Universitatea “Politehnica” din Bucureşti
Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei
Programul de masterat Ingineria Informației și a Sistemelor de Calcul

Proiect la disciplina Rețele de Calculatoare și Internet

Conducător științific

Conf. Dr. Ing. Ștefan Stăncescu

Masterand

Ing. Mihai Roșca

București
2018

Cuprins

Introducere 4
1. Calitatea serviciilor în rețelele MPLS 5
1.1. Noțiuni generale 5
1.2. Implementarea QoS 7
1.2.1. Modelele utilizate 7
2. Implementarea QoS prin MPLS 14
2.1. Detectarea de erori MPLS 16
2.2. Protecția și recuperarea MPLS 19
2.3. Mentenanța serviciilor de tip punct-la-punct și multipunct 19
Concluzii 21
Bibliografie 22
Lista figurilor 24

Introducere

Încă de la apariția primelor informații legate de omul modern, se poate observa o creștere a necesității de comunicare, alimentată de dorința de cunoaștere. Dacă se analizează metodele de transmitere a datelor se observă o evoluție surprinzătoare deoarece acestea au variat de la scrisorile transmise cu ajutorul porumbeilor călători, până la curieri care aveau ca scop livrarea informațiilor și protejarea acestora cu prețul vieții. Astfel, s-a ajuns în timpurile moderne la o evoluție surprinătoare prin care informațiile au devenit transmise în timp real.

Acest lucru se datorează tehnologiei utilizată în zilele noastre, devenind practic punctul cheie ce asigură evoluția umana. De aceea, în fiecare zi apar tehnologii noi, menite să le înlocuiască pe cele precedente prin prezentarea unui plus substanțial față de acelea.

Rețelele moderne permit comunicarea printr-o multitudine de tehnologii cum ar fi telefonia, radioul, televiziunea și cel mai important, rețelele de calculatoare și internet. Acestea pot fi de mai multe feluri:

- De date → rețele oferite de furnizorii de internet;
- De voce → rețelele companiilor tradiționale de telecomunicații;
- De date și voce

Pe parcursul acestei lucrări vom avea ca principal scop analizarea unei rețele care combină atât transmisia de date, cât și pe cea de voce, punând accentul pe elementele de calitate a transmisiei. Acest procedeu este cunoscut sub numele de Quality of Service – QoS, care folosit împreună cu tehnologia MPLS prezintă o multitudine de avantaje ce vor fi detaliate în cele ce urmează.

1. Calitatea serviciilor în rețelele MPLS

1.1. Noțiuni generale

Calitatea serviciilor sau QoS a încput să fie foarte utilizată în ultimii ani datorită problemelor de lățime de bandă existente în rețelele actuale. Acesta reprezintă un mijloc de prioritizare a traficului pentru pachetele considerate a fi importante dar și asigurarea integralității și livrării acestora.

Un exemplu unde traficul se bazează foarte mult pe serviciile de calitate este domeniul Voice over IP. Acesta trebuie să asigure livrarea în timp real al pachetelor, precum și o calitate foarte bună a acesora. Drept urmare, această tehnologie beneficiază de o prioritate mult mai mare comparativ cu cea a protocolului HTTP, de exemplu, care de multe ori în cazul unei de congestii este abandonat în detrimentul traficului VoIP.

Deși cele două servicii QoS, respectiv MPLS par a fi similare, dacă sunt privite din punct de vedere tehnic acestea sunt foarte diferite. MPLS – Multiprotocol Label Switching reprezintă un mecanism de suport de date ce impune anumite proprietăți asupra unei rețele de comunicație ce utilizează pachete. Practic, acesta este o tehnologie orintată pe conexiune, ce facilitează transmisia informațiilor de la nodul sursă la cel destinație. [1]

Comparativ cu modalitatea de rutare tradițională, cea bazată pe IP, unde fiecare pachet trece prin diverse etape precum analiza antetului și verificarea accestuia în tabelul de rutare, la fiecare hop al rețelei, o rețea de tip MPLS transportă datele în funcție de etichetele pe care fiecare pachet le are, decizia de expediere aparținând nodurilor.

Practic, QoS presupune setarea caracteristicilor de performanţă ale reţelei, şi cuprinde două părţi:

- găsirea unei căi prin rețea care poate oferi serviciul
- obligarea îndeplinirii acelui serviciu

Pentru implementarea acestor servicii Internet Engineering Task Force, cunoscut sub abrevierea IETF, a proiectat Serviciile Diferentiale, adică Diffserv. Acestea au dus la o simplificare majora a implementării protocolului MPLS, deoarece arhitectura inițială a acestuia prezenta rezervarea a 3 biți aferenți transportării informațiilor despre clasele de servicii. Biții experimentali reprezintă o copie a celor Precedenți prezenți în IP. Având în vedere faptul că arhitectura

MPLS se dorește a fi în strânsă legatură cu cea a protocolului IP, aceasta a ales să ofere suport pentru Diffserv, ci nu pentru serviciile QoS oferit de ATM.[1]

De asemenea, MPLS reprezintă doar o unealtă care poate oferi calitatea serviciilor dacă este folosită împreună cu mecanismele Diffserv.

Ca un scurt rezumat, putem aminti faptul că Serviciile de calitate QoS reprezintă o modalitate de prioritizare a traficului în funcție de protocol. Acesta este extrem de folosit pentru situațiile în care mai multe terminale pentru utilizatori folosesc o aceeași conexiune cu Internet-ul, deoarece se vor putea determina priorități ale traficului pentru banda pe care fiecare o va putea utiliza.

În ceea ce privește furnizorii de servicii de Internet, QoS reprezintă o oportunitate și o metodă de partajare a beneficiilor pentru fiecare abonat, oferind niveluri diferite de servicii. De exemplu, pot exista diverse planuri tarifare în funcție de resursele pe care clienții le doresc. Calitatea serviciului asociat cu protocolul MPLS este extrem de folositor pentru aplicațiile aferente unei rețea de tip VPN cum ar fi implementarea de politici și livrarea de servicii noi. [2]

Datorită tipului de date pe care acesta le dirijează în rețea, putem spune că protocolul de tip MPLS intervine la schimbul de date dintre nivelele doi, respectiv 3, aferente stivei OSI. [1] Modelul de referință OSI oferă o listă extinsă de funcții și servicii pentru fiecare nivel al asteia.

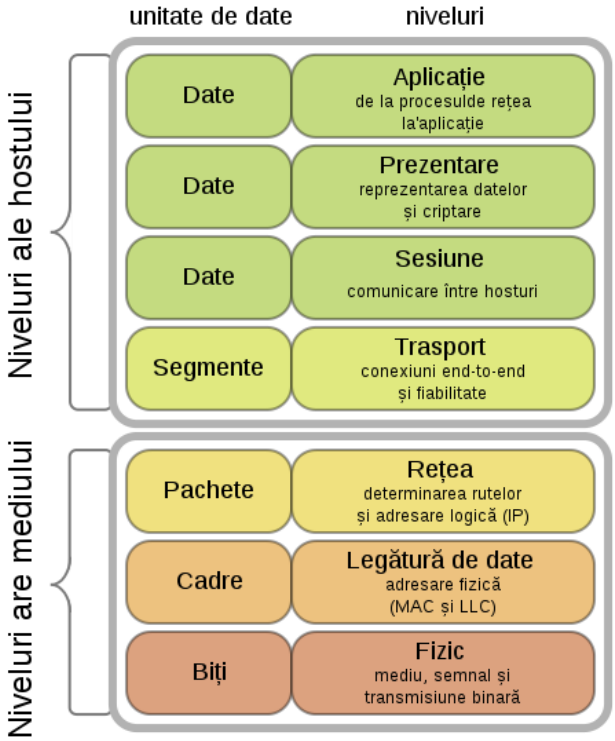

Figura 1. Modelul OSI

1.2. Implementarea QoS

1.2.1. Modelele utilizate

Pentru utilizarea eficientă a tuturor capabilităţilor oferite de implementare QoS este foarte important să se realizeze un plan elaborat. La construirea acestui plan trebuie să se ia în considerare două aspecte foarte importante:

• Ce tipuri de aplicaţii se folosesc în reţea.

• Care tehnici de QoS ar putea să îmbunătăţească performanţele reţelei.

Dacă se analizează corect primul aspect, şi se găseşte soluţia corectă relativ la cel de al doilea, atunci resursele reţelei vor fi folosite cel mai eficient.Există două modele principale folosite pentru implementarea QoS - Modelul Serviciilor Integrate (Integrated Services Model) şi Modelul Serviciilor Diferenţiate (Differentiated Services Model). [15]

IntServ îşi propunea să facă rezervări capăt la capăt pe fiecare flux, motiv pentru care nu este scalabil în Internet. Totuşi, poate fi folosit cu succes în reţele mici şi medii, în cazul în care este suportat de echipamentele de reţea. Semnalizările IntServ folosesc protocolul RSVP pentru a comunica tuturor nodurilor din cale cerinţele de trafic dorite de host-uri. Nodurile din reţea creau stări şi alocau resursele hosturilor care solicitau anumite garanţii. În cazul în care negocierea au succes, garanţiile oferite de IntServ sunt deterministe.

Din celălalt punct de vedere, DiffServ a fost văzut că o tehnologie scalabila, care nu împovărează nodurile din centrul reţelei, obligându-le să facă multe prelucrări.

A. Modelul Serviciilor Integrate

Modelul Serviciilor Integrate presupune că serviciile QoS sunt cerute în mod explicit de către aplicaţia care le necesită, prin transmiterea prin reţea a unei semnalizări adecvate. Semnalizarea cererilor de servicii QoS se realizează prin intermediul protocolului RSVP de rezervare a resurselor (Resource Reservation Protocol). Acest model are dezavantajul că da naştere unui volum semnificativ de trafic de control, care duce la utilizarea ineficientă a benzii. [11]

Se foloseşte o semnalizare de tip capăt la capăt între entitatiile comunicante pentru a se rezerva resursele necesare nodurilor reţelei. Această semnalizare foloseşte protocolul RSVP – Resource Reservation Protocol, ce ajută la

transportarea și instalarea stărilor de rezervare în noduri. Însă acest protocol prezintă și o serie de dezavantaje precum necesitatea folosirii semnalizării per flux între entități sau, cele mai importante, dezavantajele legate de scalabilitatea soluției. În ceea ce privește problema scalabilității, aceasta este datorată faptului că într-o rețea poate exista un număr foarte mare de stări într-un nod, iar astfel, traficul de menținere a rezervării poate spori problema congestiei linkului.[5]

RSVP poate fi folosit şi pentru distribuţia de etichete, utilizând anumite extensii ale acestuia, însă acest lucru este posibil doar în partea de core a reţelei datorită problemei de scalabilitate. Această practică prezintă și avantajul modalității de rezervare pe clase de echivalență și nu pe fluxuri individuale, diminuând considerabil numărul de stari si de semnalizări folosite.

Dacă se doreşte modificarea numărului de resurse folosite în mod curent pentru cale, acesta poate fi modificat cu ajutorul mesajelelor PATH. Astfel, calea ar primi o nouă rezervare în timp ce este folosită. Totuşi, dacă din diverse motive, rezervarea nu se poate face, calea va fi ştearsă şi traficul de date va fi întrerupt. Pentru a remedia această problema posibilă, mai există un mod în care se pot cere resurse suplimentare. Calea iniţială este menţinută, dar în acelaşi timp este realizată altă cale cu anumiţi parametrii de trafic doriţi. În momentul în care calea secundară este gata, traficul este dirijat prin ea şi calea originală este ştearsă. În acest caz, dacă calea secundară nu poate fi construită, calea principala rămâne în folosinţă şi nu apar întreruperi în trafic. [3]

Pe lângă protocolul RSVP-TE, pentru modificările ce țin de alocarea de bandă se mai folosește și CR-LDP care permite crearea unei căi de comutație a etichetelor, având o anumită bandă garantată. De asemenea, parametrii acestor cai pot fi modificaţi pe timpul funcţionarii caii, fără a fi nevoie să se şteargă calea principală. CR-LDP are avantajul de a fi un protocol de tip Hard State, neavând nevoie de semnalizări permanente pentru a putea menţine o cale, spres deosebire de RSVP-TE. Din acest motiv CR-LDP este preferat în reţele MPLS foarte mari, unde RSVP-TE poate să nu fie foarte scalabil. [3][11]

B. Modelul Serviciilor Diferențiate

Diferențierea serviciilor este necesară pentru a satisface diverse cerințe ale aplicațiilor și utilizatorilor dar și pentru a diferenția prețurile serviciilor. Principalul obiectiv al arhitecturii este de a oferi mecanisme scalabile pentru clasificarea traficului, cu scopul de a perimite fiecărei clase de trafic să fie tratată în mod diferit pentru a-și îndeplini sarcinile. Astfel, putem spune că modelul serviciilor diferențiate conține două componente principale:

- Condiţionarea traficului – Se realizează doar la marginea domeniului și include elemente precum policing, colorare şi shaping.
- Comportamentul în fiecare nod (Per-hop behaviour) – are la bază mecanismul de rapartizare în cozi, precum și cele de planificare și repartizare.

Principalele funcții ale acestui model includ metodele de măsurare, marcare, formare, precum și de aplicare a politicilor asupra traficului. Acest serviciu este oferit doar în interiorul unui domeniu de tip Diffserv, acătuit dintr-un set de noduri cu același tip de compotrtament- PHB și care aplică anumite reguli asupra traficului.[12]

Datorită anumitor SLA-urilor stabilite în contractul încheiat pentru achiziționarea unui astfel de serviciu, nodul de intrare are sarcina de a verifica dacă traficul de la intrare respectă regulile agreate. In cazul în care traficul receptionat nu respectă specificațiile tehnice, atunci traficul va fi marcat ca fiind neconform.

Pe baza anumitor câmpuri din antetul pachetelor de nivel trei, traficul de la intrare va fi asociat unui BA – Behaviour Aggregate și va primi un anumit cod DSCP. După ce este clasificat de nodurile de la intrare, traficul nu va mai fi reclasificat de celelalte noduri ci doar vor fi aplicate noi seturi de reguli. [9]

Clasificarea pachetelor

Primul lucru necesar pentru a aplică arhitectură DiffServ este abilitatea de a clasifică pachetele. Clasificarea este acţiunea de a examina un pachet pentru a hotărî ce fel de reguli trebuie să urmeze, şi ulterior, ce marcaj DSCP sau EXP trebuie să primească. În principal, clasificarea este realizată în funcție de codul DSCP.

Clasificarea pachetelor IP

Pachetele IP pot fi clasificate uşor. Se pot face comparaţii după orice câmp IP, dar în general se foloseşte adresa IP destinaţie, adresa IP sursă sau valoarea DSCP.Nu este necesar un algoritm de clasificare complex, deoarece ar trebui să implice o reducere a perfomanțelor de calitate. De aceea este folosită o analiză de nivel 4 a tipurilor de protocoale pentru realizarea unei clasificări mai rapide.[14]

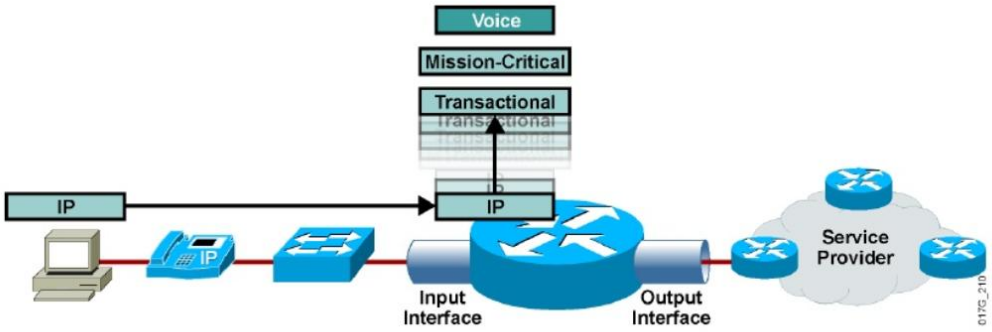

Figura 2. Procesul de clasificare al pachetelor

Clasificarea pachetelor MPLS

Clasificarea pachetelor de tip MPLS într-un domeniu pentru Diffserv este posibilă doar după valoarea biților EXP existenți în eticheta din vârful stivei. Deoarece există riscul eliminării antetului de nivel 2 nodurile de intrare nu vor analiza alte etichete ori informații de nivel 3.[13]

Policing

Funcţia de policing implică măsurarea traficului utilizatorului şi compararea măsurătorii cu un contract de servicii încheiat cu furnizorul. Practic, nu se permite traficului nefolositor să intre în rețea în cazul în care acesta depășește capacitatea cozilor. [16]

Acest procedeu intervine la marginea rețelei, de accea toate pachetele care intră în rețea sunt de tip IP. Excepțiile sunt cele în care este implicată o arhitectură de tip Carrier Supporter, ce implică oferirea unor servicii de transpot altui furnizor, dacă aceștia sunt de acord să folosească în comunicarea dintre aceștia trafic de tip MPLS.[13]

Marcarea

Această etapă este legată de regulile de policing, deoarece, așa cum a fost expus anterior, traficul rezultat în urma procedeelor este marcat a fi conform sau

neconform, însă acestea nu sunt dependente. De exemplu, între cele două valori DSCP a pachetului IP, respectiv valoarea EXP, se poate face mappig. Biții EXP pot lua valoarea 0 sau pot avea setată această valoare, atunci când nu dorim să avem o anumită calitate pentru diverse servicii. În cazul în care un client dorește o categorie de servicii în plus care să întregească atribuțiile serviilor de calitate, este posibilă marcarea traficului care intră pe o anumită interfață.[2]

Prin faptul că marcarea se face în antetul de nivel 2,5 nodurile MPLS nu trebuie să analizeze câmpul Precedence din pachetele de tip IP pentru a hotărî tipul de tratament ce trebuie aplicat pachetului. Acest lucru este practicat deoarece în cazul unei analize de nivel 3, există posibilitatea ca operatorul rețelei de tip MPLS poate aloca pachetul unei anumite clase, fară a modifica clasa inițială. Astfel, la ieşirea din domeniul MPLS, pachetul clientului poate beneficia din nou de privilegiile cerute.[16]

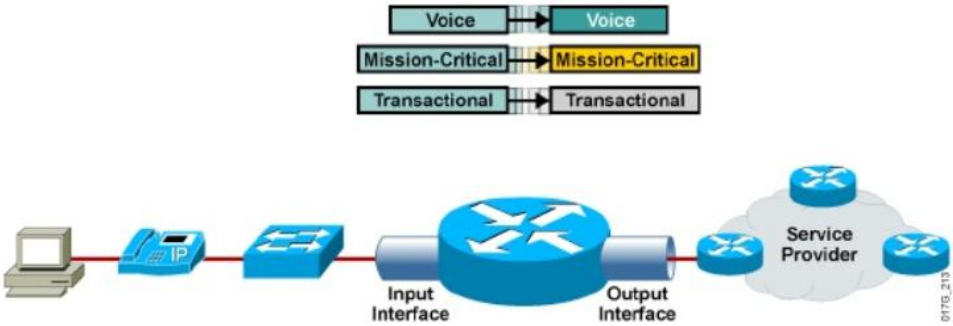

Figura 3. Procesul de marcare al pachetelor

Marcarea pachetelor IP

Antetul IP a evoluat continuu de-a lungul timpului din punct de vedere al marcării calităţii serviciilor. La început, câmpul Type of Service, cunoscut sub abrevierea ToS, era compus din 3 biți de precedență și încă 4 pentru marcarea serviciului dorit. Primii trei aveau scopul de a alege un anumit tratament, unde valorile cuprinse între 0 și 5 conțineau datele utilizatorului, iar cele cuprinse între 6 și 7 marcau traficul de control din rețea. Deşi Diffserv pune la dispoziţie 64 de clase de trafic, numai 15 au fost definite şi în practică, un furnizor poate implementa mai puţine.

Nume	*DSCP (zecimal)*	*DSCP (binar)*
Best effort	0	000000
AF11	10	001010
AF12	12	001100
AF13	14	001110
AF21	18	010010
AF22	20	010100
AF23	22	010110
AF31	26	011010
AF32	28	011100
AF33	30	011110
AF41	34	100010
AF42	36	100100
AF43	38	100110
EF	46	101110

Tabelul 1. Clase de trafic folosite în Diffserv

Marcarea pachetelor MPLS

În cazul în care este dorită realizarea unei relații între DSCP și EXP apare problema stocării pe 6 biți a DSCP și pe 3 biți a EXP. Cei trei biți EXP sunt folosiți pentru codificare în cadrul rețelelor în care multiprotocolul MPLS funcționează în mod cadru. De aceea, este necesară corespondența dintre codurile DSCP și marcajele EXP. Pentru linkurile de tip ATM care folosesc acești trei biți în combinație cu etichetele utilizate, este posibilă oferirea mai multor clase de serviciu, deși în mod normal sunt folosite doar 8. Acest procedeu este cunoscut sub abrevierea L-LSP sau Label Only Inferred LSP. [15]

Repartizarea în cozi

În cadrul acestei etape se realizează atât repartizarea în cozi, cât și selectarea planificatorului care are scopul de a servi cozile, în funcție de platformă. Aceste tehnici pot fi aplicate pentru traficul MPLS, deoarece se regăsesc foarte des asupra celui Diffserv IP. Planificatorul folosit în acest context este cel Weighted Fair Quering, iar coada folosită este una de tip First In First Out.[17][13]

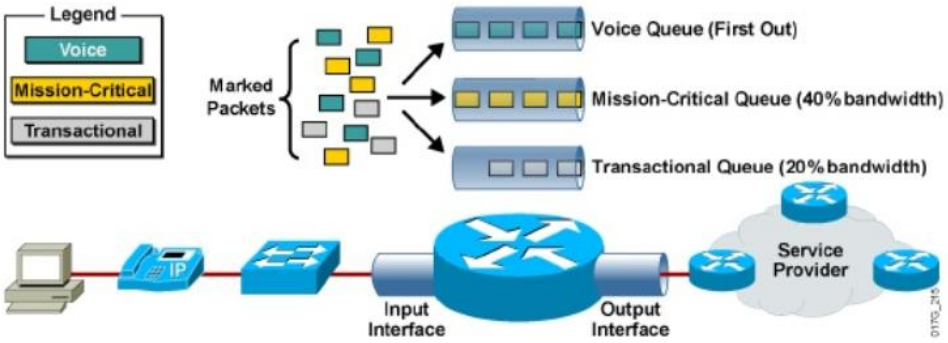

Figura 4. Repartizarea în cozi a pachetelor

Aruncarea pachetelor

Procesul de aruncare al pachetelor este poate cel mai important din cadrul protocolului MPLS, deoarece menține în limite dimensiunile cozilor asociate. Un alt avantaj este că acesta este principalul mod de a reduce debitul surselor TCP în scopul de a reduce rata de transmisie. Principiul care stă la baza acestuia este urmatorul: se preferă aruncarea unor pachete în cazul unei congestii față de pierderea celor care urmează să intre în nodul respectiv. Pentru acest lucru este folosit algoritmul Weighted Random Early Detection. [17] [16]

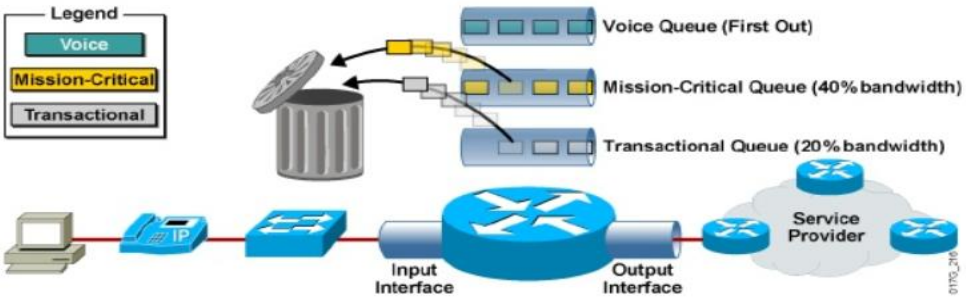

Figura 5. Aruncarea pachetelor

2. Implementarea QoS prin MPLS

Tehnologia MPLS a fost dezvoltată astfel încât să fie compatibilă cu protocolul IP. De fapt scopul primar al acesteia este de a transporta eficient şi rapid pachete IP. Că urmare, la implementarea unei soluţii QoS prin MPLS, scopul principal este că această soluţie să suporte modelele existente IP QoS. Scopul final este implementare QoS cap la cap (end to end).

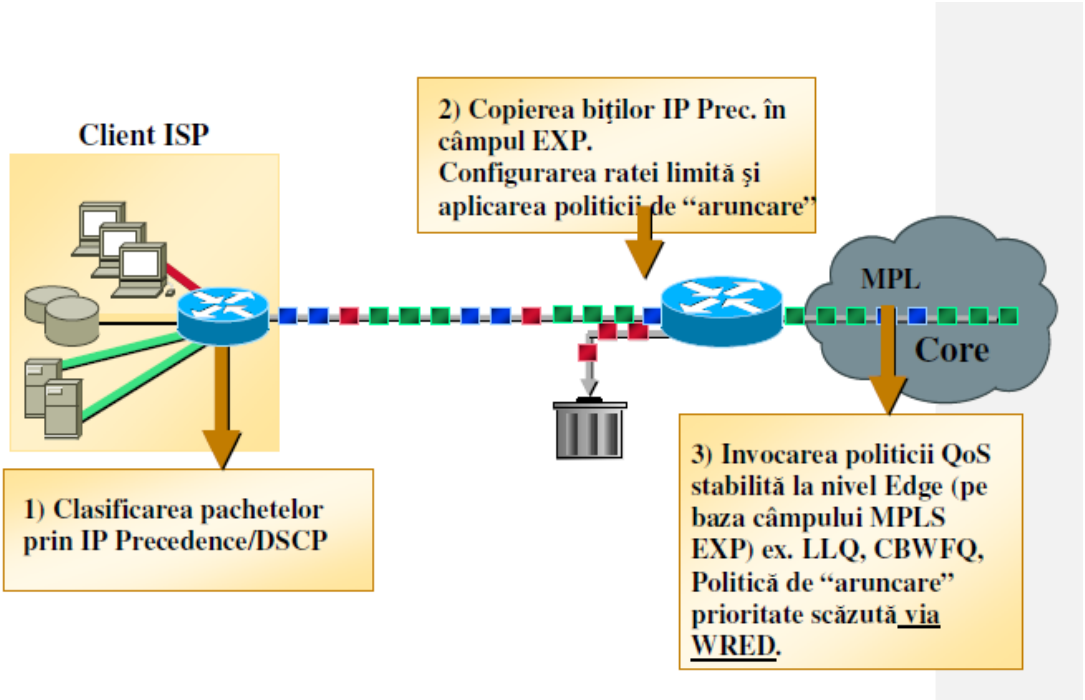

Figura 6. Funcţionarea MPLS QoS

În figura 6 este exemplificat modul de funcţionare al politicii QoS între o reţea de tip MPLS şi una de tip IP. Acest exemplu poate fi interpretat ca o comunicare între furnizorul de servicii inernet şi un client al acestuia. Din punctul de vedere al implementării acesteia nu apar probleme de compatibilitate deoarece biţii de tip IP Precedence sunt copiaţi în câmpul EXP aferent pachetelor MPLS. Ulterior, eticheta MPLS este îndepărtată, lăsând nemodificati biţii IP Precedence. [4]

În afară de mecanismele de prioritizare a traficului, una din cerinţele unei reţele care are implementată o politică de QoS este şi securizarea informaţiilor. Comutatia de etichete izolează traficul pe rute virtuale (Label Switched Paths sau LSP) în funcţie de eticheta fiecărui pachet. Forţă acestui mecanism constă în faptul că se restricţionează accesul asupra configurării. Altfel spus, numai furnizorul de

servicii poate instala rutele virtuale şi tot el determina cine le poate accesa. Nu există nici o posibilitate pentru un utilizator care transmite mesaje pe conexiunea lui normală, să reconfigureze ruta virtuală sau circuitul virtual pentru a se conecta la aceea a altui utilizator. Tocmai această caracteristică a comutaţiei de etichete permite furnizorilor de servicii să ofere reţele private virtuale prin intermediul unei infrastructuri MPLS partajate. Această facilitate nu este însă una standard care să se regăsească şi într-o reţea IP nativă, ci este specifică MPLS. [4][1]

Acesta este nivelul de securitate de baza oferit de reţeaua MPLS care este comparabil cu cel disponibil prin intermediul reţelelor de tip Frame Relay sau ATM. Cu toate acestea, anumite situaţii pot să necesite criptarea datelor atunci când ele sunt transmise de la o locaţie distanţă la altă. De exemplu, dacă avem o transmisie prin satelit, criptarea este absolut necesară, deoarece conexiunea este disponibilă oricui dispune de un receptor adecvat şi se află în rază de acţiune a respectivului satelit.

Implementarea funcţiilor QoS în cadrul infrastructurii unei reţele MPLS oferă o serie de beneficii, atât pentru furnizorii de servicii Internet, cât şi pentru clienţi. În ceea ce îi priveşte pe furnizorii de servicii, îmbunătăţirile legate de calitatea serviciilor pentru MPLS le permit acestora să clasifice pachetele în funcţie de tipul lor, de interfaţă de intrare, sau de alţi factori, prin marcarea fiecărui pachet fără a modifică structura pachetului clasic IP. De exemplu, furnizorii de servicii pot să clasifice pachetele fără a ţine cont de nivelul de prioritate pe care îl are pachetul atunci când ajunge la primul router de transport. De asemenea, ei pot să ţină cont de această prioritizare iniţială şi să aplice una suplimentară. Faptul ca potentialii clienti ale acestor implementari se pot baza pe o criptare adecvata, pe debite minime si multe altele, reprezinta beneficii care pot imbunatatii solutiile de business.[7]

DiffServ-Aware Traffic Engineering (DS-TE)

Utilizand un mecanism control-plane numit DS-TE ce are ca principal scop obtinerea abilitatii de a rezerva randul pentru largimea de banda, se ajunge la posibilitatea de construire a TE-LSP care seteaza rezervarea de subpool a largimii de banda. Deoarece pe aceasta portiune de banda se va transporta doar trafic LLC, acest lucru va duce la crearea unei a doua retele, diferite de prima dar peste care se va suprapune. [12]

2.1. Detectarea de erori MPLS

În continuare vom analiză procesul de detecţie de erori şi protocoale în reţelele MPLS, inclusive detecţia unui LSP invalid, precum şi recupararea LSP.

Separarea între planul de control şi de date

Separarea între planul de control şi de date este direct atribuită formatului şi evoluţiei unui pachet OAM. Formatul unei etichete de tip stivă, ce reprezintă header-ul pentru pachetele MPLS, este format dintr-o eticheta valoare (20 biţi), bîţîi EXP (3 biţi), bit-ul S (1 bit), şi TTL (8 biţi). [6]

Pentru a face diferenţa între un pachet OAM şi un pachet de tip date, se pot folosi diferite metode. ITU-T Y.1711 foloseşte o eticheta de tip stivă cu două intrară. Prima eticheta are aceeaşi valoare că eticheta de transport, asigurând că în majoritatea cazurilor pachetele OAM pot fi rutate pe aceeaşi cale că pachetul user.

A două eticheta are o valoare specială rezervată, 14, pentru a fi diferentiata de pachetul user. Totuşi, introducerea celei de-a două etichete poate să nu fie complet compatibilă cu algoritmul de echilibrare a sarcinilor deja existent, că atare poate să nu funcţioneze corect în reţelele ECMP deja existente.[7] Mai mult, în reţelele unde se foloseşte PHP, pot apărea mai multe limitări, acest lucru fiind subliniat în tabelul 2.

O altă opţiune este de a separa pachetele OAM de pachetele date prin folosirea de sarcina MPLS un pachet specific de IP destinat unui port deja cunoscut, precum în MPLS ping.

În acest caz eticheta de transport este acceaşi că în pachetul de date. Această metodă, totuşi, presupune că adresa destinaţie să fie o adresa non-rutabila, pentru a asigura că pachetul IP va fi procesat de routerul processor al router-ului de “ieşiri”. În acest caz se permite suportul PHP şi un ECMP limitat. [8]

Alte metode de a separa planul de control de date sunt moduri hibride, unde un pachet OAM poate fi identificat că o eticfeta specifică sau prin folosirea unui câmp specific din pachet ce face posibilă recunoaşterea uşoară. VCCV (Verificarea Conectivităţii Circuitelor Virtuale) se bazează pe această tehnică.

	Y.1711	MPLS ping/traceroute
Hardware	"Probabil" are nevoie de un hardware now (scalabilitate, manipulare TTSI,…)	Foloseste hardware-ul existent
Aplicabilitate	• In principal un mechanism de detective • Conexiune de tip punct-la-punct LSP • Detectie de LSP de tip conexiune eronata, bransa eronata	• In principal o metoda de depanare • LDP, RSVP-TE, orice alta metoda de semnalare MPLS • Detectarea consistentei FEC • Depanare: localizarea problemei si depistarea hop-by-hop
Favorabil ECMP	NU, foloseste etichete rezervate, poate afecta echilibrarea sarcinilor daca ECMP apare in timpul unui LSR	DA, algoritmi ECMP ce vor verifica toatea cele 127/8 adrese
Favorabil PHP	Exista o limitare in functie de tipul de PHP (16)	DA
Scalabilitatea/Frecventa	• Injectarea de pachete la fiecare secunda • Necesita administrarea TTSI • Calculari BIP 16	• Frecventa este impusa de operator • Foloseste informative native • Verificare ciclica a redundantei IP
Acord privind nivelul serviciilor	NU	NU

Tabelul 2. Y.1711 versus funcționalitatea ping/trace MPLS

Detecţia unei etichete LSP eşuate

Eşuarea unei etichete LSP necesită testarea de fluxuri de pachete, înafara de erori de tip network, deoarece în multe instanţe fluxul de pachete poate fi întrerup fără a fi sesizată reţeaua (link-ul/nodul). Acest lucru poate fi cauzat de probleme în

tabela de routare, unei legături de etichete eronate, aglomerarea reţelei, sau alte cauze. [10]

Verificarea conectivităţii, precum şi ping/traceroute a unei funcţii OAM sunt sugerate pentru acest tip de detectări de erori. Implementarea acestor protocoale poate fi diferită, depinzând de tehnologia pachetului.

Indiferent de tehnologia folosită, este important că pachetele OAM să folosească aceeaşi cale ca pachetele de date obişnuite.

Scenarii de defectare LSP

ITU-T Y.1711 a standardizat funcţia de verificarea conectivitatii (CV), în timp ce detecţia de redirecţionare bidirecţională (BFD) este studiată de IETF.

Figura 4.2 arată diferite scenarii de defectare.

A' si B' sunt receptorul intentionat pentru A si B, respective.

Scenariile de defectare sunt:

a) Pierderea de conexiune
b) Conexiunea eronata
c) Conexiune schimbata
d) Fuzionarea gresita
e) Loop/ replicare neintentionata

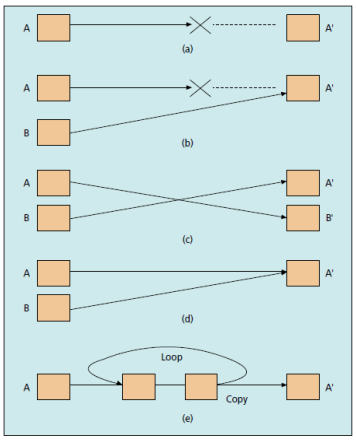

Figura 7. Scenarii de defectare LSP

2.2. Protecția și recuperarea MPLS

Protecţie şi recuperarea pot fi de tip local sau global. Protecția globală I se aplică unui LSP de tip end-to-end, în timp ce protecția locală I se aplică unui link sau nod eronat. Protecţia locală în general da un timp de convergenţă mai mic fiindcă mesajul eronat este procesat de notdul local (link protection) sau an nod imediat adiacent (node protection). Timpul de convergenţă este de circa 50 ms, fiind unul acceptabil. Protecţia cailor necesită un timp de convergenţă mai mare, deoarece mesajele de eroare trebuie să se propage către capătul reţelei, ceea ce iniţiază mecanismul de protective. [4]

Cele mai simple metode sunt 1+1 şi 1:1 arhitectură de protecţie de comutare specificat de ITU-T Y.1720.

În ceea ce priveste ahitectura 1+1, LSP-ul de protectie poate fi folosit pentru a transmite alt trafic când nu este folosit. În general, traficul este copiat si trimis catre LSP-ul acutal si cel de protectie simultan.

Bazat pe protocolul de semnalizare folosit, sunt posibile diferite opţiuni. De exemplu, o reţea de tip LDP se poate baza pe o convergenţă IGP rapidă şip e o disponibilitate ridicată pentru îmbunătăţirile de tip LDP. O reţea de tip RSVP_TE permite folosirea de multiple cai explicite când semnalizează un LSP. Mai mult, RSP_TE a fost îmbunătăţit pentru a permite repararea locală a unui tunel LSP prin realizarea unei “evitări” LSP ce oernute un singur tunel de backup pentru a proteja LSP-urile primare (modelul de portectie n:m).[6]

2.3. Mentenanța serviciilor de tip punct-la-punct și multipunct

Furnizorii de servicii de telecomunicaţii au asigurat de mult timp servicii punct-la-punct, cu cadrul OAM deja dezvoltat.

Tipic, interfetele utilizator-reţea (UNI) sunt folosite pentru a caracteriza punctele de ataşament ale clientului/furnizorului. În cazul multipunct, N>2, este nevoie de UNI, fiecare UNI având un profil de trafic recepţionat (traficul injectat în serviciul furnizorului) şi un profil de trafic trimis (traficul de iese din reţeaua furnizorului). Pentru un UNI dat, traficul recepţionat poate fi trimis către toate

celelalte UNI, către unele UNI, sau către oricare alt UNI, depinzând de serviciul furnizat. Poate fi necesar că QOS să fie initializat, ceea ce implică definirea de pierdere de pachete şi de întârzieri garantate. Asemenea garanţii poate sunt necesare să fie puse pe fiecare UNI, întrucât vitezele interfetelor diferitelor link-uri pot fi implicate. [9]

Odată definite SLA-urile, problema constă în reservarea de resurse pentru a asigura performanţă obiectivelor din SLA-uri, şi realizarea de ingineria traficului la serviciile multipunct. În final, protecţia necesară va fi adresată pentru serviciile multipunct, din moment ce metodă de protecţie pe fiecare ruta folosită pentru serviciile punct-la-punct poate să nu scaleze cu serviciile multipunct, având N*(N-1) rute implicate într-un serviciu multipunct de N noduri, în special dacă QOS este implicat.

Concluzii

Din punct de vedere practic, se poate observa faptul că două fluxuri de date similare au un comportament diferit atunci când tranzitează rețeaua, chiar dacă sursa și destinația acestora este aceeași.

De cele mai multe ori, multiprotocolul MPLS este utilizat împreună cu serviciile diferentțiate Diffserv pentru a crea o rețea pe bază de IP modelată de QoS.

O rețea IP QoS este flexibilă la întreruperile naturale și pe cele bazate pe DoS și de asemenea gestionează congestia apărută în timpul transmiterii de date, având ca scop principal oferirea unei calități consistente a vocii.

Furnizorii de servicii lucrează la standarde pentru a furniza serviciile QoS consistente chiar și în interiorul granițelor rețelei proprii.

Folosirea Serviciilor Diffserv permite crearea unor nivele de calitate bazate pe cerințele clienților, în timp ce protocolul MPLS se poate adapta cu costuri minime la orice mediu fizic.

Bibliografie

[1] Octavian Catrina , Note de Curs: *Arhitecturi şi protocoale de comunicaţii*

[2] Banica Ion, Note de Curs: *Comunicaţii de Date*

[3] Eugen Borcoci, *Note de Curs: Reţele şi servicii*

[4] Ivana Huckova, Martin Hruby - *QoS-based optimization of data flow in MPLS networks*, disponibil la http://ieeexplore.ieee.org/document/7061851/, accsesat la data 20.01.2018

[5] Ankur Dumka, Hardwari Lal Mandoria, Vibudh Fore, Kanchan Dumka - *Implementation of QoS algorithm in integrated services (IntServ) MPLS network* , disponibil la http://ieeexplore.ieee.org/document/7100407/, accesat la data 20.01.2018

[6] *E. Rosen, A. Viswanathan, R. Callon - Multiprotocol Label Switching Architecture*, 2001, disponibil la https://tools.ietf.org/html/rfc3031, accesat la data 25.01.2018

[7] Ashiq Khan, Wolfgang Kiess, David Perez-Caparros, Joan Triay- *Quality-of-service (QoS) for virtual networks in OpenFlow MPLS transport networks*, disponibil la http://ieeexplore.ieee.org/document/6710552/, accsesat la data 20.01.2018

[8] Chin-Ling Chen- *A proposal of next generation network: QoS mapping for MPLS-DiffServ and label forwarding*, disponibil la http://ieeexplore.ieee.org/document/6512903/, accsesat la data 22.01.2018

[9] A. Saika, R. El Kouch, B. Raouyane, M. Bellafkih, M. M. Himmi- *QoS in the MPLS-DiffServ network*, disponibil la http://ieeexplore.ieee.org/document/6481964/, accsesat la data 22.01.2018

[10] S. Kulkarni, R. Sharma, P. Sharan, R. B. R. Gowd- *New dynamic QoS routing algorithm for optical networks based on MPLS with delay and Bandwidth as constraints*, disponibil la http://ieeexplore.ieee.org/document/6409588/, accsesat la data 22.01.2018

[11] Ankur Dumka, Hardwari Lal Mandoria, Vibudh Fore, Kanchan Dumka-*Implementation of QoS algorithm in integrated services (IntServ) MPLS network*, disponibil la http://ieeexplore.ieee.org/document/7100407/, accsesat la data 22.01.2018

[12] Huibin Zhang, Yongli Zhao, Dahai Han, Jie Zhang, Jianchao Xing- *QoS sensitive routing in DiffServ MPLS-TP networks*, disponibil la http://ieeexplore.ieee.org/document/5620187/, accsesat la data 22.01.2018

[13] Aldous Phelps – *MPLS and DiffServ*, disponibil la http://slideplayer.com/slide/6848697/, accesat la 01.02.2018

[14] Rajesh Shinde – *QoS Deployment Experiences*, disponibil la https://www.slideshare.net/advojoy/shinde-qosmplstutorial, accesat la 29.01.2018

[15] Alexei Chpenst- *A Traffic Engineering System for DiffServ/MPLS Network*, disponibil la http://doras.dcu.ie/17195/1/alexei_chpenst_20120705115729.pdf, accesat la 27.01.2018

[16] QoS Protocols, disponibil la https://www.cisco.com/c/en/us/tech/quality-of-service-qos/index.html, accesat la 19.01.2018

Lista figurilor

Figura 1. Modelul OSI

Figura 2. Procesul de clasificare al pachetelor →
http://images.myshared.ru/9/887790/slide_5.jpg

Figura 3. Procesul de marcare al pachetelor →
https://image.slidesharecdn.com/presentacionproydesa-qos-100625180905-phpapp02/95/cisco-qos-27-728.jpg?cb=1277490077

Figura 4. Repartizarea în cozi a pachetelor →
h*ttps://image.slidesharecdn.com/presentacionproydesa-qos-100625180905-phpapp02/95/cisco-qos-36-728.jpg?cb=1277490077*

Figura 5 Aruncarea pachetelor → *https://image.slidesharecdn.com/presentacionproydesa-qos-100625180905-phpapp02/95/cisco-qos-37-728.jpg?cb=1277490077*

Figura 6. Funcționarea MPLS QoS

Figura 7. Scenarii de defectare LSP