, deoarece LSP este un tunel unidirecţional. Fluxul de pachete în cealaltă direcţie, de la dreapta la stânga între cele două routere LSR de margine ar însemna un alt tunel LSP. Se folosesc protocoale de semnalizare MPLS care asociază LSP-ul cu anumite valori ale etichetelor.

Există două protocoale principale de semnalizare pentru MPLS :

- Protocol de distribuţie a etichetelor (LDP – Label Distribution Protocol) este un protocol simplu, care nu suportă ingineria traficului.

- Protocol de rezervare a resurselor cu ingineria traficului (RSVP-TE – Resource Reservation Protocol with Traffic Engineering)

Clasa de dirijare echivalentă (Forward Equivalent Class – FEC) reprezintă un grup de pachete care sunt tratate identic de către LSR. Toate pachetele ce aparţin aceluiaşi FEC au aceeaşi etichetă.. Tratamentul de forwarding poate fi diferit şi pachetele pot aparţine de o alta clasă de dirijare. Routerul caare decide ce pachet aparţine clasei respective este routerul de intrare LSR. Această afirmaţie este logică, deoarece routerul de intrare LSR are rolul de a clasifica şi de a eticheta pachetele.

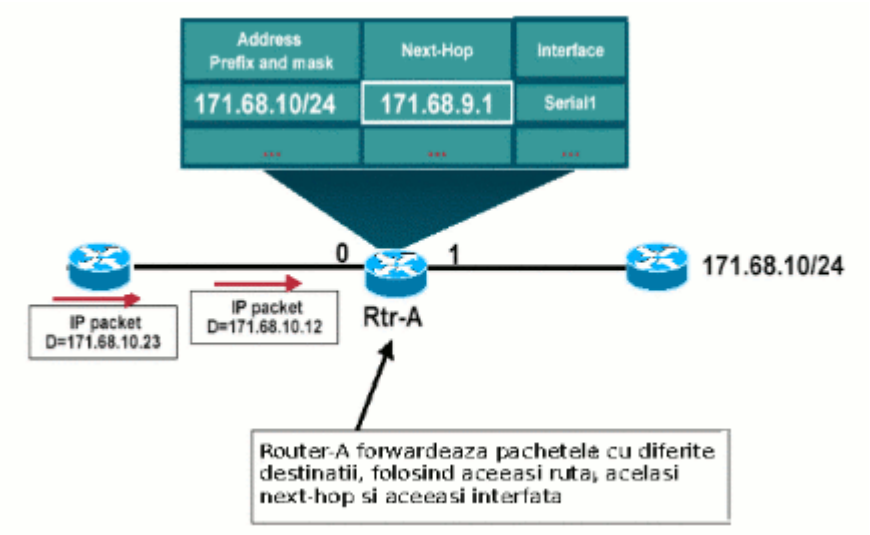

Figura 3 : Forwarding bazat pe FEC

2.4. LDP (Label Distribution Protocol)

LDP este folosit pentru a stabili transportul MPLS atunci când ingineria traficului nu este necesară. LDP poate funcţiona în mai multe moduri pentru a se potrivi cerinţelor. Cu toate acestea, cel mai comun mod de utilizare este modul nesolicitat, care stabileşte o reţea full mesh de tunele între routere.

- În modul solicitat, routerul LSR de intrare trimite o solicitare de etichetă LDP către următorul router. Această cerere este trimisă prin reţea pas cu pas de către fiecare router. Odată ce această cerere ajunge la routerul de ieşire LSR un mesaj de confirmare este generat.
- În modul nesolicitat, routerele de ieşire LSR transmit maparea etichetei pentru fiecare legătură externă la toţi vecinii lor . Aceste transmisii se răspândesc pe fiecare legătură din reţea până când ajung la routerele de intrare LSR.

Avantajul principal al LDP-ului faţă de RSVP este dat de uşurinţa configurării tunelelor full mesh folosind modul nesolicitat.

2.5. RSVP (Resource Reservation Protocol)

Protocolul de rezervare a resurselor este un protocol de nivelul 4 OSI (nivelul transport) conceput pentru a rezerva resurse într-o reţea. Acesta nu transportă date, ci este un protocol de semnalizare asemănător protocolului ICMP (Internet Control Message Protocol) . RSVP poate fi folosit de routere pentru a oferi sau a cere calitate a serviciilor (QoS – Quality of Service). RSVP nu este un protocol de rutare, dar a fost creat pentru a putea opera cu acestea. Acest protocol este foarte rar folosit astăzi în telecomunicaţii, dar extensia acestui protocol cu inginerie de trafic (RSVP – TE) a devenit din ce în ce mai răspândit în foarte multe reţele orientate pe calitatea serviciului.

Atribuţii principale :

- RSVP cere resurse pentru fluxuri de trafic într-o singură direcţie, de la expeditor la unul sau mai mulţi receptori.
- RSVP este orientat pe recepţie în care receptorul care a iniţiat un flux de date menţine rezerva de resurse pentru acest flux.
- Protocolul oferă mai multe posibilităţi de rezervare a resurselor şi permite adăugarea de noi metode de rezervare pentru a se potrivi cu aplicaţiile ce apar.

2.6. RSVP-TE şi ingineria de trafic

Ideea de bază a ingineriei traficului este de a utiliza optim infrastructura de reţea inclusiv legăturile care sunt utilizate insuficient. Asta înseamnă că ingineria traficului trebuie să ofere posibilitatea să redirecţioneze traficul pe diferite căi faţă de calea optimă

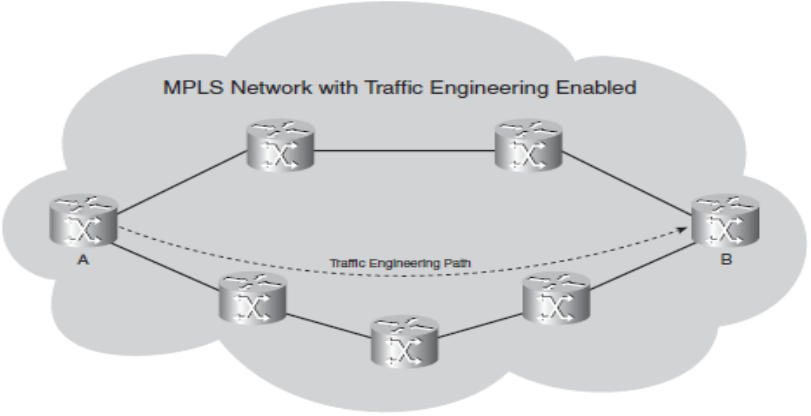

Figura 4 : Reţea MPLS cu inginerie de trafic

Administratorul acestei reţele MPLS cu inginerie de trafic poate redirecţiona traficul de la routerul A la routerul B pe calea de jos chiar dacă această cale nu este cea mai scurtă (4 hop-uri în loc de 3 hop-uri pe calea de sus). Ca atare, se poate trimite traficul şi pe legăturile care sunt mai puţin folosite pentru a elimina cât mai mult congestia reţelei. Traficul poate fi ghidat în această reţea pe calea de jos prin schimbarea unor parametrii de metrică ai protocoalelor de rutare.

Protocolul RSVP-TE este folosit pentru stabilirea transportului LSP în reţeaua MPLS acolo

unde ingineria de trafic este necesară. În principiu este folosit pentru a oferi calitatea serviciului şi de a echilibra încărcarea reţelei. RSVP permite utilizarea de rutare a sursei în cazul în care routerul LSR de intrare determină calea completă prin intermediul reţelei. Acest router poate folosi rutare cu constrângeri, folosind un algoritm de cea mai scurtă cale cu constrângeri (CSPF – Constraint Shortest Path First) pentru a determina calea către destinaţie.[1]

3. Algoritmul DORA (Dynamic Online Routing Algorithm) pentru ingineria de trafic MPLS

Considerăm problema de setare a rutelor de lăţime de bandă într-o reţea MPLS. Fiecare cerere de de configurare a căilor sosesc una câte una şi nu cunoaştem timpul de sosire sau dimensiunea viitoarelor cereri. Dimensiunea unei cereri se referă la cerinţa de lăţime de bandă pentru configurarea unei rute. Pentru fiecare cerere este nevoie de o rută cu lăţime de bandă rezervată pentru a fi configurată între nodul sursă (ingress) şi nodul destinaţie (egress).

Cel mai popular şi folosit algoritm în MPLS este SPF (Shortest path first). Acesta selectează ruta ce conţine cele mai puţine hop-uri între nodul sursă şi nodul destinaţie. O problemă evidentă cu SPF este că are tendinţa să ruteze traficul pe acelaşi set de link-uri până când aceste link-uri devin saturate. De regulă, SPF acceptă mai puţine configurări de rute într-o reţea decât alţi algoritmi mult mai avansaţi.

Algoritmul MIRA are rolul de a accepta câte rute poate suporta reţeaua folosind conceptul de legături critice. Proprietatea legăturilor critice este că atunci când capacitatea lor este redusă cu o unitate de bandă, fluxul de date maxim între nodurile sursă şi destinaţie este de asemenea redus cu o unitate de bandă. Scopul algoritmului este de a selecta rute ce conţin cât mai puţine legături critice posibile.

Algoritmul DORA este separat în două etape. Prima etapă este executată de fiecare dată când are loc o schimbare a topologiei, iar a doua etapă este executată ori de cate ori apare o cerere de setare a unei căi (path setup).

În prima etapă, operaţiunea cheie este de a atribui valoarea potenţială a căii PPV (Path potential value) la fiecare legătură cu privire la fiecare pereche sursă-destinaţie. PPV reflectă probabilitatea ca o anumită legătură să facă parte dintr-o potenţială pereche sursă-destinaţie din reţea. O valoare mare a legăturii PPV implică faptul că această legătură va fi probabil o parte din mai multe rute potenţiale şi astfel rutarea peste această legătură ar trebui să fie evitată ori de câte ori este posibil. O valoare mică a legăturii PPV înseamnă că există mai puţine rute potenţiale de a folosi această legătură şi prin urmare este de preferat să se folosească această legătură decât altele cu PPV mai mare. Fiecare sursă-destinaţie (S,D) este asociată cu o matrice PPV (S,D) de mărime egală cu numărul de link-uri din reţea şi fiecare element din matrice este iniţializat cu zero. Modul prin care elementele din matrice sunt calculate se bazează pe link-urile care sunt incluse în setul disjunct de rute pentru fiecare pereche sursă-destinaţie şi este descris în detaliu în lista de pseudocod pentru DORA.[3]

Etapa 1 :

1. Pentru fiecare pereche sursă-destinaţie (S,D) determinăm setul de rute disjuncte DP (S,D). O modalitate este de a folosi algoritmul lui Dijsktra pentru a găsi calea cea mai scurtă (numărul de hop-uri) pentru (S,D) , adăugăm această rută lui DP (S,D), apoi ştergem toate legăturile care fac parte din ruta rezultată şi repetăm aceşti paşi până când D nu mai este accesibil din S.

2. Pentru perechea sursă-destinaţie (S1,D1) construim matricea PPV (S1,D1) şi iniţializăm toate intrările cu zero. Dimensiunea matricei este egală cu numărul de link-uri din reţea.

3. Pentru fiecare pereche sursă-destinaţie (S1,D1) :
   a) Verificăm fiecare legătură din reţea şi dacă un link L face parte din orice cale în DP (S1,D1) scădem 1 din PPV(S1,D1)(L).
   b) Pentru toate perechile sursă-destinaţie altele decât (S1,D1) verificăm fiecare link L şi determinăm timpii X în care L apare în DP (S,D) , unde (S,D) nu este egal cu (S1,D1). Incrementăm PPV (S,D) cu X.

4. Pentru fiecare pereche sursă-destinaţie (S,D) normalizăm toate intrările în PPV (S,D) cu cel mai mic element PPV pe toate perechile sursă-destinaţie egale cu zero şi cel mai are element PPV pe toate perechile sursă-destinaţie egale cu 100.

Etapa 2 :

1. Să presupunem că o cerere ajunge pentru configurarea rutei între (S1,D1) cu Y lăţime de bandă. Eliminăm legăturile cu lăţime de bandă reziduală.

2. Pentru fiecare link de reţea L determinăm lăţimea de bandă reziduală RB(L), normalizăm RB(L) -1 pentru intervalul de la 0 la 100, cu cel mai mic RB(L) -1 egal cu 0 şi cel mai mare RB(L) -1 egal cu 100.

3. Pentru perechea sursă-destinaţie (S1,D1) construim o tabelă LWT (S1,D1) şi folosim ecuaţia ca să obţinem LWT(S1,D1)(L) :

$$LWT\ (S1,D1)(L) = NPPV\ (S,D) * (1 - BWP) + NRB(L) * BWP$$

4. Folosim algoritmul lui Dijkstra pentru a calcula optimizarea rutei între (S1,D1).

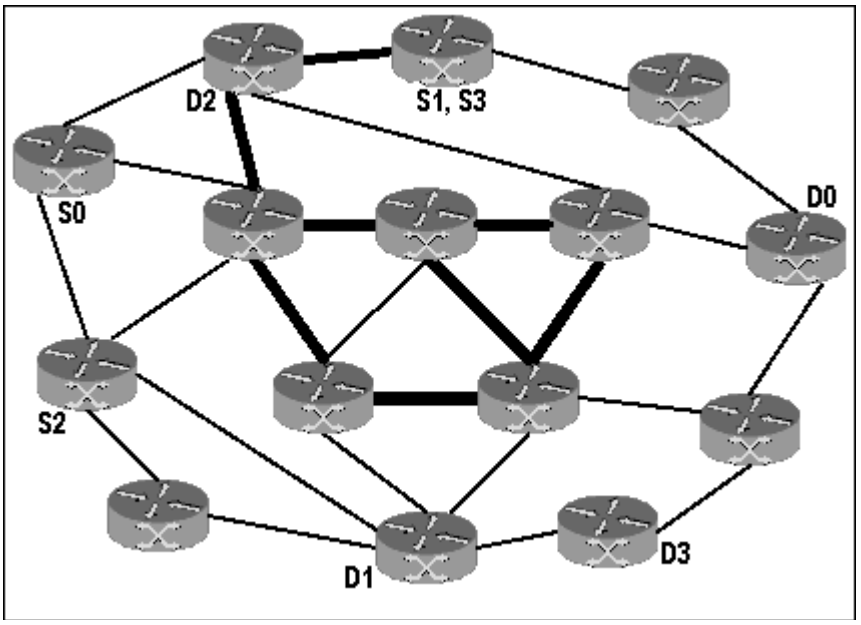

Figura 5 :Topologia reţelei folosită în experimente. Liniile groase reprezintă link-uri de 48 MB de lăţime de bandă rezervabilă, iar liniile subţiri sunt link-uri de 12 MB.

Figura arată 4 perechi de sursă-destinaţie identificate de (S0,D0), (S1,D1), (S2,D2) şi (S3,D3).

Trei experimente sunt luate în considerare. Primele 2 experimente se bazează pe rata de rejectare a rutei, care indică setup-urile de rute care sunt rejectate din cauza lipsei de resurse. Ultimul experiment studiază comportamentul algoritmului când anumite link-uri cedează. Fiecare cerere este distribuită uniform 10 KB, 20 KB, 30 KB şi 40 KB.

În primul experiment sunt trimise 2000 de cereri statice către reţea. Rutele statice se aseamănă cu tuneluri de lungă durată MPLS, odată stabilite acestea rămân permanent în reţea.

În al doilea experiment încărcăm reţeaua cu 200 de de cereri de rute statice şi apoi trimitem 1800 de cereri dinamice. Rutele dinamice reprezintă tunelele de scurtă durată MPLS. Timpul de sosire în reţea a cererilor de rute dinamice este bazat pe distribuţia Poisson cu media λ = 40 cereri/diviziune de timp şi fiecare rută dinamică are un timp de aşteptare pe o distribuţie exponenţială cu media μ =10 unităţi de timp. Configurarea experimentului 3 este la fel ca şi cu experimentul 1 cu o mică adăugare, se alege un link aleator care va fi dat jos înainte ca resursele reţelei să fie saturate. Numărul de rute necesar pentru rerutare şi procentajul rerutărilor efectuate cu succes sunt înregistrate după ce un link este căzut.

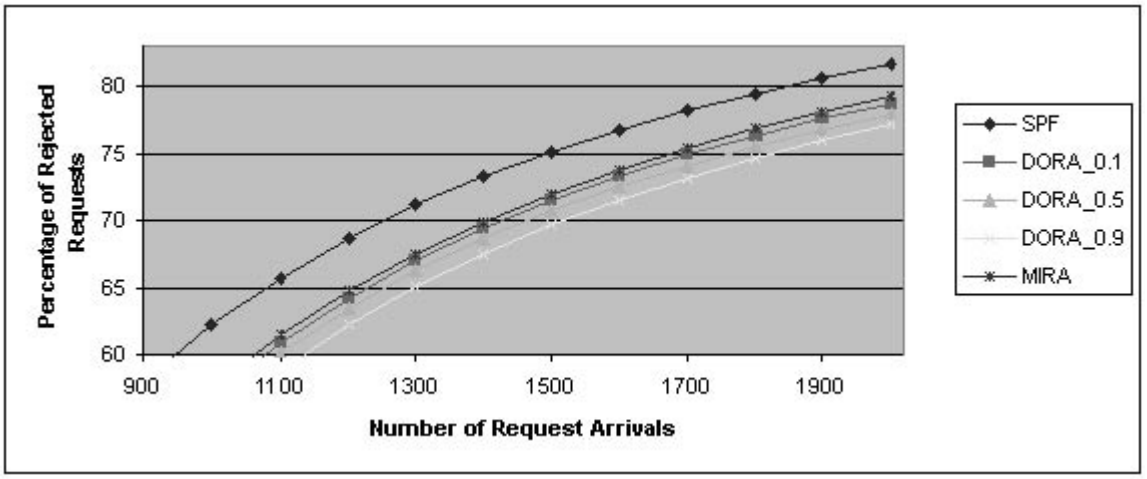

Figura 6 : Configurarea rutelor statice (Experiment 1) : Procentajul de cereri rejectate de la numărul 850 la 2000

Figura arată rezultatul partial pentru experimentul 1, care implică doar rute statice. Conform cu figura, DORA_0.9 (DORA cu BWP = 0.9) rejectează cele mai puţine cereri, urmat de DORA_0.5, Dora_0.1, MIRA şi SPF (Shortest Path First). Rezultatul înainte de cererea 850 este similară. Pentru că rutele statice rămân configurate în reţea permanent, după ce toate resursele sunt consumate, orice cerere ce soseşte va fi rejectată. Acest lucru poate fi observat prin faptul că toate curbele din figură se apropie de 100 % pe măsură ce numărul de cereri creşte.

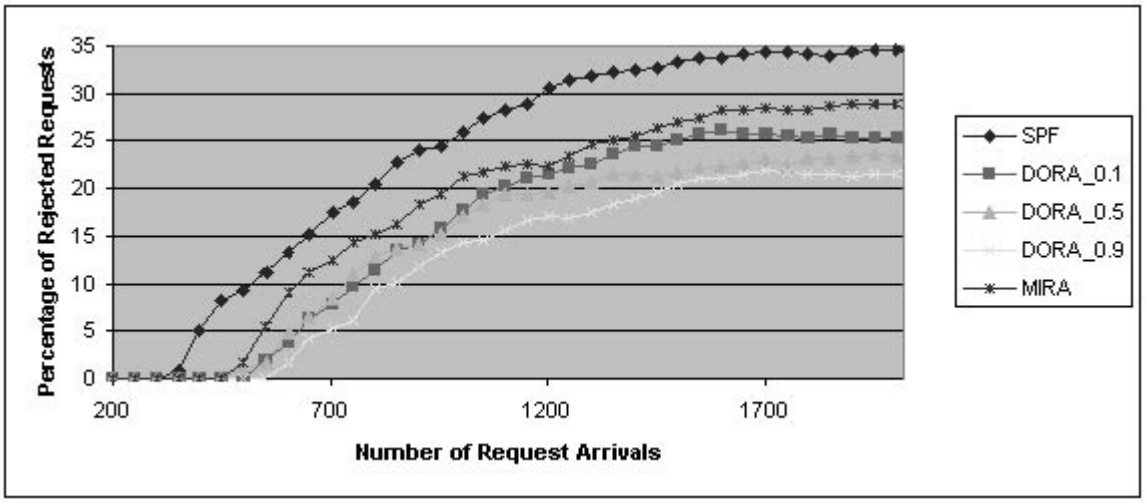

Figura 7 : Configurarea rutelor statice-dinamice (Experiment 2) : Procentajul de cereri rejectate

Rezultatul experimentului 2 ce implică şi cereri de rute statice si dinamice este reprezentat în figura 7 . Toate curbele cresc neregulat până la cererea cu numărul 1800, unde curbele intră într-o stare constantă. Asemănător cu experimentul anterior, DORA_0.9 rejectează procentajul cel mai mic de cereri, urmat de DORA_0.5, DORA_0.1, Mira şi SPF. În perioada constantă, DORA_0.9 rejectează 26 % mai puţine cereri decât MIRA, iar DORA_0.1 arată o îmbunătăţire de 12 % la numărul de cereri rejectate faţă de MIRA.

Experimentul 3 este echivalent cu primul excepţie fiind faptul că la diferite momente de timp, un link aleator este oprit iar numărul de rute ce au nevoie de rerutare şi procentajul acestora este înregistrat.

În primul experiment, condiţia unde toate cererile sunt rejectate din cauza resurselor insuficiente are loc în momentul în care peste 30% din capacitatea reţelei este ocupată. Definim punctele A,B şi C să fie cazul unde 20%, 25%, 30% din capacitatea totală a reţelei a fost saturată. Este un total de 26 de link-uri de reţea ce sunt folosite în 390 de încercări experimentale. La fiecare punct de cădere a link-ului (A,B şi C), calculăm numărul de rute necesare pentru rerutare şi procentajul rerutărilor cu succes. Rezultatele sunt în figurile următoare.

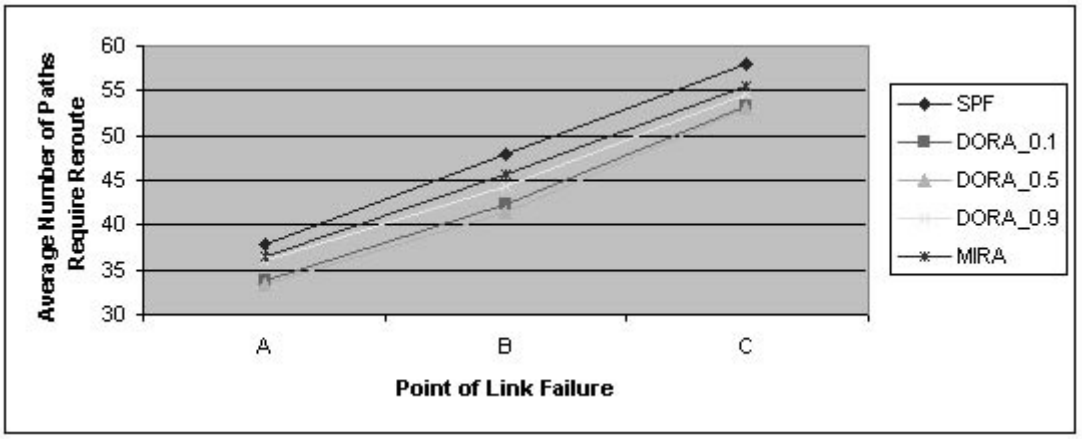

Figura 8 : Media numărului de rute necesare pentru rerutare în diferite puncte de cădere a link-ului

Figura arată media creşterii numărului de rute necesare pe măsură ce resursele reţelei sunt aproape de saturaţie. DORA_0.5 necesită cele mai puţine rute pentru se realiza rerutarea în cazul unei căderi a unui link, urmat de DORA_0.1, DORA_0.9, MIRA şi în final SPF. Valoarea de deviaţie standard pentru numărul de rute necesar rerutării este o indicaţie directă a abilităţii algoritmului de împărţire a rutelor de-a lungul reţelei.

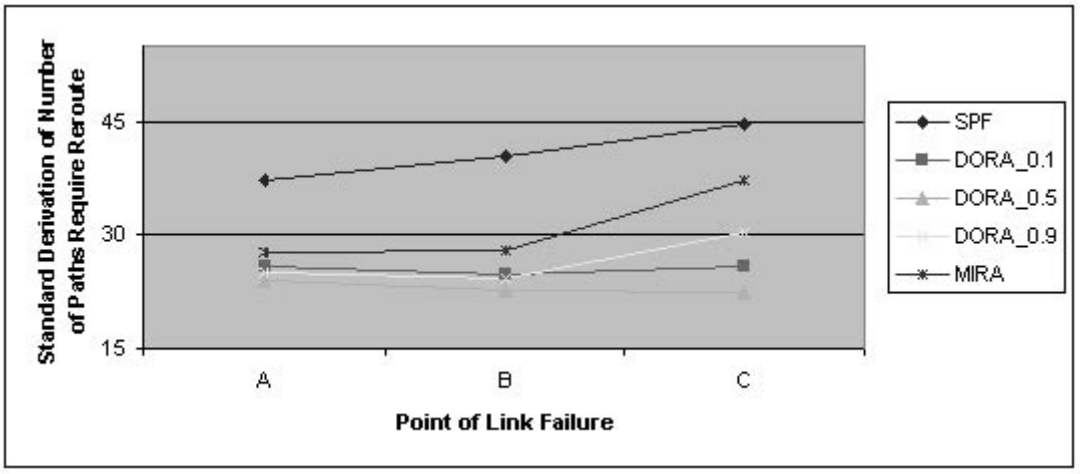

Figura 9 : Numărul de deviaţii standard a rutelor necesare rerutării la puncte diferite de căderea link-ului

Figura arată că DORA_0.5 are valoarea cea mai mică de deviaţie standard ceea ce înseamnă că este cel mai capabil de a împărţi rute de-a lungul reţelei.

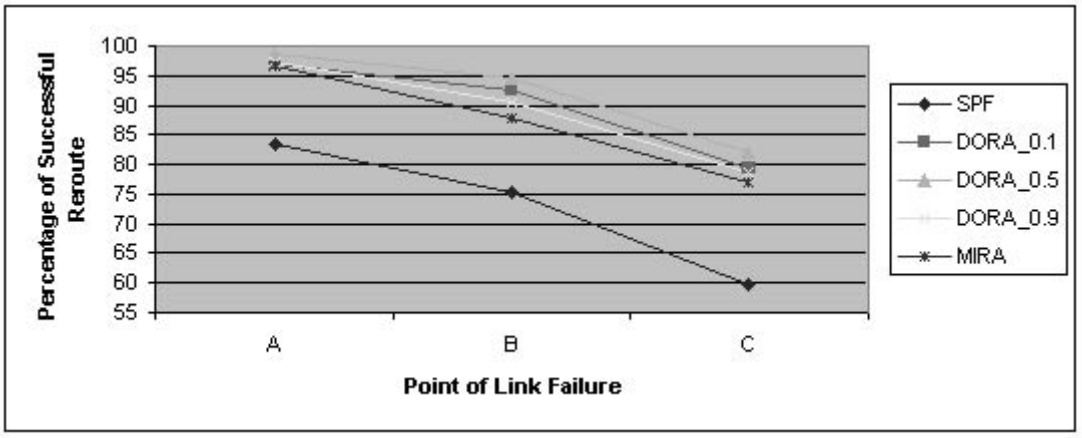

Figura 10 : Procentajul rerutărilor cu succes la diferite puncte de cădere a link-ului

Figura arată procentajul rerutărilor cu succes în cazul căderii unui link. Conform cu figura, curba descreşte pentru toţi algoritmii, pe măsură ce resursele reţelei sunt mai aproape de saturaţie. DORA_0.5 este cel mai bun algoritm cu procentajul cel mai mare de rerutări efectuate cu succes, urmat de DORA_0.9, Dora_0.1, MIRA şi SPF. Dora_0.5 este capabil să obţină aproximativ 2%, 7.9% şi 6,5% mai multe rerutări cu succes decât MIRA.

Algoritmul DORA (Dynamic Online Routing Algorithm) este un algoritm ce calculează lăţimile de bandă a rutelor garantate în reţeaua MPLS. În evaluarea performanţei am arătat că DORA rejectează mai puţine rute decât SPF şi MIRA. Mai mult decât atât, DORA obţine un procentaj mai mare de rerutări efectuate cu succes spre deosebire de SPF şi MIRA. Costul etapei 1 poate fi redus dacă se foloseşte o schemă de calcul mai bună a rutelor disjuncte pentru perechile sursă-destinaţie.[4]

4. MPLS VPN

MPLS VPN este cea mai răspândită implementare a tehnologiei MPLS. Popularitatea sa a crescut exponenţial de când s-a inventat şi este în continuă creştere. Deşi cei mai mulţi furnizori de servicii folosesc această tehnologie drept înlocuiriea serviciilor de Frame Relay şi ATM, MPLS VPN este acum un interes şi pentru marile întreprinderi. MPLS VPN poate oferi scalabilitate şi posibilitatea de a împărţi reţeaua în reţele mai mici separate, care sunt de multe ori necesare în reţelele mari ale unei organizaţii pentru a oferi reţele separate diferitelor departamente. Mulţi furnizori de servicii care folosesc această tehnologie de câţiva ani sunt interesaţi de a interconecta propria reţea cu o altă reţea MPLS VPN a unui alt furnizor de servicii pentru a îmbunătăţi scalabilitatea şi uşurinţa de funcţionare a reţelei.

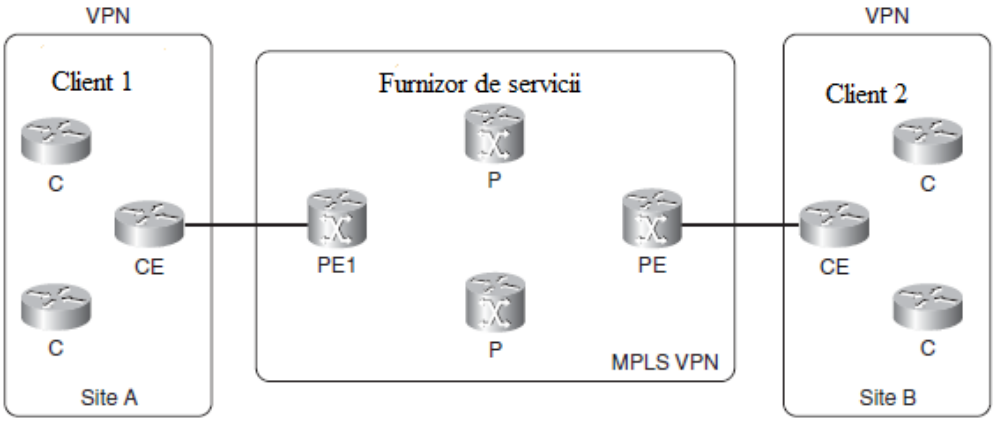

Figura 11 : Schema generală MPLS VPN

Routerul PE este un router de graniţă al furnizorului (PE – Provider edge). Are o legătură directă cu routerul de graniţă al clientului (CE – Customer edge) la nivelul 3 OSI (nivel reţea). Routerul P (Provider) este un router care nu are nicio legătură directă cu routerele clientului. În implementarea MPLS VPN, routerele P şi PE folosesc MPLS. Aceste routere trebuie să fie capabile să-şi distribuie etichetele între ele şi să transmită mai departe pachete etichetate. Un router CE are o legătură directă cu un router PE la nivelul 3 OSI. Un router de client C este un router fără o conexiune directă cu routerul PE. Acest router nu are nevoie să folosească MPLS. Pentru că routerele CE şi PE interacţionează la nivelul 3 OSI, acestea trebuie să folosească un protocol de rutare (sau rutare statică) între ele. Routerul CE are un singur peer (echivalent) în afara reţelei sale, şi anume routerul PE.

Clienţii unui furnizor de servicii au voie să aibe propria lor adresă IP. Clienţii pot folosi adrese IP înregistrate sau adrese IP private. Asta înseamnă că toate routerele P şi PE trebuie să aibă o tabelă de dirijare a fiecărui client. Singurul protocol care este capabil să formeze o tabelă cu un număr foarte mare de clienţi este BGP (Border Gateway Protocol). Toate routerele P şi PE trebuie să folosească o variantă internă a protocolului BGP (iBGP) între ele. Acest protocol are rolul de a menţine o tabelă cu reţelele IP, care arată calea folosită pentru a ajunge la reţeaua dorită prin diferite sisteme autonome (AS). Când acest protocol este rulat în interiorul unui sistem autonom, este folosit termenul de iBGP.

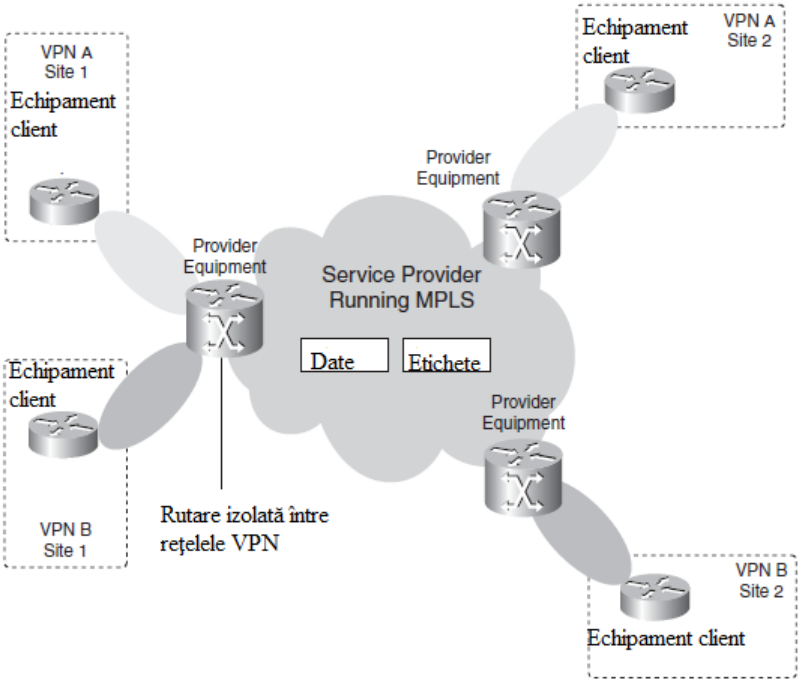

Figura 12 : Model MPLS VPN

Figura 12 arată un model de MPLS VPN: comutarea pachetelor etichetate în reţeaua furnizorului de servicii şi routerele PE ce cunosc tehnologia VPN. Pentru a realiza MPLS VPN este nevoie de construcţia unor blocuri : VRF, distingerea rutei (RD – route distinguisher), ţintele rutei (RT – route targets), dezvoltarea rutei prin MP-BGP şi transmisia pachetelor etichetate.[2]

4.1. Reţeaua MPLS VPN folosind IPv6 peste tunelele de IPv4 pe rutere Customer Edge (CE)

MPLS VPN pentru IPv4 a fost un mare succes. Mulţi furnizori de servicii folosesc MPLS VPN în reţeaua lor. Daca se doreşte să se transporte IPv6 peste reţeaua de nucleu MPLS VPN, ruterele Customer Edge trebuie să poată rula IPv6. Daca ruterele CE rulează în dual-stack – ceea ce înseamnă că pot transporta şi IPv4 şi IPv6 rezultă că se pot implementa tunele între ruterele de tip CE pentru a transporta trafic de IPv6. Transportul de IPv6 peste reţeaua MPLS VPN este o idee interesantă, pentru că nu trebuie să fie făcută nicio modificare în reţeaua MPLS, dar există şi un dezavantaj. Dezavantajul este că tunelele create dintre ruterele CE nu pot transporta IPv6 peste reţeaua MPLS VPN foarte eficient.

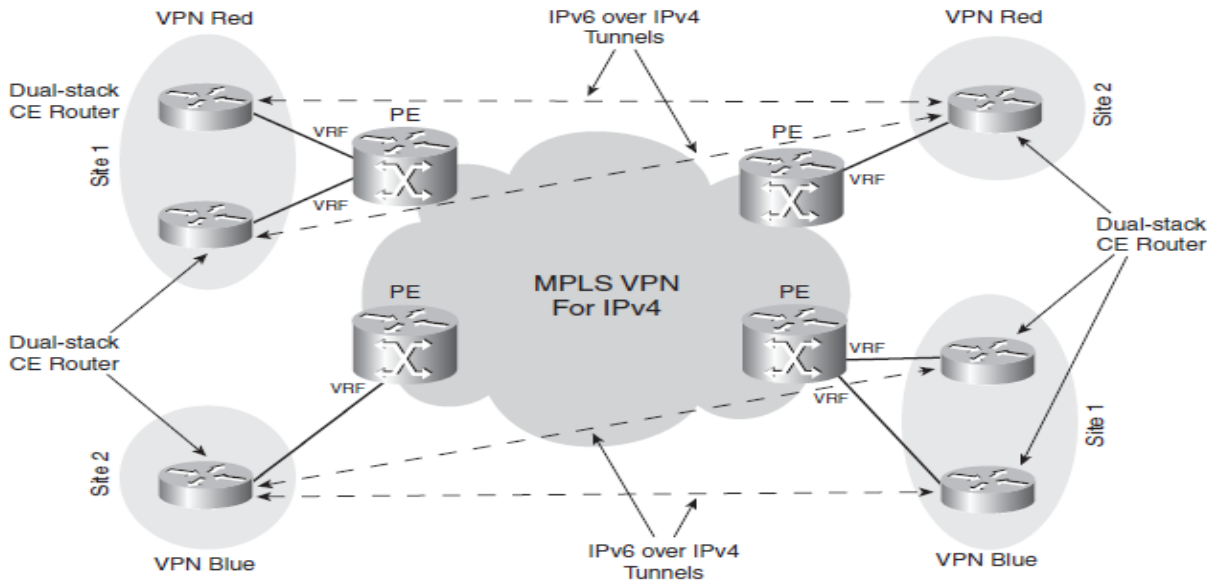

Figura 13:Reţea MPLS VPN ce transportă IPv6 peste tunele de IPv4

Figura de mai sus arată o reţea MPLS VPN pentru reţea IPv4 cu rutere Customer Edge ce folosesc tunele între ele pentru a transporta traficul de IPv6 în reţeaua de nucleu MPLS. [1]

4.2. Rutarea VPN/instanţa de forward (VRF – Virtual RoutingForwarding)

Acest nume provine din combinaţia de tabelă VRF Cisco Express Forwarding sau tabela CEF şi protocoalele de rutare IP asociate routerului PE. Routerul PE are o instanţă VRF pentru fiecare VPN ataşat. Figura 7 arată un router PE ce conţine tabela de rutare IP globală, dar şi o tabelă de rutare VRF pentru fiecare VPN conectat la routerul PE. Pentru că rutarea ar trebui să fie privată şi separată pentru fiecare client VPN în parte, fiecare VPN trebuie să aibe propria lui tabelă de rutare.

Această tabelă de rutare privată se numeşte o tabelă VRF. Interfaţa de la un router PE către un router CE poate aparţine unui singur VRF. De asemenea, toate pachetele IP primite pe acea interfaţă VRF aparţin acelui VRF. Pentru că există câte o tabelă VRF separată există şi o tabelă CEF separată per VPN pentru a transmite pachetele către routerul PE. Apoi routerul PE creează automat o tabelă VRF şi o tabelă CEF. Tabela de dirijare VRF nu diferă cu nimic faţă de o tabelă normală de dirijare, doar că este folosită exclusiv pentru tehnologia VPN şi este complet separată faţă de celelalte tabele de rutare. Tabela CEF este singura modalitate de comutare a pachetelor IP de pe o interfaţă VRF. CEF trebuie să fie activată global pe toate routerele PE şi toate interfeţele VRF din reţea.

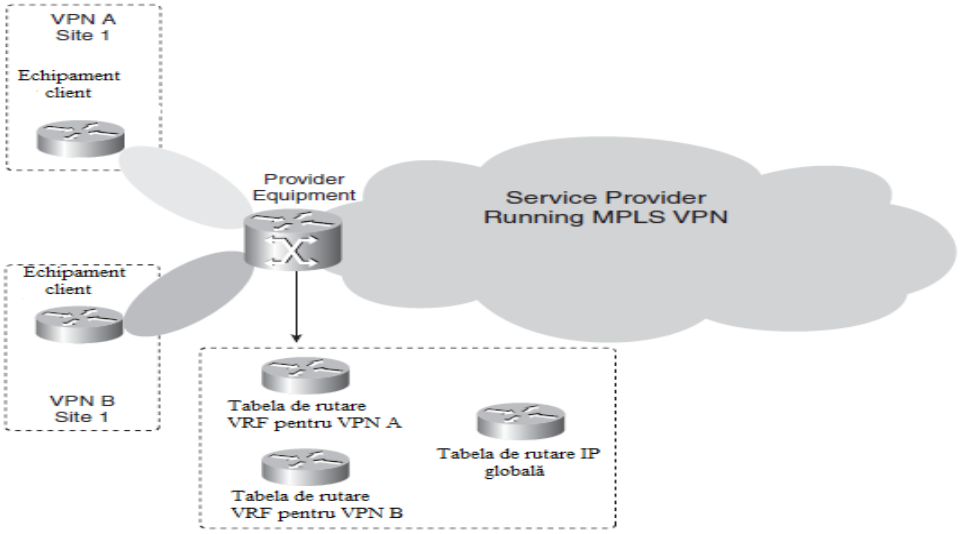

Figura 14 : VRF pe un router PE

Prefixele VPN sunt distribuite în reţeaua MPLS VPN de către multiprotocolul BGP (MP-BGP). Când BGP transmite prefixele IPv4 prin reţeaua furnizorului acestea trebuie să fie unice. În cazul în care clienţii au o suprapunere de adrese IP, rutarea nu se va face cum trebuie. Pentru a rezolva această problemă, s-a creat conceptul de RD (Route distinguisher) pentru a face prefixele IPv4 unice. Ideea de bază este că fiecare prefix al unui client primeşte o identificare unică (RD) pentru a distinge acelaşi prefix al unui alt utilizator. Un prefix derivat din combinaţia unui prefix IPv4 şi RD se numeşte prefix vpnv4. Protocolul MP-BGP trebuie să transmită aceste prefixe vpnv4 între routerele PE. RD este un câmp de 64 de biţi. Fiecare instanţă VRF pe routerul PE trebuie să aibă un RD asignat. Această valoare pe 64 de bitţi poate avea două formate: ASN: nn sau IP-address: nn, unde nn reprezintă numărul. Cel mai folosit format este ASN: nn, unde ASN reprezintă numărul de sistem autonom (ASN – Autonomous System number). Prefixul vpnv4 are o lungime de 96 de biţi, dată de lungimea adresei IPv4 (32 de biţi) şi de câmpul RD (64 de biţi). Masca are aceeaşi lungime ca şi masca de IPv4, adică 32 de biţi. De exemplu dacă folosim un prefix Ipv4 10.1.1.0/24 şi un RD 1:1, prefixul vpnv4 devine 1:1:10.1.1.0/24. Dacă RD s-a folosit doar pentru a identifica VPN-ul, comunicarea dintre diferite VPN-uri ar fi dificilă. Această comunicare este controlată de o altă caracteristică numită RT (Route targets). RT este o comunitate extinsă BGP care indică ce rute trebuie să fie importate din MP-BGP în VRF. Routerele P nu pot transmite pachetele mai departe, pentru că nu au informaţia VRF din fiecare site. MPLS poate rezolva această problemă prin etichetarea pachetelor. După procesul de etichetare, routerele P trebuie să aibă informaţii despre eticheta potrivită pentru a transmite pachetul. Modul cel mai comun este de a configura protocolul LDP (Label Distribution Protocol) între routerele P şi PE pentru ca tot traficul IP să fie etichetat. Se poate folosi şi extensia protocolului RSVP cu inginerie de trafic (RSVP-TE) când se implementează MPLS cu inginerie de trafic. Pachetele IP încapsulate cu etichetă sunt apoi transmise de la routerul de intrare PE către routerul de ieşire PE. Astfel, un router P nu trebuie să verifice niciodată adresa IP de destinaţie. Aceasta este metoda prin care sunt comutate pachetele între cele două tipuri de routere PE. Eticheta se numeşte etichetă IGP pentru că este eticheta care este legată de prefixul IPv4 în tabela globală de rutare al routerelor P şi PE. [2]

Un VRF se alcătuieşte dintr-o tabela de rutare IP, o tabelă derivate de forward şi un set de interfeţe care utilizează tabela de forward precum şi un set de reguli şi protocoale de rutare care determină ce pachete urmează să intre în tabela de forward. De regulă un VRF include informaţia de rutare care defineşte locaţia VPN a clientului care este ataşată ruterului PE.

Routerele PE menţin două tabele de rutare separate :

- Tabela globală de rutare care conţine rutele P şi PE
- Tabelele de rutare şi forwardare asociate cu unul sau mai multe locaţii conectate (rutere CE). VRF-ul este asociat cu orice tip de interfaţă fizică sau logică. Interfeţeşe pot împărţi acelaşi VRF dacă locaţiile conectate folosesc aceeaşi informaţie de rutare.
-

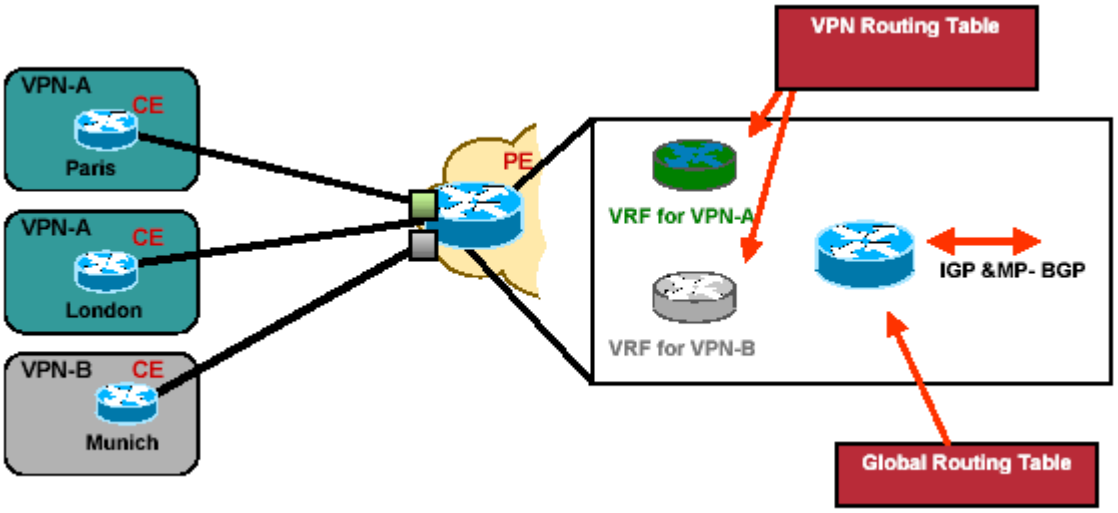

Figura 15 :Rute multiple şi instanţe de forwardare

4.3. Crearea unui VRF

```
pe-nyc(config)#ip vrf red
pe-nyc(config-vrf)# description VRF-RED

pe-nyc(config)#interface serial1/0/2
pe-nyc(config-if)# ip vrf forwarding red
% Interface Serial1/0/2 IP address 10.101.0.2 removed due to
 enabling VRF red
```

5. Concluzii

Tehnologia MPLS IP combină capacităţile de comutare ale etichetei şi noţiunea de circuit virtual specific ATM. Avantajul principal al protocolului MPLS este flexibilitatea de a funcţiona într-un mediu cu protocoale multiple de rutare.. Un alt avantaj îl reprezintă posibilitatea de a realiza ingineria traficului în reţea. Ingineria traficului asigură că datele sunt transmise în reţea eficient şi sigur în acelaşi timp. În momentul de faţă acest protocol stă la baza implementării reţelelor private VPN. De aceea foarte multe organizaţii doresc implementarea reţelelor private bazate pe protocolul MPLS.

În telecomunicaţii tehnologia MPLS IP este implementată în majoritatea reţelelor mai ales în arhitectura 4G a operatorilor de telecomunicaţii şi se dovedeşte a fi un succes având în vedere stabilitatea reţelei şi mai ales viteza de transfer a datelor prin care smartphone-urile din ziua de astăzi folosesc Internetul la o viteză mult superioară faţă de reţeaua 3G în care tehnologia ATM a fost implementată iniţial.

6. Bibliografie

[1] Luc De Ghein, CCIE : MPLS Fundamentals cap 1 - 7, 2007 Cisco Systems Inc, Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA, ISBN 1-58705-197-4.

[2] MPLS and VPN Architectures, Volume II – Jim Guichard, Ivan Pepelnjak, Jeff Apcar , June 06, 2003, ISBN : 1-58705-112-5.

[3] Dynamic Online Routing Algorithm for MPLS Traffic EngineeringW. Szeto, R.Boutaba and Y.Iraqi – Department of Computer Science, University of Waterloo, 200 Univeristy Avenue West, Waterloo, ON, Canada, N2L 3G

[4] Multiprotocol label switching architecture. RFC3031, 2001