Universitatea Politehnica București

Facultatea de Electronică, Telecomunicații și Tehnologia Informației

**Funcții oferite de tehnologia MPLS**

**Aflorei Victor**

**Pâsoi Mihai**

**Jircu Andrei**

Grupa: 441A Coordonator științific:

 Conf. Dr. Ing. **Ștefan Stăncescu**

**2014**

Contents

[1.MPLS VPN – Pâsoi Mihai 441A 3](#_Toc379145526)

[1.1 Introducere 3](#_Toc379145527)

[1.2. MPLS VPN (Multiprotocol Label Switching Virtual Private Network) 4](#_Toc379145528)

[1.3. Virtual Routing Forwarding 5](#_Toc379145529)

[1.4. Transmiterea de pachete într-o rețea MPLS VPN (Port Forwarding) 7](#_Toc379145530)

[1.5. Accesul la internet prin VPN 8](#_Toc379145531)

[2. MPLS Traffic Engineering -TE-Ingineria traficului Aflorei Victor - 441A 10](#_Toc379145532)

[2.1. Necesitatea folosirii MPLS TE 10](#_Toc379145533)

[2.2. Functionarea MPLS TE 14](#_Toc379145534)

[2.3. Distributia informatiei TE 15](#_Toc379145535)

[2.4. Rutarea si costul TE 17](#_Toc379145536)

[2.5. Forwarding Traffic in tunelele MPLS TE 18](#_Toc379145537)

[3. IPv6 peste MPLS – Jircu Andrei 441A 19](#_Toc379145538)

[3.1. Protocolul IPv6 19](#_Toc379145539)

[3.2 Adresarea IPv6 21](#_Toc379145540)

[3.3. Reteaua MPLS VPN folosind IPv6 peste tunelele de IPv4 pe rutere Customer Edge (CE) 21](#_Toc379145541)

[3.4. Transportul IPv6 peste reteaua de nucleu MPLS (6PE-Provider Edge Router) 22](#_Toc379145542)

[4. Bibliografie 25](#_Toc379145543)

# 1.MPLS VPN – Pâsoi Mihai 441A

## 1.1 Introducere

MPLS (Multiprotocol Label Switching)

Multiprotocol Label Switching (MPLS) este un mecanism în rețelele de telecomunicații de înaltă performanță, care directionează date de la un nod de rețea la altul bazată pe etichete de drum scurt, în locul adreselor de rețea lungi, evitând căutări complexe într-un tabel de rutare. Etichetele identifica link-uri virtuale (căi) între noduri la distantă. MPLS poate îngloba pachete de diferite protocoale de rețea. Suportă o gamă largă de tehnologii de acces, inclusiv T1/E1, ATM, Frame Relay și DSL.

Etichetele MPLS sunt folosite între routere, astfel încât acestea să poată construi o cartografiere label-la-eticheta. Aceste etichete sunt atașate la pachetele IP, permitând routerelor să transmită traficul uitandu-se la etichetă și nu la adresa IP destinație. Pachetele sunt transmise prin comutare de etichetă în loc de comutare de IP.

Tehnica de comutare de etichetă nu este nouă. Frame Relay și ATM o utilizează pentru a muta cadre sau celule de-a lungul unei rețele. În Frame Relay , cadrul poate fi de orice lungime, în timp ce în ATM , celulă de lungime fixă constă dintr-un antet de 5 octeți și o sarcină utilă de 48 octeti. Antetul celulei ATM și cadrul Frame Relay referă la circuitul virtual în care celula sau cadrul se află. Similitudinea dintre Frame Relay și ATM este că la fiecare hop prin întreaga rețea, valoarea " etichetei " în antet se schimbă. Acest lucru este diferit față de transmiterea de pachete IP. Când un router transmite un pachet IP, nu se schimbă valoarea care se referă la destinația de pachete, adică , nu se schimbă adresa IP de destinație a pachetului. Faptul că etichetele MPLS sunt utilizate pentru a transmite pachetele și nu adresa IP destinație au condus la popularitatea MPLS-ului. [1]

Beneficiile MPLS

Aici sunt enumerate câteva din beneficiile de a rula MPLS în rețea. Aceste beneficii include următoarele:

■ Utilizarea unei infrastructuri de rețea unificată

■ O mai bună integrare IP pe ATM

■ Modelul peer-to-peer pentru MPLS VPN

■ Flux optim de trafic

■ Inginerie de traffic

## 1.2. MPLS VPN (Multiprotocol Label Switching Virtual Private Network)

Rețea virtuală privată

O rețea VPN este o rețea care emulează o rețea privată pe o infrastructură comună. VPN

ar putea oferi comunicare la straturile OSI 2 sau 3. VPN, de obicei, aparține unei societăți și are mai multe site-uri interconectate în infrastructura furnizorului de servicii comune.

Rețeaua privată impune că toate site-urile clientilor sunt în măsură să interconecteze și sunt complet separate de alte VPN. Aceasta este cerința de conectivitate minima. Cu toate acestea, modele VPN la stratul de IP ar putea necesita mai mult decât atât. Ele pot oferi conectivitate între diferite VPN-uri când este dorit, și chiar conectivitate la Internet. MPLS VPN oferă toate acestea. Acest model este posibile deoarece furnizorul de servicii se execută MPLS-ul în rețeaua backbone.

Figura 1. Schematica de ansamblu MPLS VPN

Arhitectura de ansamblu MPLS VPN

Pentru a realiza MPLS VPN, este nevoie de blocuri de construcție elementare pe routere PE. Aceste blocuri sunt următoarele: VRF, distingere de traseu (RD), obiective de traseu (RT), traseu de propagare prin MP-BGP și transmiterea de pachete etichetate.

##  1.3. Virtual Routing Forwarding

O rutare virtuală/forwarding (VRF) este o rutare VPN și instant de transmitere. Este numele combinației de tabela de rutare VPN, tabela VRF Cisco Express Forwarding (CEF) și protocoalele de rutare IP asociate unui router PE. Un router PE are o instanță VRF pentru fiecare VPN atașat. Se poate observa din figura 2 că un router PE deține tabelul global de rutare IP, dar, de asemenea, câte un tabel de rutare VRF per VPN conectat la PE.

Pentru că traseele ar trebui să fie separate și private pentru fiecare client (VPN) pe un router PE, fiecare VPN ar trebui să aibă propria tabelă de rutare. Acest tabel de rutare privat se numeste tabela de rutare VRF.

Interfața pe de un router PE spre un router CE poate aparține doar unui VRF. Ca atare, toate pachetele IP primite pe interfața VRF sunt în mod clar identificate ca aparținând acelui VRF. Deoarece există un tabel de rutare separat pe VPN, există o tabelă de CEF separat pe VPN ce transmite aceste pachete pe router-ul PE. Aceasta este tabela VRF CEF. Ca și în tabela de rutare globală și tabela de CEF globală, tabelul VRF CEF este derivat din tabelul de rutare VRF.[2]



Figura 2. VRF pe un router PE

RD:

Prefixele VPN sunt propagate în întreaga rețea MPLS VPN de Multiprotocol BGP (MPBGP). Problema este că atunci când BGP poartă aceste prefixe IPv4 din furnizorul de servicii rețea , acestea trebuie să fie unice. În cazul în care clienții au avut adresare IP suprapusă, rutarea ar fi greșită. Pentru a rezolva această problemă, conceptul de RD a fost realizat pentru a face prefixele IPv4 unice.

Ideea de bază este că fiecare prefix de la fiecare client primește un identificator unic (RD) pentru a distinge același prefix de la diferiți clienți. Un prefix derivat din combinația de prefix și RD este numit un prefix vpnv4. MP - BGP trebuie să transporte aceste prefixe între routerele PE. Un RD este un câmp de 64 de biți folosit pentru a face prefixele VRF unice, atunci când MP - BGP le poartă. RD nu indică de care VRF aparține prefixul. Funcția de CD nu este cea a unui VPN de identificare, deoarece unele scenarii mai complexe de VPN ar putea necesita mai mult de un CD pe VPN. Fiecare instanță VRF pe router PE trebuie să aibă un RD atribuit. Această valoare pe 64 de biți poate avea două formate: ASN:nn sau IP - adresa:nn , unde nn reprezintă un număr. Cele mai frecvent utilizate format este ASN:nn, unde ASN reprezintă numărul de sistem autonom. De obicei, furnizorul de servicii foloseste ASN:nn, unde ASN este numărul de sistem autonom pre care autoritatea de numerele alocate de Internet IANA atribuie la furnizorul de servicii și nn este numărul pe care furnizorul de servicii atribuie unic la VRF. RD nu impune semantica, ea este doar folosită pentru a identifica în mod unic rutele VPN. Acest lucru este necesar deoarece rutele IPv4 de la un client ar putea fi suprapuse cu rutele IPv4 de la altul. Combinația de CD cu prefixul IPv4 furnizează un prefix vpnv4, din care adresa este de 96 biti. Masca este de 32 de biti , la fel cum este pentru un prefix IPv4.

RT:

Dacă RD au fost folosite doar pentru a indica VPN, comunicarea între site-uri de diferite VPN-uri ar fi problematică. Un site de companie A nu ar fi în măsură să vorbească cu un site de companie B deoarece RD nu s-ar potrivi. Conceptul de a avea site-uri ale companiei A capabile de a vorbi cu site-uri din compania B este numit VPN extranet. Simplul caz de comunicare între site-uri de aceeași companie cu același VPN se numeste intranet. Comunicarea dintre site-uri este controlat de o altă caracteristică MPLS VPN, numit RTS.

Un RT este o comunitate extinsa BGP care indică ce rute trebuie să fie importate din MPBGP în VRF. Exportarea unui RT înseamnă că traseul vpnv4 exportat primește o suplimentare de comunitate BGP extinsă, aceata este RT - configurat sub ip VRF pe router-ul PE, atunci când traseu este redistribuit de la tabela de rutare VRF în MP - BGP. Importul de RT înseamnă că traseul vpnv4 primit de la MP - BGP este verificat pentru o potrivire de comunitate extinsă. Acesta este traseul țintă cu cele din configurație. În cazul în care rezultatul se potrivește, prefixul este pus în tabela de rutare VRF ca un traseu IPv4. Dacă potrivirea nu are loc, prefixul este respins. [1]



Figura 3. RT-uri

## 1.4. Transmiterea de pachete într-o rețea MPLS VPN (Port Forwarding)

Pachetele nu pot fi transmise ca pachete IP pure între site-uri, iar routerele P nu le pot transmite, deoarece acestea nu au informațiile VRF de la fiecare site . MPLS poate rezolva această problemă prin etichetarea pachetelor. Routere P trebuie să aibă doar informația de transmitere corecta pentru eticheta să transmită pachetele. Modul cel mai comun este de a configura Label Distribution Protocol (LDP) între toate routerele P și PE astfel încât tot traficul IP are etichetele schimbate între ele. Se poate folosi, de asemenea, RSVP cu extensii pentru inginerie de trafic (TE) atunci când se pune în aplicare MPLS TE, dar PLDM este cea mai comună pentru MPLS VPN. Pachetele IP sunt apoi transmise etichetele. Un router P nu trebuie să efectueze o căutare a adresei IP destinație. Acesta este modul în care pachetele sunt commutate între PE intrare și PE ieșire. Această etichetă se numește etichetă IGP, pentru că este eticheta care este legată la un prefix IPv4 în tabelul de rutare globală a routerelor P și PE și IGP-ul rețelei furnizorului de servicii face transmisia.

Pentru ca ieșirea routerului PE să știe cărui pachet VRF îi aparține, se adaugă o altă etichetă în eticheta stivă MPLS. Această etichetă indică cărui pachet VRF îi aparține. Prin urmare, toate pachetele de client sunt transmise cu două etichete: eticheta IGP ca eticheta de sus și eticheta VPN ca eticheta de jos. Eticheta VPN trebuie să fie pusă pe către intrarea de router PE pentru a indica la ieșirea routerului PE cărui pachet VRF aparține.



Figura 4. Transmiterea de pachete într-o rețea MPLS VPN

Traficul VRF-la-VRF are două etichete în rețeaua MPLS VPN. Eticheta de sus este eticheta IGP și este distribuită de către LDP sau RSVP pentru TE între toate routerele P și PE hop cu hop. Eticheta de jos este eticheta VPN care este transmisă prin MP-iBGP de la PE la PE. Routerele P utiliza eticheta IGP pentru a transmite pachetul către router-ul correct ieșire PE. Ieșirea de router PE utilizeaza eticheta VPN pentru a transmite pachete IP la router-ul corect CE. [1]

## 1.5. Accesul la internet prin VPN

Internet routing-ul se face de obicei cu ajutorul unui tabel BGP al rețelei MPLS VPN a serviciului furnizor. Acest tabel BGP este în spațiul de rutare globală, nu în contextul VRF. În mod implicit, site-urile VRF pot comunica doar cu alte site-uri VRF din același VPN și cu nimic în spațiu de rutare la nivel global. Prin urmare, trebuie făcut ceva pentru a oferi acces la Internet (context global) pentru routerele CE (context VRF). Accesul la Internet este posibil numai pentru subrețele IP ale clientului care nu fac parte din spatiul privat de adresare IP (RFC 1918).

O soluție care ar putea părea mai simplă este de fapt cea mai rea. Furnizorul de servicii ar putea plasa complet tabela de internet routing în VRF. Cu toate acestea, ar însemna că un enorm număr de rute va fi plasat în VPN. Furnizorul ar putea face acest lucru o dată și să pună toți clienții care necesită acces la Internet în acest VRF. Dar ideea ca fiecare client să posede propria sa rețea privată ar fi complet pierdută. O altă soluție ar putea fi ca furnozirul de servicii să pună tabela de rutare Internet în fiecare VRF a fiecărui client care necesită acces la Internet.

Asta ar putea fi și mai dezavantajos, deoarece numărul enorm de rute de Internet ar putea fi replicate de mai multe ori și cauza probleme de scalare pe ruterele PE. Prin urmare, ar trebui să evite această soluție.

Accesul la Internet prin tabela de rutare globală:

O modalitate simplă de a oferi acces la Internet, la routere CE este de a avea o interfață de la routerele PE la CE care se află în spațiul de rutare la nivel global. Router-ul PE are o interfață VRF spre router-ul CE, dar poate avea o a doua interfață care nu este într-un VRF spre routerul CE. Routing-ul de pe CE ar trebui să aibă grijă să trimită traficul VPN la interfața VRF și traficul de Internet la interfața în spațiul de rutare la nivel global pe router PE. Dezavantajul este că va fi nevoie de o a doua legătură între PE și CE, folosind o interfață suplimentară pe ambele routere. Pentru a rezolva acest lucru, este posibilitatea de a utiliza subinterfaces când încapsularea pe stratul Layer 2 este Frame Relay sau încapsulare 802.1Q. Cu toate acestea, în cazul în care încapsularea Layer 2 nu permite subinterfețe, o altă posibilă soluție ar putea fi lipirea doar cu interfața VRF pe routerul PE și crearea unui tunel GRE în spațiul de rutare la nivel global pe interfața VRF.

Accesul la Internet prin tabela de rutare globală cu rute statice:

Se oferi acces la Internet pentru clienții VPN prin transmiterea traficului lor la gateway-ul Internet al furnizorului de servicii. Poarta de acces Internet este cunoscută pentru toate routerele P în rețeaua MPLS VPN deoarece adresa IP a gateway-ului este cunoscută în tabela de rutare globală a serviciului furnizor. Se execută eBGP cu un router de un furnizor de Internet. Routere PE deja rulează BGP, astfel încât să poată oferi servicii de MPLS VPN. Routere PE pot rula, de asemenea, o sesiune iBGP peering pentru IPv4. Pentru a oferi acces la Internet la o VRF, tabela de rutare la nivel global trebuie să transmită traficul. Acest lucru are loc prin crearea unei rute statice în tabelul VRF pe routerul PE și specificând un hop următor, care este în tabela de rutare la nivel global. Pentru a face acest lucru, se utilizează cuvinte cheie la nivel global pe ruta VRF static. Acest lucru asigură faptul că traficul care curge de la router CE la PE prin interfața VRF și că este trimis în funcție de ruta statică de unde este transmis următorul hop în tabela de rutare la nivel global. Configurarea unei rute statice pe router PE și specificarea unui hop lângă router-ul CE realizează acest lucru. Pentru a se asigura că poarta de acces Internet știe despre acest traseu, se distribuie ruta statică în BGP sau IGP a furnizorului de servicii. Deoarece traficul nu mai este VPN - la - VPN, dar este transmis în tabela de rutare la nivel global, are o singură etichetă în rețeaua MPLS VPN. [1]

# 2. MPLS Traffic Engineering -TE-Ingineria traficului Aflorei Victor - 441A

 Ingineria traficului (TE) sau capacitatea de a conduce trafic printr-o rețea a fost în prim plan pentru un timp, dar a fost în principal prezentă în rețelele ATM sau în rețele Frame Relay. Rolul TE este de a dirija trafic de la o margine a unei rețele la alta în modul cel mai optim. În aceste rețele, circuitele virtuale au avut rolul de a transporta traficul de la o margine a rețelei la alta peste ATM sau switch-uri Frame Relay. Traficul de la un site la altul este atent planificat și mapat peste aceste circuite virtuale. Acest lucru este cunoscut ca modelul de suprapunere (*overlay model*). În zilele noastre, protocolul dominant în rețele este în mod clar protocolul IP. Deși rețelele IP timpurii au fost implementate într-o infrastructură ATM sau Frame Relay, tot mai multe rețele se bazează pe o soluție pură IP sau o soluție IP care rulează peste o rețea MPLS-enabled. Prin urmare, a fost nevoie de o soluție de TE pentru rețelele IP. Deși TE nu putea să fie încă posibil într-o rețea pură IP este posibil într-o rețea IP/MPLS cu soluția MPLS TE.[1]

##  2.1. Necesitatea folosirii MPLS TE

Rutarea în rețelele IP este reglementată de necesitatea de a transporta trafic de-a lungul rețelei cât mai repede posibil. Acesta este motivul pentru care rutarea IP se bazează pe principiul de rutare cu costuri minime. Fiecare protocol de rutare IP are un cost asociat pentru toate link-urile din rețea. Acumularea costurilor fiecării link a unui drum este utilizată pentru a calcula calea cu costul cel mai mic pentru a transmite traficul prin rețea. Costul este una din metricile asociate unui link (de exemplu Open Shortest Path First [OSPF] și Intermediate System-to-Intermediate System [IS-IS]); alte metrici fiind: o metrică compozit (de exemplu, Interior Gateway Routing Protocol [IGPR] și Enhanced Interior Gateway Routing Protocol [EIGRP]) sau pur și simplu o numerotare a numărului de hop-uri traversate (de exemplu, Routing Information Protocol [RIP] și RIP versiunea 2).

 Paradigma IP forwarding este bazată pe transmiterea pe calea cu costul cel mai mic. Mai mult, pachetele IP sunt transmise peste fiecare hop (router) bazându-se exclusiv pe adresa IP destinație și independent de modul în care pachetele IP sunt transmise pe traseu, înainte sau după acest hop. De asemenea, paradigma IP forwarding nu ia în considerare lățimea de bandă disponibilă legăturii, care poate diferi în mod semnificativ de costul atribuit legăturii. Prin urmare, un router poate transmite în continuare trafic IP pe un link, chiar dacă acest link aruncă deja pachete din cauza lipsei de lățime de bandă necesară pentru a transmite toate fluxurile de trafic pentru care tabela de rutare indică acest lucru. Rezultatul acestui comportament în transmiterea de pachete IP este că unele link-uri din rețea ar putea fi suprasolicitate, în timp ce alte link-uri ar putea fi utilizate insuficient. Desigur, se poate menține un ochi pe ratele de trafic pe link-urile de rețea și se poate plănui o upgradare a capacității legăturii pentru a se servi aceste suprasolicitări. Adăugarea de lățime de bandă link-urilor este ceva ce nu se poate realiza peste noapte, aceasta necesită o planificare și are nevoie de timp. Deoarece modelele de trafic între site-uri se pot schimba destul de brusc și nu sunt întotdeauna permanente, TE poate aduce o soluție de orientare a traficului (sau o parte din el) departe de link-urile supraîncărcate.

 Figura de mai jos reprezintă o rețea unde se folosește IP forwarding.



Figura 5. Rețea cu IP Forwarding

 Dacă fiecare link din această rețea are același cost, cel mai mic cos de la router-ul R1 la router-ul R1 este calea R1-R2-R5. In mod evident, tot traficul de la R1 la R5 va utiliza calea R1-R2-R5 iar calea R1-R3-R4-R5 nu va avea trafic. Într-o rețea reală lucrurile nu sunt la fel de simple. Multe fluxuri de trafic pot exista și încărcarea pe link-uri ar putea varia foarte mult.

 Putem distribui încărcarea mai uniform jucându-ne cu costul link-urilor pentru fiecare protocol de rutare. Acest lucru ar putea distribui traficul mai uniform, dar nu se poate distribui încărcarea perfect, deoarece în rețelele reale, link-urile nu vor avea niciodată aceeași lățime de bandă. În rețeaua din figura de mai sus, ne putem asigura că cele două căi sunt egale asigurându-ne că suma costurilor link-urilor din calea R1 - R2 - R5 și din calea R1 - R3 - R4 - R5 sunt egale. Rezultatul va fi echilibrarea încărcării de trafic între R1 și R5 pe cele două căi. Acest lucru funcționează bine pentru traficul între R1 și R5, dar cu siguranță vom avea trafic care intră în rețea prin R2 și o părăsește prin R4, același lucru fiind posibil si în cazul celorlate noduri. Aceasta este aceeași problemă, deoarece există două căi de la R2 la R4; una conține 2 hop-uri iar celalaltă trei. Putem avea aceeași problemă între routerele R3 și R5 sau la oricare dintre celelalte. Cu alte cuvinte, problema încărcării egale a link-urilor cu trafic este o sarcină imposibilă dacă tocmai am încerca să ajustăm costul fiecărui link din rețea.

 Pentru a spori și mai mult complexitatea problemei, viteza pe oricare din link-uri poate fi upgradată, pentru a permite mai multă lățime de bandă pe anumite legături. În acel moment, avem nevoie din nou de o planificare de la zero și trebuie să schimbăm manual costul fiecărui link în întreaga rețea. Acest lucru nu este durabil din punct de vedere operațional.

 MPLS TE este o soluție pentru această problemă în următoarele moduri:

 - MPLS TE oferă eficiența răspândirii traficului în rețea, evitând link-urile underutilized și overutilized;

 - MPLS TE ia în considerare lățimea de bandă configurată (static) pe link-uri;

 - MPLS TE ia în considerare atributele link-urilor (de exemplu, întârziere, bruiaj);

 - MPLS TE se adaptează automat la schimbarea lățimii de bandă și a atributelor link-urilor;

 - rutare bazată pe sursă este aplicată încărcării TE în opoziție cu rutarea pe bază de IP destinație.[3]

 MPLS TE permite o schemă TE unde router-ul head end a unei căi (label switched path LSP), poate calcula cea mai eficientă cale prin rețea față de router-ul tail end a LSP-ului. Router-ul head end poate face acest lucru în cazul în care acesta cunoaște topologia întregii rețele. Mai mult decât atât, router-ul head end trebuie să știe lățimea de bandă rămasă pe toate link-urile din rețea. În cele din urmă, trebuie să activăm MPLS pe routere astfel încât să putem stabili legătura LSP de la un capăt la altul. Faptul că este folosit label switching și nu IP forwarding permite rutarea pe bază de sursă în loc de rutarea bazată pe IP destinație.

 Figura de mai jos prezintă un exemplu de rutare bazată pe sursă MPLS TE.



Figura 6. MPLS TE Head End Router

 Pentru a ilustra acest concept, routerele R6 și R7 au fost adăugate în fața router-ului R1. Să presupunem că routerele R6 și R7 doresc să transmită trafic spre R5. Dacă această rețea rulează numai IP forwarding, acest trafic urmează numai calea R1 - R2 - R5, indiferent de ceea ce am configurat pe routerele R6 și R7. Asta se datorează faptului că transmiterea de pachete IP se face independent în fiecare hop din rețea. Prin urmare , router-ul R1 nu știe ce sunt capabile să facă routerele R6 și R7 și el transmite traficul în funcție de propria decizie bazându-se pe tabela sa de rutare. R6 și R7 ar putea avea politici diferite. R6 ar putea dori să trimită traficul de-a lungul drumului R6 - R1 - R2 - R5, în timp ce R7 ar putea dori să transmită traficul de-a lungul drumului R7 - R1 - R3 - R4 - R5, ceea ce este imposibil de realizat într-o rețea IP simplă. În cazul în care rețeaua rulează MPLS, putem configura aceste două căi ca două LSP-uri diferite astfel încât se folosesc etichete diferite. La router-ul R1, diferitele valori ale etichetelor de intrare indică dacă pachetul aparține LSP-ului cu R6 ca head end sau LSP-ului cu R7 ca head end. R1 transmite apoi pachetul pe una din cele două LSP-uri, dar nu transmite pachetul în conformitate cu propria decizie cum este în cazul IP forwarding.

 Avem posibilitatea să implementăm MPLS TE în orice rețea care are LSR-uri. Cu toate acestea, deoarece lățimea de bandă și alte atribute ale link-urilor trebuie să fie cunoscute de către head end-ul LSR a LSP-ului, protocolul de rutare utilizat între punctele finale MPLS TE (head end and tail LSR) trebuie să fie un protocol de rutare link state. Cu un protocol de rutare link state, fiecare router construiește o stare a propriilor link-uri, care este apoi inundată către toate celelalte routere din aceeași zonă. Acest lucru înseamnă că toate routerele din acea zonă au toate informațiile despre topologie. Head end-ul LSR își poate da astfel seama cum se stabilește LSP-ul în MPLS TE. Acest lucru permite rutarea bazată pe sursă. Acest LSP se numește un *tunel MPLS TE*. Cu toate acestea, nu este asemănător unui tunel GRE. Un tunel TE este unidirecțional deoarece un LSP este unidirecțional și el are configurația tunelului TE numai pe router-ul head end LSR și nu pe router-ul tail end LSR a LSP-ului. Mai mult decât atât, un tunel TE trebuie semnalizat, în timp ce un tunel GRE nu.

 Dacă TE este activat în rețea, îl putem folosi în două moduri distincte. În primul rând, putem crea tunele MPLS TE între fiecare pereche de LSR-uri aflate la marginea rețelei. Ca atare, putem orienta tot traficul în rețea, putem evita congestionarea ei și putem da traficului caracteristicile (lățime de bandă, întârziere, bruiaj) de care are nevoie. Un exemplu bun este MPLS VPN, unde putem crea un tunel TE de la fiecare router PE la orice alt router PE. În al doilea rând, putem activa MPLS TE peste tot în rețea dar nu putem avea tunele TE până când acestea sunt necesare. Putem crea tunelurile TE la cerere. Un bun exemplu în acest sens este atunci când facem tunele TE pentru a ghida traficul în jurul unui hotspot sau în jurul punct supraîncărcat din rețea. La fel de important ca modul cum dirijăm traficul cu LSPs TE prin rețea este cum mapăm traficul prin ele. Atunci când nu intră trafic în tunelele TE ele sunt inactive.

## 2.2. Functionarea MPLS TE

 **Pietrele de temelie ale MPLS TE:**

 - Constrângerile link-urilor (cât de mult trafic poate suporta fiecare link și care tunel TE poate folosi link-ul);

 - Distribuirea de informații TE (realizată de protocolul de rutare link-state care rulează peste MPLS TE-enable);

 - Un algoritm (calcul cale [PCALC]) pentru a calcula cea mai bună cale de la head end LSR la tail end LSR;

 - Un protocol de semnalizare (Resource Reservation Protocol [RSVP]) pentru a semnala tunelul TE în întreaga rețea;

 - O modalitate de a transmite traficul prin tunelul TE. [1]



Figura 7. Blocurile de construcție TE pentru rețeaua din fugura 6. Un tunel TE sau LSP se întinde de la R6 la R5

 Primul nume folosit pentru MPLS TE a fost de Routing with Resource Reservation, de asemenea, cunoscut sub numele de RRR. Acest nume indică faptul că un motiv important de a avea MPLS TE este acela de rutare sau de direcționare a traficului în funcție de resurse sau de constrângeri. Aceste resurse sunt lățimea de bandă a link-urilor și unele atribute pe care le specifică operatorul. Aceste atribute sunt configurate pe link-uri și sunt avertizate de către protocolul de rutare link-state (OSPF sau IS-IS). În loc de a crea un nou protocol care să transporte această informație și să o anunțe la toate LSR-urile, OSPF și IS-IS au fost extinse pentru a alipi această informație. Când configurăm un tunel TE pe un LSR, el devine head end LSR al tunelului TE sau TE LSP. Apoi specificăm LSR-ul destinație al tunelului TE și constrângerile la care acesta trebuie să adere.

 În interiorul IOS-ului, o bază de date TE este construită din informațiile TE pe care protocolul link-state le trimite. Acest set de date conține toate link-urile care sunt activate pentru MPLS TE și caracteristicile sau atributele lor. Din această bază de date MPLS TE, cu ajutorul căii (PCALC) sau constrângerilor SPF (CSPF) se calculează ruta cea mai scurtă care însă aderă la toate constrângerile (cel mai importantă fiind lățimea de bandă) de la LSR-ul head end la LSR-ul tail end. PCALC sau CSPF este un algoritm shortest path first (SPF) modificat pentru MPLS TE astfel încât constrângerile să fie luate în considerare. Lățimea de bandă disponibilă pentru TE și atributele sunt configurabile pe toate link-urile rețelei. Configurăm lățimea de bandă necesară și atributele tunelului TE pe configurația LSR-ului head end. PCALC potrivește cerința de lățime de bandă și atributele tunelului TE cu cele de pe link-uri și dintre toate căile posibile o alege pe cea mai scurtă. Calculul se face pe LSR-ul head end.

## 2.3. Distributia informatiei TE

Un protocol de rutare link-state trebuie să inunde constrângerile link-urilor în rețea pentru toate routerele pe care rulează TE.

 **Necesitatea unui IGP ­­(Interior Gateway Protocol)**

UnInterior Gateway Protocol (IGP) trebuie să fie capabil să trimită toate informațiile despre topologia rețelei (starea link-urilor) tutror routereler din zona în care TE a fost activat. Doar un protocol link-state poate efectua această sarcină deoarece el inundă starea tuturor legăturilor unui router tuturor routerelor din acea zonă. Prin urmare, fiecare router din acea zonă știe toate căile alternative pentru a ajunge la destinație. Un protocol de rutare distance vector nu poate efectua această sarcină. Acesta este conceput doar pentru a transmite cel mai bun traseu (ruta din tabela de rutare) prin urmare, informațiile privind căile alternative sunt pierdute.

 Head end-ul tunelului TE trebuie să dispună de toate informațiile despre topologie pentru a vedea toate căile posibile, dar de asemenea aceasta trebuie să aibă disponibile toate informațiile despre constrângerile link-urilor. Aceste informații despre constrângeri reprezintă colecția resurselor de informații ale link-urilor asociate cu TE. Protocolul de rutare link-state trebuie extins pentru a putea transporta aceaste resurse de informații.

 Resursele TE a unui link sunt:

 - metric TE;

 - lățimea de bandă maximă;

 - lățimea de bandă maximă rezervabilă;

 - lățimea de bandă care nu a fost rezervată;

 - grupul administrativ.[1]

 Metrica TE este un parametru pe care îl putem folosi pentru a construi o topologie TE diferită de topologia IP. Ca atare, metrica TE a unui link poate fi diferită de costul OSPF sau metrica IS-IS pentru link-ul respectiv. Lățimea de bandă maximă este de lățime de bandă totală a link-ului. Lățimea de bandă maximă reservabilă este lățimea de bandă disponibilă pentru TE pe link-ul respectiv. Lățimea de bandă care nu a fost rezervată este restul de lățime de bandă disponibilă pentru TE. Grupul administrativ este un câmp de 32 biți. Operatorul de rețea poate seta individual fiecare bit din acest domeniu 32 de biți și poate alege un configurație optimă lui.

 **Extensiile OSPF pentru TE**

RFC-ul 2370 descrie o extensie a protocolului OSPF unde trei noi link-state advertisements (LSAs) sunt definite și sunt numite LSA-uri opace. Aceste trei noi LSA-uri reprezintă pentru OSPF un mecanism generalizat de extindere. Ele pot transporta informații pentru a fi utilizate de către OSPF sau direct de către orice aplicație. Aceste LSA-urile reprezintă exact ceea ce avea nevoie MPLS TE pentru a introduce informațiile sale în OSPF. OSPF acum poate inunda această informație în întreaga rețea.

 Trei tipuri de LSA-uri opace există și diferă doar în domeniul în care aplică inundațiile (flooding). LSA-ul opac de tip 9 are un domeniu de aplicare a inundațiilor numai link-local; LSA-ul opac de tip 10 are ca domeniu de aplicare a inundațiilor întreaga arie și LSA-ul opac de tip 11 are ca domeniu de aplicare a inundațiilor întreg sistemul autonom. Asta înseamnă că LSA-ul de tip 9 este trimis doar pe link, dar niciodata mai departe, LSA-ul de tip 10 sunt oprite de routerele de graniță din zona respectivă iar LSA-urile de tip 11 sunt inundate de-a lungul domeniului OSPF, la fel ca și LSA-ul de tip 5.[1]

 **Extensiile IS-IS pentru TE**

 RFC-ul 3784 descrie extensiile aduse de IS- IS, care îi permit să transporte informațiile MPLS TE. Două noi IS - IS TLV-uri (type-length-value) au fost definite. Acestea permit ca informația MPLS TE să fie transportată de către IS - IS. Cu toate acestea, în același timp, s-au făcut alte câteva modificări în ceea ce privește aceste TLV-urile, cum ar fi extinderea metricii link-urilor de la un maxim de 63 la un nou maxim de 224-1, utilizarea sub-TLV-urilor precum și introducerea down bit-ului. Primul nou TLV reprezintă TLV-ul IS Reachability TLV extins, sau TLV-ul tip 22. Acesta este succesorul IS Reachability TLV (TLV tip 2). Acest TLV descrie vecinii IS - IS și printre altele costul până la aceștia. Cel de-al doilea nou TLV este IP Reachability TLV extins sau TLV tip 135. Acesta este succesorul TLV-ului IP Reachability TLV (TLV tip 128 și TLV tip 130). Ambele noi TLV-uri au formatul metricii extins care permite metrici mai mari. TLV-ul IS Reachability extins este TLV-ul care transportă sub-TLV-urile folosite de MPLS TE.

## 2.4. Rutarea si costul TE

Când calea unui tunel TE este calculează mai mulți factori intră în joc. Rezultatul calculului este drumul cel mai scurt posibil de la toate căile pentru care caracteristicile link-urilor se potrivesc cu caracteristicile necesare tunelului TE. Rețeaua prezentată în figura de mai jos ilustrează necesitatea acestui calcul.



Figura 8. Exemplu de rețea TE

 **Atributele link-rilor TE**

Fiecare link din rețeaua MPLS activat pentru TE poate avea caracteristici care trebuie să fie inundate astfel încât router-ul head end să-și poată da seama dacă tunelul TE poate folosi un anumit link. Un link care este activat pentru TE poate avea următoarele caracteristici configurate pentru TE:

 - Lățimea de bandă maximă rezervată;

 -Attribute flags;

 - Metrica TE;

 - Shared risk link groups;

 - Lățimea de bandă maximă rezervată pe sub-pool.

## 2.5. Forwarding Traffic in tunelele MPLS TE

 Crearea unui tunel TE și având-ul operațional este o parte. Asigurarea că acesta este utilizat pentru a transmite traficul reprezintă cealaltă parte. Putem activa tunelul TE pentu a transmite trafic în șase moduri:

 - Rutarea statică

 - Rutarea Policy-based

 - Autoroute announce

 - Forwarding adjacency

 - Maparea directă a traficului AToM în tunele TE

 - Selecția tunelului bazată pe clasă

 **Rutare statică**

 Un mod simplu de a trimite trafic în tunelul TE este de a configura o rută statică pe router-ul head end. Trebuie doar să configurăm tunelul TE ca interfață de ieșire în traseul static.

 Rutarea Policy-based

 Rutarea bazată pe politici (PBR) utilizează o politică de configurată pe interfața de intrare pentru a trimite trafic la un anumit hop viitor. Când utilizăm PBR, putem dirija traficul pe anumite trasee care diferă traseul obișnuit bazându-ne exclusiv pe adresa IP destinație.

 Autoroute announce

 Practic, autoroute announce modifică algoritmul SPF, astfel încât LSR poate introduce prefixe IP în aval de cel mai apropiat tunel TE router-ul tail end în tabela de rutare a routerului head end pe care tunelul TE în are ca următorul hop.

 Forwarding adjacency

 Forwarding adjacency este o caracteristică MPLS TE prin care IGP-ul poate vedea un TE LSP ca un link. IGP-ul de pe router-ul head end al tunelului TE reclamă TE LSP ca o legătură cu o anumită metrică IGP asociate ei. Orice router din aceeași zonă ca și router-ul head end include această legătură atunci când se rulează algoritmul SPF.

 Selecția tunelului bazată pe clasă

 Selecția tunelului pe bază de clasă (instruirea asistată de calculator) este o caracteristică TE prin care putem transmite diferite clase de servicii (COS) de trafic pe diferite tuneluri TE. Aceste tuneluri TE pot fi tuneluri pool la nivel mondial sau tuneluri sub-pool, dar toate tunelurile TE trebuie să fie între aceleași routere head end si tail end.

# 3. IPv6 peste MPLS – Jircu Andrei 441A

## 3.1. Protocolul IPv6

IPv6 este succesorul lui IPv4. Ai putea crede ca ar trebui sa fie IPv5,dar acela a fost doar un experiment si a fost abandonat.IPv6 este protocolul IP de generatie urmatoare. Este similar cu IPv4 in multe privinte, dar de asemenea este diferit in multe feluri. Una dintre cele mai mari diferente de se poate vedea “cu ochiul liber” este adresa IP mai mare (128 biti). Aceasta este principala caracteristica pentru oameni ca sa se mute de pe IPv4 si sa inceapa implementarea IPv6.Obtinerea unei adrese IPv4 in ziua de azi nu mai este asa de usor cum a fost acum 20 de ani. Adresele IPv4 au 4 octeti sau 32 de biti. A devenit evident ca, odata cu cresterea actuala a internetului se va ramane fara adrese IP disponibile.

 IETF (Engineering Task Force) a facut o adresa IP de 128 biti. Asta face ca adresa IPv6 sa fie de patru ori mai mare decat adresa IPv4. Adresa IPv4 pe 32 de biti prevede aproximativ 4,3 miliarde de adrese, iar adresa IPv6 prevede aproximativ 3,4 \*10^38 adrese.

 Cele mai mari schimbari in IPv6 comparat cu IPv4 sunt dimensiunile mai mari ale adreselor si header-ul simplificat.

IPv4 Header



IPv6 Header



 Schimbarea evidenta este lungimea adresei. Adresa sursa si adresa destinatie sunt de patru ori mai mare in header-ul IPv6. De asemenea, antetul este simplificat deoarece anumite campuri au fost omise. De exemplu, antetul nu mai are o suma de control (checksum). Asta inseamna ca nu mai trebuie recalculate suma de control a header-ului IP la fiecare hop (ruter) din retea, ce ofera o expediere mai simpla si mai rapida. Sarcina de verificare a header-ului IP se afla in present pe portocoalele de la nivelele superioare, cum ar fi TCP si UDP.

 In afara de suma de control, campul Fragment Offset a disparut. Acest lucru este posibil, deoarece ruterele nu pot fragmenta pachetele, asa cum au facut cu pachetele IPv4.

Campul IHL (Internet Header Length) a fost scos, deoarece header-ul IPv6 are mereu lungimea de 40 de biti.

Campul Hop Limit are aceeasi functie ca si Time-to-live (TTL) din IPv4. Campul Type of Service (tip de serviciu) a devenit acum campul Traffic Class ( clasa de trafc) in IPv6. Functionalitatea este asemanatoare ca si campul Type of Service pentru ca indica informatii despre calitatea serviciului (QoS) a pachetului IP. Exista si un camp nou, si anume campul Flow Label (flux eticheta). Acest camp are 20 de biti lungime si indica fluxul de care apartine pachetul IPv6. [2]

## 3.2 Adresarea IPv6

 Exista trei categorii de adrese IPv6: unicast,anycast si multicast. Adresa unicast este o adresa IP pe o singura interfata. O adresa anycast este o adresa care poate fi atribuita mai multor interfete pe mai multe noduri. Un pachet care este destinat adresei IPv6 respective este trimis catre cea mai apropiata interfata cu adresa anycast. Cea mai apropiata interfata inseamna calea cea mai scurta in functie de protocolul de rutare folosit.

 O adresa multicast este o adresa care este atribuita mai multor interfete pe mai multe noduri. Un pachet este trimis pe toate interfetele ce folosesc adresa multicast respectiva. Adresa de broadcast a fost eliminate din tranzitia de la IPv4 la IPv6. Adresele multicast sunt utilizate in present in loc de adresa de broadcast. Adresa de 128 de biti este scrisa in formatul urmator : x:x:x:x:x:x:x:x, fiecare x reprezentand o valoare hxazecimala de 16 biti, pentru un total de 128 de biti ai adresei IPv6. Un exemplu de o astfel de adresa este : 2001:DB08:7654:3210:FEDC:BA98:7654:3210.

Dupa cum se poate observa, reprezentarea unei adrese IPv6 este destul de lunga in comparative cu reprezentarea scurta punctata zecimal a unei adrese IPv4.Putem scurta adresa IPv6 prin inlocuirea a mai multor grupuri de 16 biti de zero. Putem face acest lucru doar o singura data intr-o adresa IPv6, desi, in caz contrat, adresa scurtata ar putea deveni ambigua.

Cand IETF a creat IPvv6 au aplicat lectiile invatate de la IPv4. IPv4 a avut clase de retea A,B si C pentru adrese unicast. Acest lucru a dus la rutare classfull si la o risipa de adrese IP, deoarece marile retele de clasa A si B nu au fost niciodata utilizate in mod eficient. IPv6 are doar prefixe fara clase si rutare fara clase, astfel adresele IPv6 sunt utilizate mai eficient decat adresele IPv4.

## 3.3. Reteaua MPLS VPN folosind IPv6 peste tunelele de IPv4 pe rutere Customer Edge (CE)

 MPLS VPN pentru IPv4 a fost un mare succes. Multi furnizori de servicii folosesc MPLS VPN in reteaua lor. Daca se doreste sa se transporte IPv6 peste reteaua de nucleu MPLS VPN, ruterele Customer Edge trebuie sa poata rula IPv6. Daca ruterele CE ruleaza in dual-stack – ceea ce inseamna ca pot transporta si IPv4 si IPv6 rezulta ca se pot implementa tunele intre ruterele de tip CE pentru a transporta trafic de IPv6. Transportul de IPv6 peste reteaua MPLS VPN este o idee interesanta, pentru ca nu trebuie sa fie facuta nicio modificare in reteaua MPLS, dar exista si un dezavantaj. Dezavantajul este ca tunelele create dintre ruterele CE nu pot transporta IPv6 peste reteaua MPLS VPN foarte eficient.



 *Retea MPLS VPN ce transporta IPv6 peste tunele de IPv4*

Figura de mai sus arata o retea MPLS VPN pentru retea IPv4 cu rutere Customer Edge ce folosesc tunele intre ele pentru a transporta traficul de IPv6 in reteaua de nucleu MPLS. [1]

## 3.4. Transportul IPv6 peste reteaua de nucleu MPLS (6PE-Provider Edge Router)

In retelele ce folosesc MPLS astazi, pachetele etichetate pot fi pachete IPv6, fara nevoia de a avea nevoie de rutere P (Proivder Core Router) pentru a rula IPv6. Solutia este data de 6PE (Provider Edge Router).

 6PE este numele dat de CISCO pentru transportul direct de pachete IPv6 peste reteaua de nucleu MPLS.Este de retinut ca reteaua MPLS nu trebuie sa ruleze neaparat MPLS VPN. Retelele IPv6 nu apartin unui VPN (Virtual Private Network),deci nu exista nicio interfata VRF (Virtual Routing and Forwarding) pe ruterele “de granita” (PE).

 In solutia 6PE, ruterele PE sunt in dual-stack,adica pot rula si IPv4 si IPv6. Routerele CE (Customer Edge) ce ruleaza IPv6 sunt conectate la ruterul PE (Provider Edge Router) printr-o intervata normala.Interfata nu este parte din VRF pentru IPv6 chiar daca poate exista o interfata asemanatoare intr-un VRF pentru IPv4.Distributia rutarii IPv6 dintre ruterele PE se face prin MP-iBGP (Multiprotocol-Internal Border Gateway Protocol). In acelasi timp, MP-iBGP distribuie etichetele pentru a fi folosite de prefixele specifice IPv6. Etichetele BGP identifica pachetele IPv6 la iesire.Ruterul de iesire PE verifica eticheta BGP din LFIB (Label forwarding information base) si apoi transporta pachetul la iesirea ruterului CE (Customer Edge).

 Figura de mai sus arata o retea MPLS ce ruleaza 6PE. Ruterele PE au rutere CE ce sunt conectate la acestea. Unele dintre ruterele CE ruleaza IPv6, pe cand altele ruleaza IPv4. Ruterele PE pot avea chiar si o interfata VRF sis a ruleaze MPLS VPN pentru IPv4 pentru cateva rutere CE. Interfele care sunt pe ruterele PE fata de ruterele CE ce ruleaza IPv6 nu sunt intr-un VRF. Ruterele PE sunt in full mesh . Sesiunile iBGP distribuie prefixele IPv6 si etichetele MPLS corespunzatoare.

Un avantaj al 6PE-ului este ca routerul P nu trebuie sa ruleaze IPv6 sau sa fie capabil sa ruleze IPv6.De aceea, solutia 6PE poate fi implementata foarte repede peste o retea nucleu MPLS deja existent. Un al doilea avantaj este ca pachetele IPv6 sunt etichetate direct fara a fi nevoie de un antet in plus. Un motiv pentru implementarea solutie 6PE este ca majoritatea furnizorilor de servicii au deja o retea nucleu MPLS din cauza popularitatii MPLS VPN. Functionarea 6PE este asemanatoare cu functionarea MPLS VPN. Persoanele care sunt familiar cu MPLS VPN pot intelege repede solutie 6PE.

Asemanari cu MPLS VPN pentru IPv4 :

* Este nevoie de full mesh pentru MP-IBGP (Multiprotocol - Internal Border Gateway Protocol)
* Este nevoie de rutare static intre PE si CE
* Pachetele IPv6 sunt etichetate cu 2 etichete [1]

# 4. Bibliografie

[1] - *MPLS Fundamentals* - Luc De Ghein

[2] - *MPLS and VPN Architectures* - Pepelnjak and Guichard

[3] - *Traffic Engineering with MPLS* - Osborne and Simha

Figurile au fost preluate din *MPLS Fundamentals -* Luc De Ghein