ŠIROKOPOJASNE TELEKOMUNIKACIONE MREŽE
– Poglavlje 4 –

4 MPLS

IP mreže predstavljaju uz eternet mreže (koje u suštini rade na drugom sloju OSI modela) najpopularnije paketske tehnologije. IP mreže se baziraju na IP mrežnom protokolu, pri čemu u praksi egzistiraju dve verzije IP protokola - IPv4 i IPv6 verzije. IP protokol je baziran na principu najboljeg pokušaja (*best effort*), pri čemu se koristi CL (*ConnectionLess*) princip konekcije. Putanja paketa kroz mrežu se određuje u svakom ruteru ponaosob, pri čemu ruteri donose odluke o prosleđivanju na osnovu rada protokola rutiranja poput OSPF, RIP, BGP i dr. Ovo svojstvo potiče iz primarnog cilja IP mreža u njihovim počecima, a to je da IP mreže budu robusne, i da paket uvek dođe do svog cilja ako postoji bar jedan ispravan put kroz mrežu između izvorišta i odredišta. Navedeno svojstvo potiče od originalnog zahteva Ministarstva odbrane SAD koje je želelo kreirati veoma robusnu mrežu koja bi radila i u otežanim uslovima gde mreža trpi značajna oštećenja u infrastrukturi.

Međutim, IP mreže su se proširile i na civilni sektor i postale najznačajnija paketska tehnologija koja je, između ostaloga, predstavljena u vidu globalne Internet mreže, pa se javio problem potrošnje IP adresa. Stoga je uvedeno besklasno adresiranje u kome mrežni deo adrese može da ima proizvoljnu dužinu, za razliku od prvobitnog klasnog adresiranja. Ovo je dovelo do problema implementacije efikasnih mehanizama usmeravanja paketa u ruterima. Ruteri su sadržavali tabele usmeravanja koje su se pretraživale na osnovu odredišnih IP adresa u paketima. Pošto je mrežni deo bio nepoznate dužine pretraga je bila komplikovana (dodatna komplikacija je bila mogućnost nalaženja više rešenja od kojih se biralo ono sa najvećim poklapanjem u skladu sa LPM (*Longest Prefix Matching*) pravilom) i došlo je do problema u proširivanjima kapaciteta rutera jer ruteri nisu mogli da rade usmeravanje na prevelikim brzinama. Stoga je predložena tehnika usmeravanja na bazi labela fiksne dužine na osnovu koje je nastala MPLS (*MultiProtocol Label Switching*) tehnika. Koren ove tehnike leži u ideji koju je pokrenula kompanija Ipsilon, a koju je posle razradila i uvela u svoje uređaje kompanija Cisco pod nazivom *tag switching*. IETF organizacija je potom standardizovala princip usmeravanja na bazi labela pod nazivom MPLS. Pošto je usmeravanje bilo na bazi kraćih labela fiksne dužine, implementacija pretrage tabela usmeravanja na bazi labela je bila jednostavna i podržavala je velike brzine. Pri tome, kao što naziv protokola MPLS sugeriše, usmeravanje na bazi labela je moglo da se koristi simultano za različite mrežne protokole (IP, IPX, AppleTalk...), ali u praksi je MPLS bio korišćen za IP protokol.

Uskoro je tehnologija dovoljno uznapredovala da podrži i usmeravanje na bazi odredišnih IP adresa na velikim brzinama, ali MPLS protokol je, ipak, opstao. Razlog opstanka MPLS protokola leži u činjenici da je upotreba MPLS-a omogućavala implementaciju naprednih servisa u IP mreže koje IP mreže originalno (samo sa IP protokolom) ne bi mogle adekvatno da podrže. Pre svega, formiranje tunela za kreiranje VPN (*Virtual Private Networks*) mreža, kao i podrška za QoS u IP mrežama. Naime, MPLS je uneo mogućnost formiranja kola (fiksnog puta) u IP mrežama čime je omogućeno i formiranje tunela, ali i pružanje QoS servisa nekom korisničkom toku, jer ako tok ne bi išao istim putem bilo bi teško adekvatno pružiti QoS uslugu toku (takođe, veoma teško bi bilo efikasno implementirati u klasičnoj IP mreži ispitivanje za svaki paket ponaosob kom toku pripada - na primer, morali bi se ispitivati pored polja IP zaglavlja i polja zaglavlja transportnog protokola što bi zahtevalo veliku moć procesiranja u ruterima pa bi ruteri trošili veću količinu resursa, dok je u MPLS mreži dovoljna samo labela pridružena paketu). U suštini, usmeravanje na bazi labela je veoma slično prosleđivanju ćelija u ATM mrežama, tako

da se može reći da je uvođenjem MPLS protokola u IP mreže dobijena podrška za određene funkcionalnosti iz ATM mreža koje IP mreže originalno nisu podržavale čime je IP tehnologija postala kompletnija i time se dodatno učvrstila kao najdominantnija paketska tehnologija. Napomenimo da se u današnjim mrežama implementiraju linkovi brzina do 100Gb/s (OTN mreže iz prethodnog poglavlja su standardizovale interfejse brzina do 100Gb/s), a uskoro će se instalirati i još veće brzine. Na nivou ovih brzina, usmeravanje paketa na bazi odredišnih IP adresa ponovo postaje kritično (naročito u slučaju velikih tabela usmeravanja sa više od 400000 zapisa) tako da se uloga MPLS protokola kao alternativa u prosleđivanju paketa ponovo aktuelizuje.

U okviru ovog poglavlja će prvo biti predstavljene dve osnovne arhitekture za QoS podršku u IP mrežama - diferencijalni servisi (DiffServ) i integisrani servisi (IntServ). Potom će biti izloženi osnovni principi MPLS protokola i usmeravanja paketa na bazi labela. Pošto je za rad MPLS protokola neophodan mehanizam za razmenu labela između rutera, biće izloženi najpoznatiji protokoli za razmenu labela LDP (*Label Distribution Protocol*) i RSVP-TE (*Resource Reservation Protocol - Traffic Engineering*). Na kraju poglavlja će biti ukratko izloženo proširenje MPLS protokola, GMPLS (*Generalized MPLS*) koji proširuje MPLS podrškom za dodatne mrežne tehnologije pored paketskih mreža.

4.1. Arhitektura za QoS podršku u IP mrežama

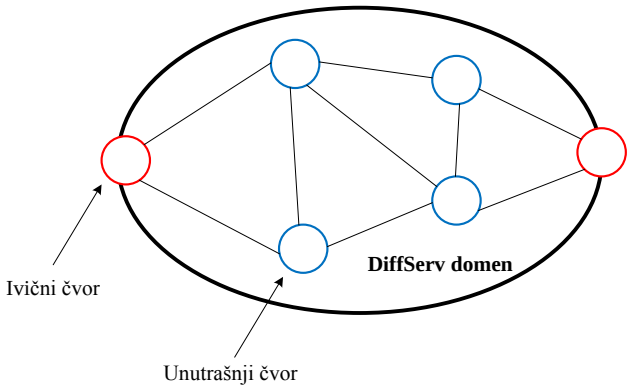
U okviru IP mreža su definisane dve osnovne arhitekture za QoS podršku u IP mrežama:

- DiffServ - diferencijalni servisi
- IntServ - integrisani servisi

Diferencijalni servisi se baziraju na ideji da se korisnički tokovi (tj. njihovi paketi) raspoređuju u odgovarajuće klase servise, i da se potom u ruterima vrši opsluživanje na nivou agregiranih tokova, odnosno da se pri opsluživanju koristi samo informacija kojoj klasi servisa pripada paket. U ovom slučaju nema razlikovanja individualnih tokova. Integrisani servisi se zasnivaju na ideji da se posmatraju individualni tokovi i da se individualnim tokovima rezervišu resursi na početku veze u svim ruterima kroz koje će dotični tok prolaziti. Opsluživanja u ruterima se stoga vrše na nivou individualnih tokova. Očigledno, diferencijalni servisi su skalabilniji tj. mogu da podrže više tokova, ali s druge strane je očigledno i da integrisani servisi mogu da pruže striktnije garancije kvaliteta servisa tokovima (naravno, postoje i druge razlike između ove dve arhitekture kao što ćemo videti u nastavku teksta). Otuda je generalna ideja da diferencijalni servisi budu zastupljeni u jezgru mreže gde je broj tokova ogroman, a da integrisani servisi budu zastupljeni po obodu mreže gde je broj tokova, ipak, manji. Ali, sama implementacija, ipak, dominantno zavisi od samih provajdera usluga. QoS u IP mrežama je i dalje otvorena oblast u kojoj se i dalje vrše istraživanja jer trenutna rešenja i dalje nisu idealna i ima prostora za značajna unapređenja. Tipični problemi su efikasna i ekonomična implementacija QoS podrške u ruterima, pružanje striktnih garancija, dogovor između provajdera u slučajevima veza koje prolaze kroz različite domene pod kontrolom različitih provajdera i pre svega problem kreiranja oblaka u kojem bi svi ruteri podržavali jednu ili drugu arhitekturu (teško je odjednom zameniti sve rutere, pa je moguće da korisnički tok prolazi i kroz rutere koji nemaju QoS podršku, čime se gubi mogućnost garantovanja QoS servisa, a taj problem je naročito izražen ako tok prolazi kroz više domena tj. velik broj rutera). U naredne dve sekcije će biti detaljnije izloženi principi obe arhitekture.

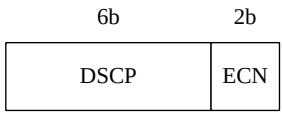
4.1.1. DiffServ

Osnovna definicija DiffServ arhitekture je izložena u preporukama RFC 2474 i RFC 2475. U okviru DiffServ arhitekture se definiše DiffServ domen kojeg sačinjavaju ruteri sa DiffServ podrškom i koji su pod kontrolom istog provajdera (slika 4.1.1.1). Ruteri na ivici domena se nazivaju ivičnim ili graničnim ruterima, a ruteri u unutrašnjosti domena se nazivaju unutrašnji ruteri.



Slika 4.1.1.1. DiffServ domen

Korisnici sa provajderom sklapaju dogovor (*SLA - Service Level Agreement*) u okviru koga definišu parametre svog saobraćaja i željeni kvalitet usluge koji mreža treba da pruži korisniku. Saobraćaj se tipično predstavlja u vidu parametara bušne kofe *b* i *r*, gde *b* predstavlja veličinu bursta, a *r* prosečan protok. Između DiffServ domena se takođe sklapa dogovor (SLA). SLA dogovor u oba slučaja može da se podesi statički (administratori domena vrše podešavanje), ali može i dinamički pomoću nekog protokola (na primer, RSVP). Da li će dogovor biti postignut ili ne zavisi i od trenutnih tokova u mreži, pa ako tok traži resurse koji ne mogu da se zadovolje dogovor neće biti postignut.



Slika 4.1.1.2. Struktura polja klase servisa u IP zaglavlju

Tabela 4.1.1.1 - Definisane DSCP vrednosti

DSCP	PHB (*Per Hop Behavior*) klasa servisa
000000	Difolt klasa (*best effort* saobraćaj)
101110	EF (*Expedited Forwarding*) klasa
001010, 001100, 001110, 010010, 010100, 010110, 011010, 011100, 011110, 100010, 100100, 100110	AF (*Assured Forwarding*) klasa
*xxx*000	CS (*Class Selector*) klasa

Tabela 4.1.1.2 - AF klasa

	Potklasa 1	Potklasa 2	Potklasa 3	Potklasa 4
Nizak prioritet	001010 (AF11)	010010 (AF21)	011010 (AF31)	100010 (AF41)
Srednji prioritet	001100 (AF12)	010100 (AF22)	011100 (AF32)	100100 (AF42)
Najviši prioritet	001110 (AF13)	010110 (AF23)	011110 (AF33)	100110 (AF43)

Korisnički tokovi se raspoređuju u odgovarajuće klase servisa. Klasa servisa se stavlja u odgovarajuće polje IP zaglavlja (*ToS* polje u IPv4 zaglavlju, odnosno *Traffic Class* polje u IPv6 zaglavlju). Struktura klase servisa je prikazana na slici 4.1.1.2. DSCP (*DiffServ CodePoint*) polje označava klasu servisa i dužine je 6 bita, dok preostala dva bita čine ECN (*Explicit Congestion Notification*) polje koje se koristi u mehanizmu eksplicitnog obaveštavanja o zagušenju u mreži kojim mrežni čvorovi mogu da obaveste korisnika na prijemu da je došlo do zagušenja u mreži (korisnik na prijemnoj strani tada može transportnim protokolom da obavesti korisnika na predajnoj strani da je došlo do zagušenja u mreži tj. ne mora se, na primer, čekati da TCP sam na osnovu gubitaka paketa u mreži detektuje zagušenje). Trenutno definisani DSCP kodovi su predstavljeni u tabeli 4.1.1.1. Difolt klasa predstavlja saobraćaj najboljeg pokušaja tj. *best effort* saobraćaj. EF klasa se koristi za saobraćaj koji je veoma osetljiv na kašnjenja i varijacije kašnjenja (džiter), odnosno za tzv. neelastičan saobraćaj koji ne dozvoljava varijacije kvaliteta servisa u svom opsluživanju (na primer, telefonski saobraćaj). EF klasa ima najviši prioritet pri opsluživanju, ali ako agregirani EF saobraćaj postane prevelik može doći do problema u kvalitetu opsluživanja, pa se za ovaj saobraćaj obavezno vrši procena da li može da se prihvati ili ne na osnovu trenutnih EF tokova u mreži. AF klasa pokušava da ostvari željene protoke korisnika, ali uz varijacije u opsluživanju agregiranih tokova u zavisnosti od trenutnog stanja u mreži. Ideja je da ovi tokovi dobiju bolje opsluživanje od *best effort* saobraćaja. Definišu se 4 potklase u AF klasi (što je veći redni broj potklase to je ona prioritetnija), pri čemu se za svaku potklasu dodatno definišu 3 nivoa prioriteta. Na ovaj način se može izvršiti finija klasifikacija korisničkog saobraćaja. Tabela 4.1.1.2 prikazuje DSCP vrednosti po potklasama. CS klasa je uvedena za kompatibilnost sa starijim sistemima koji su koristili najviša tri bita u ToS polju IPv4 zaglavlja za označavanje prioriteta saobraćaja (CS0-CS7 koji su određeni vrednošću xxx bita, pri čemu CS7 ima najviši prioritet, a CS0 najniži), iako se u suštini to veoma retko zaista i implementiralo. CS0 klasa je u suštini ekvivalentna difolt klasi tj. obe klase predstavljaju *best effort* saobraćaj i imaju istu DSCP vrednost.

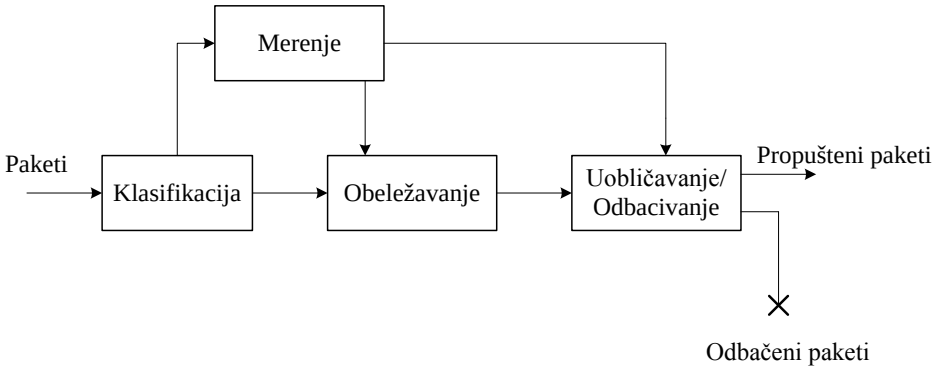
Tabela 4.1.1.3 - Osnovne karakteristike tipova saobraćaja

Tip saobraćaja	Karakteristike	Tolerancija na gubitke	Tolerancija na kašnjenje	Tolerancija na džiter
Mrežna kontrola	Paketi promenjive dužine, kratke poruke neelastičnih zahteva, potencijalno *bursty* saobraćaj	Niska	Niska	Visoka
Telefonija	Mali paketi fiskne dužine, konstantan protok male vrednosti, neelastični saobraćaj	Veoma niska	Veoma niska	Veoma niska
Signalizacija	Paketi promenjive dužine, tipično *bursty* saobraćaj i kratko trajanje sesije	Niska	Niska	Visoka
Multimedijalna konferencija	Paketi promenjive dužine, konstantni intervali slanja, adaptivan protok, osetljiv na gubitke	Niska do srednja	Veoma niska	Niska
Interaktivnost u realnom vremenu	RTP/UDP tokovi, uglavnom promenjiv protok, neelastični saobraćaj	Niska	Veoma niska	Niska
Multimedijalni striming	Paketi promenjive dužine, adaptivan i promenjiv protok	Niska do srednja	Srednja	Visoka
Brodkast video	Konstantan ili promenjiv protok, neelastičan saobraćaj, nije *bursty* prirode	Veoma niska	Srednja	Niska
Podaci osetljivi na kašnjenje	Promenjiv protok, *bursty* tokovi kratkog trajanja, elastičan saobraćaj	Niska	Niska do srednja	Visoka
OAM	Paketi promenjive dužine, elastični i neelastični saobraćaj	Niska	Srednja	Visoka
Podaci visokog protoka	Promenjiv protok, *bursty* tokovi dugog trajanja	Niska	Srednja do visoka	Visoka
Podaci niskog prioriteta	Elastični saobraćaj koji nije u realnom vremenu	Visoka	Visoka	Visoka

U preporuci RFC 4594 je navedena preporučena klasifikacija za različite tipove saobraćaja da bi se postiglo optimalno opsluživanje tokova u DiffServ domenu. Tabela 4.1.1.3 prikazuje osnovne karakteristike i zahteve tipova saobraćaja, a tabela 4.1.1.4 prikazuje preporučenu klasifikaciju tipova saobraćaja po DiffServ klasama. Sav preostali saobraćaj koji ne može da se svrsta u navedene tipove saobraćaja predstavlja *best effort* saobraćaj kojem se dodeljuje DSCP vrednost 000000 tj. difolt klasa, što je isto što i CS0 klasa.

Tabela 4.1.1.4 - Preporučena klasifikacija tipova saobraćaja

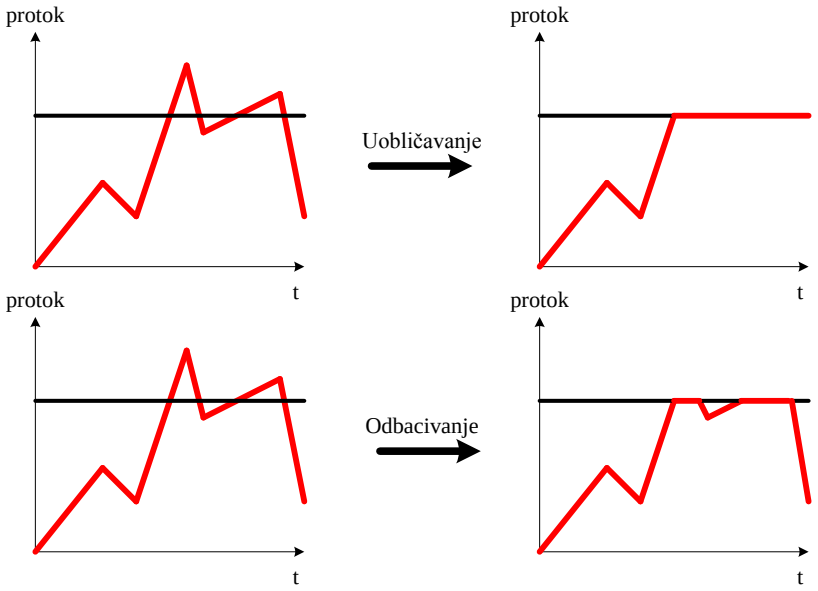
Tip saobraćaja	Klasa servisa	DSCP vrednost	Primer aplikacije
Mrežna kontrola	CS6	110000	Protokoli rutiranja
Telefonija	EF	101110	IP telefonija (VoIP)
Signalizacija	CS5	101000	IP telefonska signalizacija (VoIP signalizacija)
Multimedijalna konferencija	AF41,AF42,AF43	100010, 100100, 100110	H.323 video konferencija
Interaktivnost u realnom vremenu	CS4	100000	Interaktivno igranje
Multimedijalni striming	AF31,AF32,AF33	011010, 011100, 011110	Striming video/audio na zahtev
Brodkast video	CS3	011000	Brodkast TV
Podaci osetljivi na kašnjenje	AF21,AF22,AF23	010010, 010100, 010110	Klijent/server transakcije
OAM	CS2	010000	OAM
Podaci visokog protoka	AF11,AF12,AF13	001010, 001100, 001110	Uskladišti i prosledi aplikacije
Podaci niskog prioriteta	CS1	001000	Aplikacije za prenos podataka koje nemaju garancije protoka



Slika 4.1.1.3. Procesiranje korisničkih paketa u ulaznom ivičnom ruteru

Granični čvorovi, koji primaju korisnički tok u DiffServ domen, vrše procesiranje paketa korisničkog toka kao što je prikazano na slici 4.1.1.3. Funkcija klasifikacije vrši ispitivanje zaglavlja paketa (pre svega IP zaglavlja, ali može da se ispituje i transportno zaglavlje (TCP, UDP...), pa čak i aplikacioni deo paketa, kao i interfejse na koji je paket pristigao) da bi odredila kojoj klasi servisa pripada paket. Potom, funkcija obeležavanja vrši dodelu odgovarajuće klase paketu u IP zaglavlju. Funkcija obeležavanja postavlja odgovarajuću vrednost DSCP koda u IP zaglavlju paketa. Funkcija uobličavanja vrši uobličavanje toka, a funkcija odbacivanja vrši odbacivanje paketa koji su narušili dogovorene saobraćajne parametre. Na slici 4.1.1.4 je prikazana razlika između funkcije uobličavanja i odbacivanja. Funkcija odbacivanja odbacuje svaki paket koji naruši dogovor, dok funkcija uobličavanja implementira bafer kojim se mogu zakasniti paketi koji narušavaju saobraćajne parametre tako da njihovo zakašnjeno slanje bude u skladu sa dogovorenim saobraćajnim parametrima. Očigledno, funkcija uobličavanja unosi dodatno kašnjenje u korisnički tok. Funkcija merenja prati saobraćajne parametre korisničkog

toka i detektuje pakete koji narušavaju dogovorene saobraćajne parametre. Informacija o paketima koji narušavaju dogovor se prosleđuje funkcijama obeležavanja, uobličavanja i odbacivanja, a ove potom vrše odgovarajuće akcije na tim paketima u zavisnosti od konkretne implementacije tih funkcija.



Slika 4.1.1.4. Funkcije uobličavanja i odbacivanja

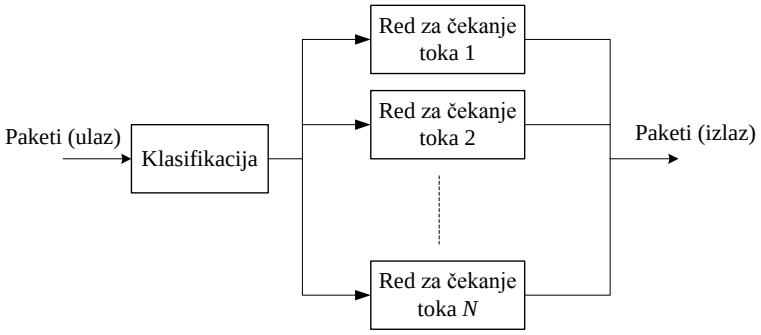
Unutrašnji čvorovi vrše opsluživanje paketa na bazi klasa servisa. Tipično se vrši opsluživanje po prioritetima klasa tako da paketi klase servisa višeg prioriteta budu prvi opsluženi, a poslednja klasa je *best effort* saobraćaj koji samim tim trpi najveća kašnjenja i najveće gubitke paketa u slučaju zagušenja. Očigledno, opsluživanje sa stanovišta paketa je po hopu (*per hop behavior*), odnosno u svakom ruteru se vrši identičan princip opsluživanja (sam princip opsluživanja zavisi od konkretne implementacije, na primer, može se koristiti WFQ (*Weighted Fair Queueing*) algoritam opsluživanja). Ovo omogućava jednostavniju realizaciju unutrašnjih rutera jer je najkomplikovaniji proces opsluživanja (klasifikacija, obeležavanje, uobličavanje, odbacivanje) smešten u ivične rutere. Međutim, DiffServ arhitektura dozvoljava da i unutrašnji ruteri mogu da vrše slične funkcije kao i ivični čvorovi samo na nivou agregacije tokova po klasama servisa i da menjaju vrednosti DSCP koda u slučaju paketa koji sa stanovišta unutrašnjeg čvora narušavaju saobraćajne parametre (ali sada sa stanovišta agregiranih tokova). Pri tome je menjanje DSCP koda uvek na lošiju klasu servisa, tipično *best effort* klasu saobraćaja.

DiffServ arhitektura je veoma skalabilna jer njena kompleksnost zavisi od broja klasa servisa, a ne broja individualnih korisničkih tokova pa je samim tim moguće podržati veliki broj tokova. Najveće procesiranje se odvija u ulaznim ivičnim čvorovima. U unutrašnjim čvorovima se vrši opsluživanje agregiranih tokova sa stanovišta klasa servisa čime je postignuta ekonomična implementacija unutrašnjih rutera. Mana je što ova arhitektura ne može da pruži striktne garancije jer ne razlikuje individualne tokove, a takođe, granularnost QoS nivoa nije velika pošto se opslužuju agregirani tokovi podeljeni u nekoliko klasa servisa. Takođe, mana je i problematična podrška multikast tokovima jer se takvi tokovi račvaju u mreži, a i broj korisnika se tipično menja tokom vremena (pa se time mogu dodati nove grane u multikast stablo) pa je teško ispitati da li može da se zadovolji traženi SLA nivo ili ne pošto je ispitivanje sa stanovišta

izvorišta saobraćaja (korena multikast stabla) pa je potrebno ispitati sve grane ponaosob što predstavlja značajan problem u slučaju veoma razgranatog stabla.

4.1.2. IntServ

Osnovna definicija IntServ arhitekture je izložena u preporuci RFC 1633. IntServ arhitektura se zasniva na individualnom opsluživanju tokova tako što se vrši uspostava veze za tok tokom koje se vrši rezervisanje resursa u ruterima duž kojih će prolaziti paketi dotičnog toka. Očigledno, mora se koristiti odgovarajuća signalizacija tj. signalizacioni protokol koji će omogućiti rezervisanje resursa u ruterima na putu toka. RSVP protokol se koristi u procesu rezervacije resursa i on će biti objašnjen nešto kasnije u okviru ovog poglavlja. Nakon rezervisanja resursa, paketi toka mogu početi da se šalju, a ruteri na putu će obezbediti da tok primi željeni kvalitet servisa. Struktura ravni podataka u ruterima sa stanovišta IntServ arhitekture je prikazana na slici 4.1.2.1. Klasifikacija ispituje pristigli paket da bi odredila kom toku pripada dotični paket i potom ga prosleđuje u odgovarajući red za čekanje. Raspoređivanje paketa iz svih tokova (redova za čekanje) za slanje na izlazni link se vrši po odgovarajućem algoritmu raspoređivanja. Koji algoritam raspoređivanja će se koristiti zavisi od same implementacije tj. standard ne definiše sam algoritam raspoređivanja već sami proizvođači biraju koji algoritam će koristiti u svojim proizvodima (na primer, može se koristiti WFQ algoritam).



Slika 4.1.2.1. Ravan podataka - logička shema u IntServ arhitekturi

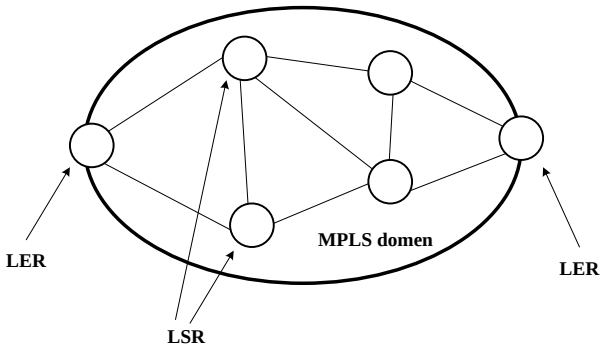
Da bi IntServ arhitektura mogla da funkcioniše neophodno je da se specificira željeni kvalitet servisa, ali isto tako i da se opišu karakteristike saobraćaja. Željeni kvalitet servisa se opisuje sa stanovišta prijemne strane koja definiše tzv. RSPEC (*Request Specifications*) specifikacije željenog kvaliteta servisa, na primer, maksimalno kašnjenje s kraja na kraj. RSPEC se često označava i terminom *Receiver Specifications* da bi se označilo da ovu specifikaciju zadaje prijemna strana. Karakteristike saobraćaja opisuje predajna strana što je i logično jer je ona ta koja će slati podatke u mrežu. Predajna strana definiše TSPEC (*Traffic Specifications*) specifikacije saobraćaja, tipično u vidu karakteristika bušne kofe (veličina bursta (odnosno dubina kofe) *b* i protok *r*). TSPEC se često označava i terminom *Transmitter Specifications* da bi se označilo da ovu specifikaciju zadaje predajna strana. Na osnovu ovih parametara se procenjuje da li mreža može da prihvati ovakav tok ili ne. Ako se tok prihvati, u svim ruterima na putu toka će biti rezervisani resursi za dotični tok.

Trenutno su definisane tri klase servisa u IntServ arhitekturi - najbolji pokušaj (*best effort*), kontrolisano opterećenje (*controlled load*) i garantovani servis (*guaranteed service*). Klasa najbolji pokušaj, ustvari, predstavlja tokove koji ne zahtevaju QoS od mreže tj. zahtevaju uslugu koju bi dobili i u slučaju kada mreža ne implementira QoS podršku. Klasa kontrolisano opterećenje (definisana u RFC 2211) pruža uslugu tokovima u kojima garantuje veoma slično

ponašanje tj. opsluživanje tokova nezavisno od trenutnog opterećenja mreže, odnosno tokovi će primati veoma sličan kvalitet servisa i u slučaju kada je mreža slabo opterećena i kada je mreža preopterećena (zagušena). U ovoj klasi se ne definiše RSPEC, već samo TSPEC specifikacija kojom se opisuje saobraćaj toka. Klasa garantuje uslugu samo za pakete koji ispunjavaju TSPEC specifikacije, a paketi koji naruše TSPEC specifikaciju se ili odbacuju ili se prosleđuju kao *best effort* paketi. Ovu klasu koriste aplikacije koje nemaju veoma striktne zahteve u pogledu protoka i kašnjenja već dozvoljavaju manje varijacije u opsluživanju. Aplikacije koje imaju veoma striktne zaheve u pogledu kvaliteta servisa (na primer, VoIP) moraju koristiti klasu garantovani servis (definisana u RFC 2212). Ova klasa definiše i RSPEC i TSPEC specifikacije. TSPEC specifikacija i dalje opisuje karakteristike saobraćaja, a RSPEC specifikacija definiše željeni nivo kvaliteta servisa, poput gornje granice kašnjenja kroz mrežu. Ova klasa pruža veoma striktne garancije tokovima nezavisno od trenutnog stanja mreže, naravno pod uslovom da korisnički tok poštuje tj. ne narušava TSPEC specifikaciju saobraćaja (i ovde se paketi koji narušavaju TSPEC specifikaciju ili odbacuju ili prosleđuju kao *best effort* saobraćaj). Očigledno, u mreži procenat saobraćaja koji koristi garantovani servis ne sme biti prevelik jer se tada ne bi mogle poštovati striktne garancije jer je jasno da ovaj saobraćaj ima najviši prioritet prilikom opsluživanja u ruterima.

IntServ arhitektura omogućava specificiranje kvaliteta servisa na nivou samih tokova pri čemu se TSPEC i RSPEC specifikacijama mogu fino podesiti parametri kvaliteta servisa. Takođe, IntServ arhitektura specificira kvalitet servisa na nivou čitavog puta toka, tj. s kraja na kraj čime tok dobija zaista željeni kvalitet servisa, za razliku od DiffServ arhitekture gde individualni kvalitet servisa zavisi od trenutne količine agregiranih tokova i njihovo trenutnog saobraćaja. Naravno, mana je što su sada svi ruteri značajno opterećeni jer svi ruteri na putu moraju da rade sa individualnim tokovima što predstavlja značajno opterećenje rutera pa otuda IntServ arhitektura nije skalabilna. Takođe, problem i DiffServ i IntServ arhitekture je zahtev da svi ruteri na putu toka moraju da podržavaju DiffServ ili IntServ arhitekturu (u zavisnosti koja od njih se koristi) jer je dovoljno da samo jedan ruter na putu ne podržava QoS (DiffServ ili IntServ) pa da se izgube garancije kvaliteta servisa toku.

4.2. MPLS osnove

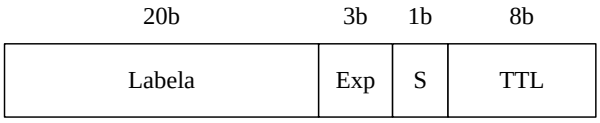


Slika 4.2.1. MPLS domen

U okviru MPLS arhitekture se definiše tzv. MPLS domen, koji se često naziva i MPLS oblak, koga sačinjavaju ruteri koji imaju sposobnost prosleđivanja na bazi MPLS labela. Primer MPLS domena je prikazan na slici 4.2.1. Ruteri koji prosleđuju pakete na bazi MPLS labela se

nazivaju LSR (*Label Switching Routers*) ruteri, pri čemu se ivični LSR ruteri, koji se nalaze na granici MPLS domena, nazivaju i LER (*Label Edge Routers*) ruteri.

LSR ruteri vrše prosleđivanje na bazi MPLS labela. Važno je naglasiti da LSR ruteri procesiraju samo MPLS labele, a ne procesiraju zaglavlje mrežnog sloja (IP zaglavlje) čime je proces procesiranja i usmeravanja paketa značajno uprošćen u odnosu na klasične IP rutere. Naravno, LSR ruteri se uglavnom mogu konfigurisati da procesiraju i IP zaglavlje ako za takvim procesiranjem ima potrebe. MPLS labela se može smestiti u zaglavlje jedinice podataka drugog sloja ukoliko ima mesta za nju. Na primer, u VPI/VCI polje zaglavlja ATM ćelija, DLCI polje FR (*Frame Relay*) okvira. Takođe, MPLS labela se može smestiti i u IPv6 zaglavlje (u polje *Flow Label*). Ukoliko nema prostora za smeštanje MPLS labele, onda se koristi tzv. *shim* zaglavlje koje u suštini predstavlja polje MPLS labele koje se smešta između zaglavlja drugog i trećeg sloja (sloja linka podataka i mrežnog sloja), na primer, između eternet zaglavlja i IPv4 zaglavlja ili PPP zaglavlja i IPv4 zaglavlja. Otuda se za MPLS često kaže da je u pitanju protokol 2.5 sloja da bi se naglasilo da on operiše između drugog i trećeg sloja OSI modela. Struktura MPLS labele (preciznije *shim* zaglavlja) definisane u preporuci RFC 3032 je prikazana na slici 4.2.2.

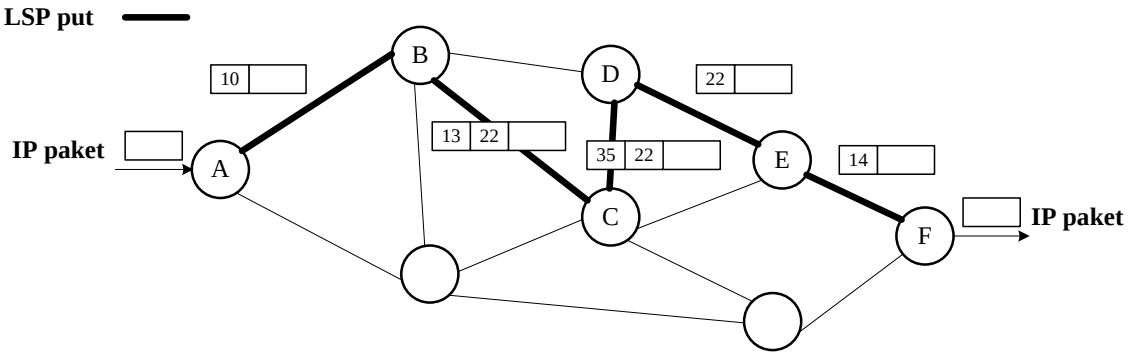


Slika 4.2.2. MPLS labela (*shim* zaglavlje)

Polje labele predstavlja samu vrednost MPLS labele. Eksperimentalno polje je rezervisano u eksperimentalne svrhe i može se iskoristiti za definisanje QoS prioriteta i ECN obaveštavanje o zagušenju. S bit označava da li je u pitanju hijerarhijski najniža labela (vrednost 1) ili ne (vrednost 0). Naime, dozvoljeno je kreiranje hijerarhije MPLS domena, gde svaki hijerarhijski nivo dodaje svoju labelu (pod labelom se podrazumeva kompletno *shim* zaglavlje) pa se stoga kreira tzv. stek labela (stek labela može imati proizvoljnu dubinu). S bit stoga označava da li je u pitanju hijerarhijski najniža labela u steku (ona koja je prva dodata na paket). TTL (*Time To Live*) polje se koristi kao zamena za TTL polje iz IP zaglavlja. Naime, TTL polje iz IP zaglavlja se dekrementiralo za 1 prilikom svakog prolaska kroz ruter, čime se sprečavalo da paket beskonačno kruži u mreži. Pošto se u LSR ruterima procesira samo labela, a ne i IP zaglavlje, onda je potrebno obezbediti mehanizam koji bi i dalje dekrementirao originalno TTL polje prilikom prolaska paketa kroz rutere. Otuda na ulazu u MPLS domen, LER ruter u TTL polje *shim* zaglavlja stavlja vrednost TTL polja iz IP zaglavlja (u slučaju da već postoje labele u steku labela onda se kopira TTL polje iz labele na vrhu steka). Prilikom prolaska kroz LSR ruter, TTL polje iz *shim* zaglavlja se dekrementira. Na izlasku iz MPLS domena, LER ruter upisuje vrednost TTL polja iz *shim* zaglavlja u TTL polje IP zaglavlja (ili u TTL polje sledeće labele u steku) čime je postignuto da TTL polje IP zaglavlja bude ispravno ažurirano u prolasku kroz MPLS domen. Inače, TTL polje se u IPv6 zaglavlju naziva *Hop Count* polje.

Kao što smo već naveli, usmeravanje paketa kroz MPLS domen se vrši na bazi labela. Labele imaju lokalni značaj (slično kao VPI/VCI identifikatori u ATM mrežama). LER ruteri na ulazu u MPLS domen dodaju labelu paketu. LSR ruteri prosleđuju pakete na bazi labele tako što za primljenu labelu traže odgovarajući zapis u tabeli usmeravanja na bazi labela. Takođe, u okviru tog zapisa se nalazi i podatak o novoj vrednosti labele kojom treba zameniti labelu u primljenom paketu pre nego što se paket prosledi na odgovarajući izlaz LSR rutera. Na kraju,

LER ruter na izlazu iz MPLS domena skida labelu sa paketa. U suštini MPLS ruteri (LSR i LER) mogu vršiti tri osnovne operacije nad labelama - dodavanje (*push*), skidanje (*pop*) i zamena (*swap*). Dodavanje labele označava operaciju kojom se labela dodaje na stek labela i nju tipično rade LER ruteri na ulazu u MPLS domen. Skidanje labele označava operaciju kojom se skida labela sa steka labela i nju tipično rade LER ruteri na izlazu iz MPLS domena. Zamena labela označava da se labela sa vrha steka zameni novom vrednošću pre nego što se paket prosledi dalje i ovu operaciju tipično rade LSR ruteri, ali i ulazni LER ruteri na granicama između dve hijerarhije MPLS domena. Put paketa kroz MPLS domen se naziva LSP (*Label Switched Path*) put. Primer usmeravanja paketa kroz MPLS domene i LSP puta je dat na slici 4.2.3. Treba primetiti iz datog primera da labele imaju lokalni značaj.

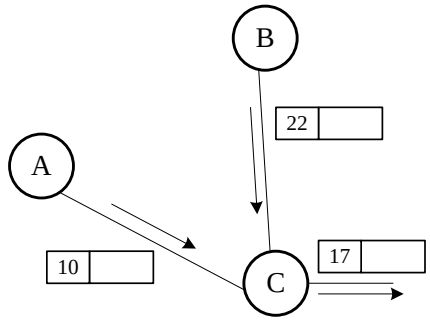


Slika 4.2.3. Primer usmeravanja kroz MPLS domene

Kada IP paket (bez labela) dođe u ruter na ulazu u MPLS domen, vrši se procesiranje zaglavlja IP paketa, a takođe se na osnovu odredišne IP adrese vrši pretraga tabele usmeravanja na bazi IP adresa. Kao rezultat se dobija izlazni port na koji treba usmeriti paket, kao i vrednost labele koju treba dodati na paket (pošto paket ulazi u MPLS domen). Stoga, ruter A, koji predstavlja ulaz u MPLS domen, dodaje paketu labelu vrednosti 10 (operacija dodavanja). Ruter B predstavlja ulaz u hijerarhijski viši MPLS domen. Vrši se pretraga tabele usmeravanja na bazi labela za primljenu labelu 10 i kao rezultat se dobijaju izlazni port na koji treba proslediti paket, nova vrednost labele, kao i vrednost labele koja će se dodati na vrh steka labela (labela hijerarhijski višeg MPLS domena). Stoga, ruter B vrši zamenu labele 10 labelom 22, a potom dodaje još jednu labelu vrednosti 13 (operacije zamene i dodavanja). Ruter C vrši pretragu tabele usmeravanja na bazi labela za primljenu labelu 13 na vrhu steka labela i dobija novu vrednost labele, kao i izlazni port na koji treba proslediti paket. Ruter C vrši zamenu labele sa vrha steka, pa se labela 13 menja labelom 35 (operacija zamene). Ruter D predstavlja izlaz iz hijerarhijski višeg MPLS domena. Na osnovu labele 35 sa vrha steka vrši pretragu tabele usmeravanja na bazi labela i kao rezultat dobija izlazni port na koji treba proslediti paket, kao i informaciju da treba da skine labelu sa vrha steka. Otuda, ruter D samo skida labelu sa vrha steka (operacija skidanja). Ruter E vrši zamenu labele 22 sa labelom 14 (operacija zamene) pošto je na osnovu pretrage tabele usmeravanja na bazi labela za labelu 22 dobio izlazni port na koji treba usmeriti paket, kao i novu vrednost labele. Na kraju ruter F, koji je ruter na izlazu iz MPLS domena, vrši pretragu tabele usmeravanja na bazi labela za labelu 14 i dobija informaciju da treba da skine labelu sa steka. Stoga, ruter F skida labelu sa paketa (operacija skidanja). Potom, ruter F vrši procesiranje IP zaglavlja i vrši pretragu tabele usmeravanja na bazi IP adresa. Kao rezultat se dobija izlazni port na koji treba usmeriti paket (bez labela). Kao što vidimo poslednji ruter na LSP putu vrši dve pretrage tabela usmeravanja - jedna pretraga tabele usmeravanja na bazi labela i jedna pretraga tabele usmeravanja na bazi IP adresa. Otuda je razvijena i tehnika skidanja labele na

zadnjem hopu (*penultimate hop popping*). Ova tehnika podrazumeva da pretposlednji čvor na LSP putu samo skine labelu sa steka i ne stavi novu vrednost, tako da poslednji ruter na LSP putu radi sa IP paketom bez labela čime bi se vršila samo pretraga tabele usmeravanja na bazi IP adresa pa bi se poslednji ruter na LSP putu rasteretio nepotrebne pretrage tabele usmeravanja na bazi labela. Da bi se ova tehnika smela primeniti u pretposlednjem čvoru LSP puta, poslednji čvor LSP puta to mora egzaktno zahtevati od pretposlednjeg čvora.

Da bi se dodelila labela IP paketu mora da se definiše logika u dodeljivanju labele, pa se definiše tzv. FEC (*Forwarding Equivalence Class*) klasa. U preporuci RFC 3031 se FEC klasa se definiše kao mrežni prefiks, ali dozvoljeno je korišćenje i drugih definicija koje bi uključivale polja IP ili transportnih zaglavlja, kao i interfejse po kojima pristižu paketi (na primer, FEC klase mogu da budu formirane imajući u vidu i QoS zahteve ili da bi se kreirao VPN tunel). Mrežni prefiks se koristio u originalnoj upotrebi MPLS protokola, a to je pojednostavljenje procesa usmeravanja paketa kroz mrežu. Svi paketi čija odredišna IP adresa ima isti mrežni prefiks pripadaju istoj FEC klasi u slučaju definicije iz RFC 3031. FEC klasa se vezuje za MPLS labelu, pa je očigledno da će paketi iste FEC klase prolaziti kroz identičan LSP put i imati identično opsluživanje ako ulaze u MPLS domen na istom mestu. Određivanje pripadnosti paketa FEC klasi se vrši samo na ulazu u MPLS domen jer se u ostalim ruterima (LSR) vrši procesiranje samo labele, odnosno usmeravanje samo uz pomoć labele bez ikakvog procesiranja mrežnog zaglavlja. Vezivanje labele za FEC klasu može biti na nivou platforme (uređaja) ili na nivou interfejsa. Na nivou platforme, labela je jedinstvena na nivou čitavog uređaja pa se otuda jedna labela dodeljena nekoj FEC klasi ne sme koristiti za neku drugu FEC klasu (labele se dodeljuju iz istog skupa labela). Na nivou interfejsa labela je jedinstvena samo na nivou interfejsa pa se može desiti da se upotrebi ista labela za dve različite FEC klase, ali na dva različita interfejsa uređaja (svaki interfejs ima svoj skup labela).



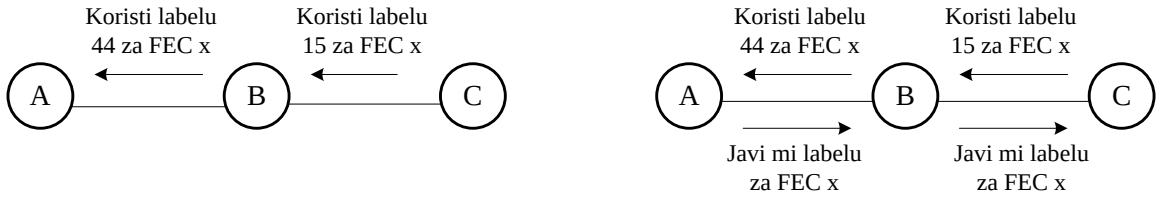
Slika 4.2.4. Spajanje labela

Pošto paketi koji pripadaju istoj FEC klasi mogu ući na različitim mestima u MPLS domen, a izaći na istom mestu, LSP putevi ovih paketa će se spajati u MPLS domenu. Otuda je dozvoljeno tzv. spajanje labela (*label merging*). Paketi iste FEC klase koji dolaze sa različitih ulaznih interfejsa i/ili sa različitim labelama u LSR ruter će se u slučaju spajanja labela prosleđivati na isti izlaz LSR rutera, pri čemu će nova vrednost labele (na izlazu) biti identična za sve te pakete. Primer spajanja labela je dat na slici 4.2.4. U MPLS prenosu preko ATM mreža spajanje labela može da izazove probleme usled interlivinga ćelija različitih tokova pošto su zbog male dužine ćelija originalni paketi podeljeni na više ćelija. Nakon spajanja tokova dolazi do problema rekonstrukcije paketa iz ćelija na izlazu iz ATM mreže jer se izgubila informacija o tome gde su ćelije ušle u MPLS domen. Rešenje je da se ili ne vrši spajanje tokova (spajanje labela) ili da se napravi dva nivoa hijerarhije MPLS labela (praktično formira se VP put koji

predstavlja spojeni tok, a VCI se koristi za identifikaciju originalnih tokova) ili da se vrši rekonstrukcija paketa u ATM čvoru gde se vrši spajanje pa da se potom šalju rekonstruisani paketi jedan za drugim (naravno, opet u vidu ATM ćelija) u spojenom toku što komplikuje rad takvog ATM čvora.

LSR/LER ruter kada izvrši vezivanje labele za FEC klasu formira automatski i odgovarajući zapis u tabeli usmeravanja na bazi labela. Pri tome, labela koju je ruter vezao za FEC klasu je dolazna labela koju nose paketi dotične FEC klase. Vezivanje labele može biti nezavisno (*independent*) ili uređeno (*ordered*). U slučaju nezavisnog vezivanja, ruter čim prepozna novu FEC klasu vrši vezivanje labele (slobodne labele iz skupa labela) za nju. U uređenom vezivanju, ruter vrši vezivanje labele za FEC klasu samo ako je on izlazni LER ruter za dotičnu FEC klasu ili ako je primio oglašenu labelu za tu FEC klasu od rutera koji predstavlja sledeći hop za dotični ruter.

Labelu, koju je ruter vezao za FEC klasu, ruter oglašava svojim susedima. Uzvodni (*upstream*) sused će da prihvati tu labelu i upiše je u odgovarajuće mesto u svojoj tabeli usmeravanja na bazi labela (ili IP adresa ako je u pitanju LER ruter na ulazu u MPLS domen). Uzvodni sused je onaj čiji je sledeći hop za dotičnu FEC klasu upravo dotični ruter koji je oglasio labelu. U uzvodnom ruteru u zapisu koji odgovara dotičnoj FEC klasi će biti uneta vrednost labele koja se mora staviti na vrh steka labela (ulaz u MPLS domen - LER ruter) paketa ili koja mora zameniti labelu sa vrha steka (LSR ruter) paketa. Susedni ruteri koji nisu uzvodni ruteri u zavisnosti od konfigurisanog moda rada ili ignorišu oglašavanje ili ga prihvataju. U slučaju konzervativnog moda (*Conservative Label Retention Mode*) ruter, koji nije uzvodni svom susedu (od kog je primio oglašavanje), ignoriše oglašavanje labele svog suseda. U slučaju liberalnog moda (*Liberal Label Retention Mode*) nizvodni ruter prihvata oglašavanje labele svog uzvodnog suseda i zapisuje ga za eventualnu buduću upotrebu. Konzervativni mod je ekonomičniji jer ruter čuva samo one labele koje zaista i koristi, a liberalni mod troši više resursa jer čuva sve oglašene labele. Međutim, liberalni mod omogućava brže prilagođavanje na promene u mreži jer se brže mogu aktivirati novi LSP putevi u slučaju ispada nekih LSP puteva zbog promena u topologiji mreže. Ovaj način oglašavanja tabela je bezuslovan način oglašavanja labela (*Unsolicited Downstream*). Pored njega postoji i oglašavanje u uzvodnom smeru na zahtev (*Downstream-on-Demand*). U ovom slučaju ruteri ne oglašavaju svoje labele koje su vezali za FEC klase, već to čine samo ka (uzvodnim) susedima koji pošalju eksplicitan zahtev za labelom. Primeri navedena dva metoda oglašavanja labela su prikazana na slici 4.2.5.



Bezuslovno oglašavanje

Oglašavanje u uzvodnom smeru na zahtev

Slika 4.2.5. Oglašavanje labela

Sam princip oglašavanja labela zahteva odgovarajući signalizacioni protokol. MPLS ne specificira određeni protokol već dozvoljava upotrebu proizvoljnog protokola pri čemu je dozvoljeno koristiti i više protokola uporedo. MPLS preporuka predviđa dva načina realizacije

ovih signalizacionih protokola - signalizacioni protokol razvijen specijalno za ovu namenu (oglašavanja labela) i postojeći protokoli rutiranja i signalizacije koji se proširuju tako da podrže i oglašavanje labela. LDP (*Label Distribution Protocol*) predstavlja signalizacioni protokol razvijen specijalno za oglašavanje labela. Sa druge strane, RSVP i BGP protokoli su prošireni tako da podrže i oglašavanje MPLS labela.

Da bi se mogao uspostaviti LSP put neophodno je pravilno konfigurisati tabele usmeravanja na bazi labela u LSR/LER ruterima. U tabeli usmeravanja na bazi labela je neophodno da postoji u zapisu informacija o izlaznom portu na koji treba proslediti paket (tj. informacija o nizvodnom ruteru koji predstavlja sledeći hop na putu). Ova informacija se dobija na osnovu rada protokola rutiranja i na osnovu nje ruter može znati za dotičnu FEC klasu i samim tim i labelu vezanu za tu FEC klasu na koji izlazni port treba proslediti pakete dotične FEC klase. Princip usmeravanja paketa kroz MPLS domen (tj. uspostavljanja LSP puta za FEC klasu) koristeći ovu informaciju se naziva hop po hop rutiranje (*hop-by-hop routing*) jer svaki LSR/LER ruter nezavisno od drugih rutera u MPLS domenu određuje svoj izlazni port na koji će usmeriti paket. Ovaj princip je identičan principu formiranja zapisa u tabelama usmeravanja na bazi IP adresa, odnosno principu usmeravanja kroz IP mreže. Drugi način uspostavljanja LSP puta je eksplicitno rutiranje (*explicit routing*). U slučaju eksplicitnog rutiranja, ulazni LER ruter određuje put kroz MPLS domen. Pri tome, može da se specificira striktna putanja ili labava putanja. Striktna putanja precizno definiše sve deonice LSP puta, dok labava putanja definiše samo pojedine rutere kroz koje LSP put mora proći, ali se na putu mogu naći i nespecificirani ruteri. Na primer, striktni put za mrežu sa slike 4.2.3 bi mogao da se definiše kao A-B-D-E-F i tada LSP put prolazi kroz samo te rutere i nijedne druge. Ako bi se definisao labavi put A-B-D-E-F tada mogu da se prođu i neki drugi ruteri pored navedenih pa je tako moguće da se formira LSP put A-B-C-D-E-F. Važno je napomenuti da se uvek uspostavlja jednosmeran LSP put (za razliku od ATM mreža gde su uspostavljeni putevi bili bidirekcioni). Pošto LSP put formiran eksplicitnim rutiranjem ne mora da bude najkraći put onda se ne mogu koristiti samo klasični protokoli rutiranja. Otuda su definisana proširenja protokola rutiranja (na primer, OSPF-TE) koja omogućavaju razmenu detaljnijih informacija o mreži čime se omogućava ulaznom LER ruteru da lakše odabere eksplicitnu putanju. Eksplicitno rutiranje je veoma važno u slučaju kada se želi formirati VPN tunel, kao i u slučaju impementacije QoS podrške.

Na kraju napomenimo da se za jednu labelu može vezati više zapisa u tabeli usmeravanja na bazi labela. Ova opcija je zgodna u slučaju kada se želi vršiti balansiranje saobraćaja za neku FEC klasu na više puteva kroz MPLS domen. Sam MPLS standard ne definiše na koji način se određuje koji od zapisa će se koristiti u slučaju da više zapisa odgovara labeli paketa. Takođe, važno je uočiti da je MPLS protokol CO (*Connection Oriented*) tipa jer se mora uspostaviti LSP put pre prosleđivanja paketa kroz MPLS domen.

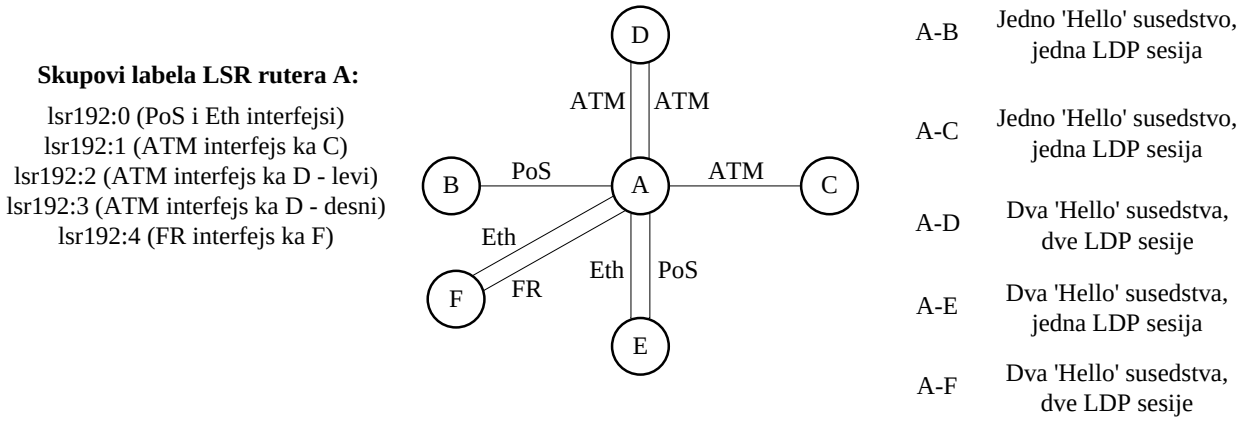
4.3. LDP

LDP (*Label Distribution Protocol*) protokol se koristi za proces distribucije (oglašavanja) labela tj. njihovih vezivanja za FEC klase između LSR/LER rutera. LDP protokol je definisan u preporuci RFC 5036. LSR ruteri (pod LSR ruterima ćemo podrazumevati i LER rutere u okviru ovog potpoglavlja) koji međusobno razmenjuju LDP poruke se nazivaju LDP pirovi (*peers*). LDP poruke se mogu podeliti u četiri logičke grupe:

- Poruke otkrivanja (*discovery messages*) - Ove poruke se koriste za otkrivanje potencijalnih LDP suseda.
- Poruke sesije (*session messages*) - Da bi dva LDP pira mogla da razmenjuju LDP poruke, mora da se uspostavi LDP sesija između njih. Ova grupa poruka se koristi za uspostavljanje, održavanje i raskidanje LDP sesija.
- Poruke oglašavanja (*advertisment messages*) - Ove poruke se koriste za oglašavanje labela tj. vezivanja labela za FEC klase. Oglašavanje podrazumeva oglašavanje novih mapiranja labela, promenu i brisanje postojećih mapiranja labela (pod mapiranjem labele se podrazumeva vezivanje labele za FEC klasu).
- Poruke obaveštenja (*notification messages*) - Ove poruke se koriste za slanje obaveštenja, na primer, obaveštenja o detektovanim greškama u sesiji.

Pošto se za razmenu LDP poruka mora uspostaviti LDP sesija, LDP protokol koristi TCP protokol kao transportni protokol, sem za poruke otkrivanja za koje koristi UDP transportni protokol.

Već smo ranije naveli da ruteri mogu da kreiraju skup labela koje mogu da vezuju za FEC klase na nivou uređaja ili na nivou interfejsa. Stoga je bitno da u LDP sesiji sa susedom ruteri znaju koji skup labela treba da koriste. LDP identifikator skupa labela je predstavljen u vidu 6 bajtova, gde prva 4 bajta predstavljaju globalno jedinstvenu identifikaciju rutera, a preostala dva bajta identifikuju skup labela dotičnog rutera. Skup labela na nivou uređaja uvek ima vrednost 0 za identifikaciju skupa labela (poslednja dva bajta LDP identifikatora skupa labela). Notacija koja se koristi za navođenje LDP identifikatora je *<LSR ID LSR rutera>*:*<ID skupa labela LSR rutera>*. Na primer, lsr191:0, lsr200:2.



Slika 4.3.1. Primer ’Hello’ susedstava i LDP sesija

Razlikuju se dva nivoa interakcije između LDP suseda sa stanovišta LSR rutera - LDP sesija i LDP ’Hello’ susedstvo. LDP ’Hello’ susedstvo označava slanje i prijem ’Hello’ poruka koje spadaju u grupu poruka otkrivanja. U suštini koliko linkova ima između dva rutera toliko će biti i ’Hello’ susedstava između njih. S druge strane, da bi LDP oglašavanje labela moglo da otpočne mora da se uspostavi LDP sesija između suseda. Broj LDP sesija koji se uspostavlja zavisi od ukupnog broja skupa labela dotičnog LSR rutera. Tipično ako se koriste ATM ili FR linkovi tada se za njih skup labela vezuje na nivou interfejsa, a za ostale tipove linkova se uglavnom koristi vezivanje na nivou uređaja. Na slici 4.3.1 je prikazano tumačenje LDP sesije i

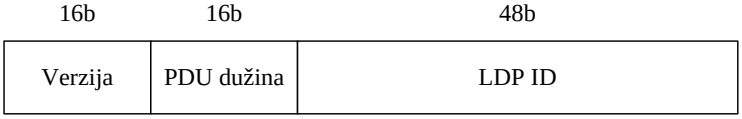
LDP ’Hello’ susedstva na konkretnom primeru. LSR ruter A za svaki ATM i FR interfejs definiše zaseban skup labela (na nivou interfejsa), a za sve ostale interfejse (PoS i Eth) definiše jedan skup labela na nivou uređaja. Kao što se vidi iz datog primer ID rutera A je lsr192. Broj ’Hello’ susedstava između dva rutera odgovara broju linkova između njih, dok je broj LDP sesija jednak broju skupova labela koji ruter A oglašava svojim susedima. Na primer, rutera A oglašava dva skupa labela susedu F, pa je neophodno kreirati dve LDP sesije, po jednu za svaki skup.

Postoje dva mehanizma otkrivanja suseda - osnovni (*basic*) i prošireni (*extended*). U osnovnom mehanizmu LSR ruter periodično šalje LDP Link Hello poruku na multikast adresu 224.0.0.2 i UDP port 646, pri čemu se u okviru poruke nalazi LDP identifikator skupa labela. Ruter koji primi ovakvu poruku zna da se nalazi u susedstvu rutera koji je poslao LDP Link Hello poruku i stoga može da otpočne uspostavu LDP sesije sa njim. Prošireni mehanizam se koristi za otkrivanje suseda koji nisu direktno povezani sa dotičnim ruterom. Tada LSR ruter periodično šalje LDP Targeted Hello poruke na određenu unikast IP adresu udaljenog suseda koji se želi otkriti (UDP port na koji se šalje poruka je i dalje isti kao i u osnovnom mehanizmu tj. UDP port 646). LSR ruter koji primi LDP Targeted Hello poruku može da je ignoriše ako ne želi da uspostavi susedstvo. Ako taj LSR ruter odluči da uspostavi susedstvo tada počinje periodično da šalje LDP Targeted Hello poruke ka ruteru od koga je primio LDP Targeted Hello poruku. Struktura Hello poruke u oba slučaja je ista, razlika je u IP adresi odredišta, tj. u jednom slučaju se koristi multikast adresa, a u drugom unikast adresa.

LDP sesija se uspostavlja u dva koraka. Prvo se uspostavlja TCP virtuelno kolo (onaj koji inicijalizuje uspostavu veze koristi TCP port 646 tj. šalje zahtev za uspostavom TCP veze na taj port), a potom se preko TCP virtuelnog kola uspostavlja (inicijalizuje) LDP sesija. Pošto se *hello* poruke neprestano periodično šalju, one će se ignorisati (neće izazvati uspostavu LDP sesije) u slučaju da je LDP sesija već uspostavljena sa dotičnim LSR susedom i skupom labela na koji se odnosi *hello* poruka. Da se ne bi nepotrebno započinjala sesija sa obe strane, utvrđen je mehanizam određivanja ko će započeti uspostavu sesije. Mehanizam se sastoji u poređenju IP adresa odgovarajućih interfejsa (interfejsi preko kojih se razmenjuju LDP poruke za uspostavu) LSR rutera. Ruter čija je IP adresa veća će biti aktivan ruter u procesu uspostave LDP sesije, a ruter čija je IP adresa manja će biti pasivan ruter u procesu uspostave LDP sesije. Napomenimo da se za IP adresu uzima ili adresa navedena unutar *hello* poruke ili ako ona nije navedena izvorišna IP adresa paketa koji je nosio *hello* poruku. U slučaju da se utvrdi na osnovu IP adresa da ruteri ne pripadaju istoj mreži tada se sesija neće ni započeti uspostavljati, već će sve *hello* poruke od takvog suseda biti ignorisane. Nakon što se principom trostrukog rukovanja uspostavi TCP virtuelno kolo, razmenjuju se inicijalizacione LDP poruke kojima se uspostavlja LDP sesija. Aktivni ruter šalje LDP Initialization poruku u okviru koje navodi parametre LDP sesije, poput vrednosti tajmera, verzije LDP protokola, metode oglašavanja labela, opsega vrednosti za VPI/VCI identifikatore u slučaju ATM linka, itd. Pasivni ruter po prijemu ove poruke ispituje parametre sesije. Ukoliko su navedeni parametri neprihvatljivi, pasivni ruter šalje Session Rejected/Parameters Error Notification poruku kojom raskida sesiju (pokreće se i raskid TCP virtuelnog kola). Ako su parametri prihvatljivi, pasivni ruter šalje svoju Initialization poruku sa svojim parametrima sesije, a takođe šalje i KeepAlive poruku kojom potvrđuje prihvatanje parametara sesije iz primljene Initialization poruke. Aktivni ruter po prijemu Initialization poruke odgovara sa KeepAlive porukom ako su mu parametri sesije prihvatljivi i tada je sa njegovog stanovišta LDP sesija uspostavljena. Ako aktivnom ruteru nisu prihvatljivi parametri sesije, tada on šalje Session Rejected/Parameters Error Notification poruku (pokreće se i raskid

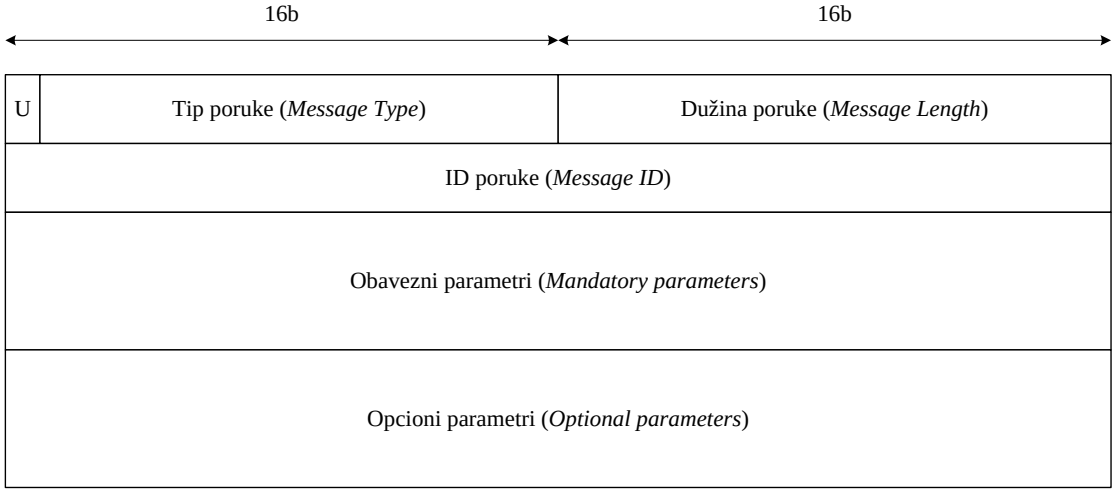
TCP virtuelnog kola). Pasivni ruter po prijemu KeepAlive poruke zna da su njegovi parametri sesije prihvaćeni i sa njegovog stanovišta LDP sesija je uspostavljena.

LSR ruteri za svako ’Hello’ susedstvo održavaju *hello* tajmer koji se resetuje po prijemu *hello* poruke. Ako tajmer istekne smatra se da ’Hello’ susedstvo više ne postoji. Kada se unutar jedne LDP sesije ugase sva ’Hello’ susedstva, LDP sesija se raskida. Takođe, LSR ruteri održavaju za svaku LDP sesiju *keepalive* tajmer koji se resetuje po prijemu LDP poruke te sesije (ako LSR ruter nema šta da šalje, šalje se *keepalive* poruka). Kada ovaj tajmer istekne, LDP sesija se raskida.



Slika 4.3.2. Zaglavlje LDP PDU jedinice

LDP poruke se prenose u tzv. LDP PDU (*Protocol Data Unit*) jedinicama, pri čemu jedna LDP PDU jedinica može da sadrži jednu ili više LDP poruka. Struktura zaglavlja LDP PDU jedinice je prikazana na slici 4.3.2. Iza zaglavlja slede LDP poruke. Verzija definiše verziju LDP protokola (RFC 5036 specificira verziju 1). PDU dužina označava dužinu LDP PDU jedinice u bajtovima, ne računajući pri tome polja verzija i PDU dužina iz zaglavlja LDP PDU jedinice. LDP ID polje predstavlja LDP identifikator skupa labela koji smo ranije opisali. LDP poruke su formatirane na način prikazan na slici 4.3.3.

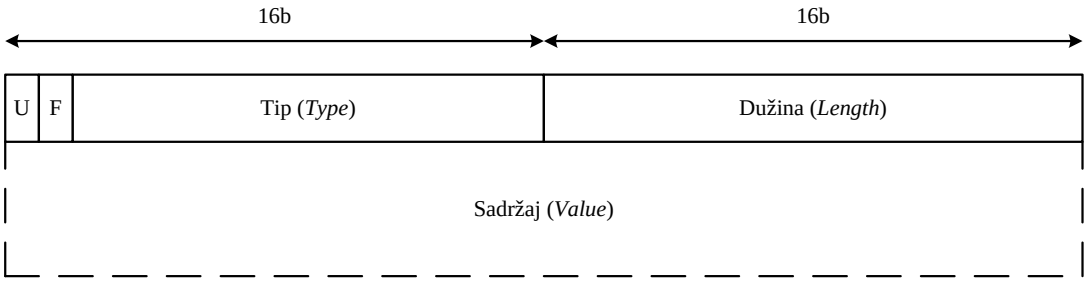


Slika 4.3.3. Format LDP poruka

Bit U (*Unknown*) označava prijemnoj strani kako da se ponaša ako primi LDP poruku koju ne prepoznaje. Ako je U bit setovan (vrednost 1) tada prijemna strana jednostavno ignoriše poruku, i nastavlja sa procesiranjem ostalih LDP poruka u LDP PDU jedinici, u suprotnom ako U bit nije setovan (vrednost 0) prijemna strana mora da pošalje LDP poruku obaveštenja kojom se izvor poruke obaveštava da dotična LDP poruka nije prepoznata. Tip poruke definiše koja LDP poruka je u pitanju. Dužina poruke predstavlja ukupnu dužinu u bajtovima polja ID poruke, obavezni parametri i opcioni parametri. ID poruke nosi identifikaciju poruke koja može da se koristi u slanju obaveštenja izvoru poruke jer navođenjem ID-a poruke u obaveštenju izvorna strana će znati na koju njenu poslatu poruku se odnosi obaveštenje. Obavezni parametri su parametri koji moraju da se nađu u okviru dotičnog tipa LDP poruke (svaki tip ima svoj skup

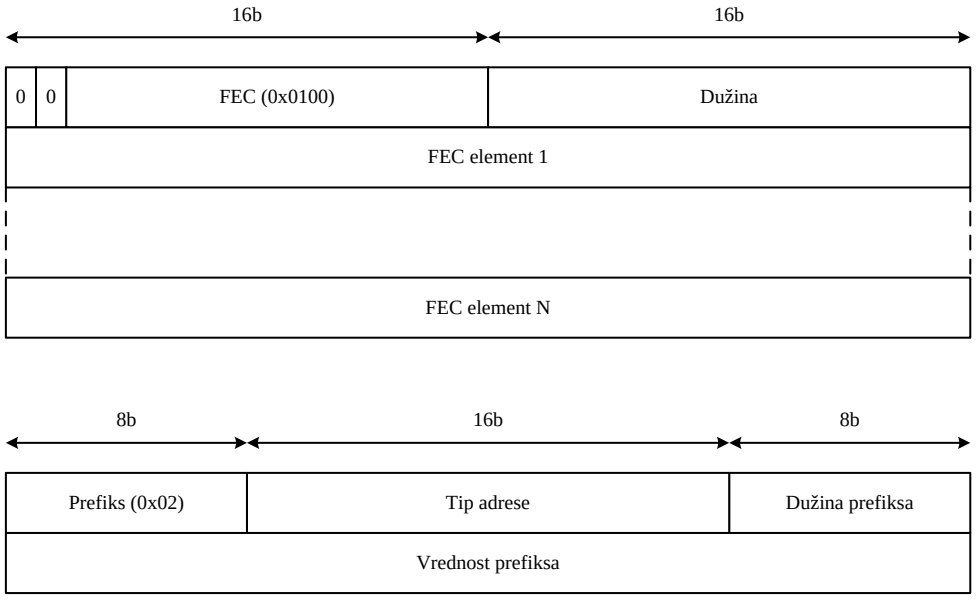
obaveznih parametara), a opcioni parametri su oni koji mogu, ali i ne moraju da se nađu u dotičnom tipu LDP poruke.

Kodiranje parametara se vrši po TLV principu (tip (*type*), dužina (*length*), sadržaj (*value*)) koji je veoma čest u protokolima IP mreža. Struktura parametara je prikazana na slici 4.3.4.



Slika 4.3.4. Struktura parametara

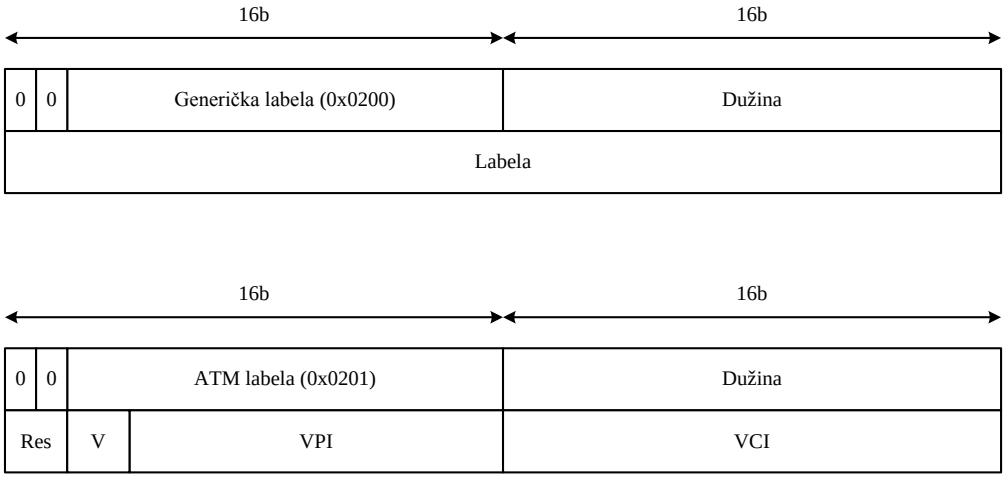
Bit U označava prijemnoj strani kako da se ponaša ako primi parametar koji ne prepoznaje. Tumačenje U bita je identično kao u slučaju tumačenja U bita sa slike 4.3.3 samo na nivou parametara. F (*Forward Unknown*) bit specificira ponašanje prijemne strane sa stanovišta prosleđivanja u slučaju prijema nepoznatog parametra. F bit se tumači samo ako je U bit setovan (vrednost 1) i ako se LDP poruka koja sadrži dotični nepoznat parametar mora proslediti dalje. Vrednost 1 F bita označava da se dotični parametar prosleđuje, a vrednost 0 da se dotični parametar ne prosleđuje dalje sa LDP porukom u kojoj se nalazi. Tip označava tip parametra čime se određuje način tumačenja polja sadržaj. Dužina definiše dužinu sadržaja parametra u bajtovima. Sadržaj predstavlja sadržaj, tj. vrednost parametra. Poznatiji parametri su FEC, labela, lista adresa, broj hopova, vektor puta i status. Spisak svih parametara se može naći u RFC 5036.



Slika 4.3.5. Struktura FEC parametra

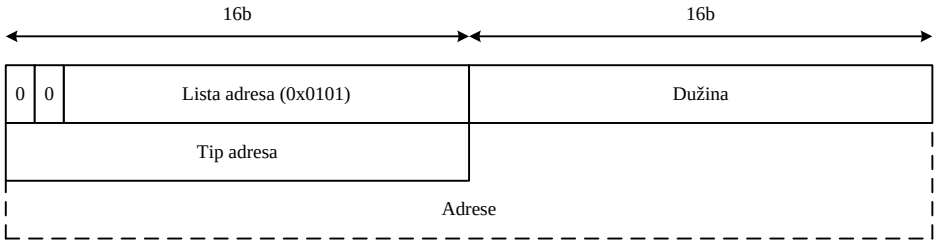
FEC parametar se koristi za navođenje FEC klasa na koje se labela u LDP poruci odnosi (labela se smešta u svoj parametar). Struktura FEC parametra je prikazana u gornjoj polovini slike 4.3.5. Kao što se vidi FEC parametar se sastoji od jednog ili više FEC elemenata. Postoje

dva tipa FEC elementa - džoker i prefiks. Džoker element se sastoji iz samo jednog bajta vrednosti 0x01 i koristi se za označavanje svih FEC klasa za koje je vezana labela iz poruke. Džoker je zgodan kada se želi ukinuti ili osloboditi neka labela, pa je onda znatno zgodnije navesti džoker element umesto da se navode sve FEC klase vezane za labelu ponaosob. Prefiks element navodi egzaktno FEC klasu. Struktura prefiks elementa je prikazana u donjoj polovini slike 4.3.5. Tip adrese definiše tip mrežne adrese (IPv4, IPv6) i na osnovu njega se zna kako tumačiti polje vrednost prefiksa. Dužina prefiksa označava broj bita iz polja vrednost prefiksa koji zaista spadaju u prefiks. Vrednost prefiksa sadrži sam prefiks i eventualnu dopunu tako da dužina ovog polja bude jednaka celom broju bajtova.



Slika 4.3.6. Struktura parametra labela

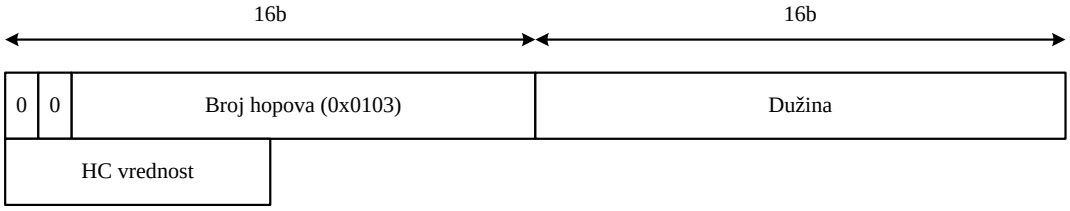
Parametar labela se koristi za specificiranje labele koja se oglašava. Struktura ovog parametra je prikazana na slici 4.3.6. U gornjoj polovini slike je prikazan parametar za slučaj generičke labele, a u donjoj za slučaj ATM labele. Generička labela u polju labele koristi samo prvih 20 bita jer je to dužina labele kao što se može videti i sa slike 4.2.2 koja prikazuje strukturu *shim* zaglavlja. ATM labela se predstavlja u vidu vrednost VPI i VCI identifikatora. V polje u ATM labeli označava da li se koriste VPI i VCI delovi u labeli (V=01 - samo VPI se koristi, V=10 - samo VCI se koristi, V=00 - i VPI i VCI se koriste). Res (*Reserved*) biti su rezervisani za eventualnu buduću upotrebu.



Slika 4.3.7. Struktura parametra lista adresa

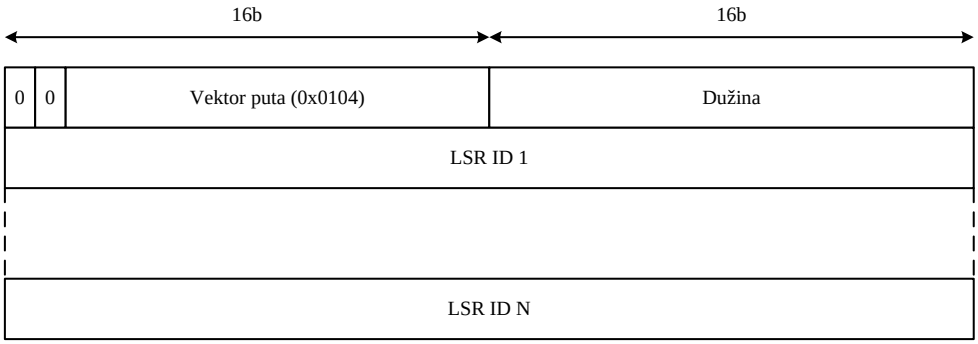
Parametar lista adresa se koristi za oglašavanje adresa. Struktura parametra lista adresa je prikazana na slici 4.3.7. Tip adresa označava koje adrese se koriste (IPv4, IPv6) da bi se znalo tumačiti polje adrese koje sadrži listu adresa (IPv4 su 32-bitne adrese, a IPv6 128-bitne adrese, pa se na osnovu tipa adrese zna koliko bita treba uzeti po jednom članu liste).

Parametar broj hopova se može koristiti za računanje broja hopova u procesu uspostave LSP puta. Struktura parametra broj hopova je prikazana na slici 4.3.8. Polje HC (*Hop Count*) vrednost predstavlja trenutni broj hopova i svaki posredni čvor na LSP putu će inkrementirati ovu vrednost.

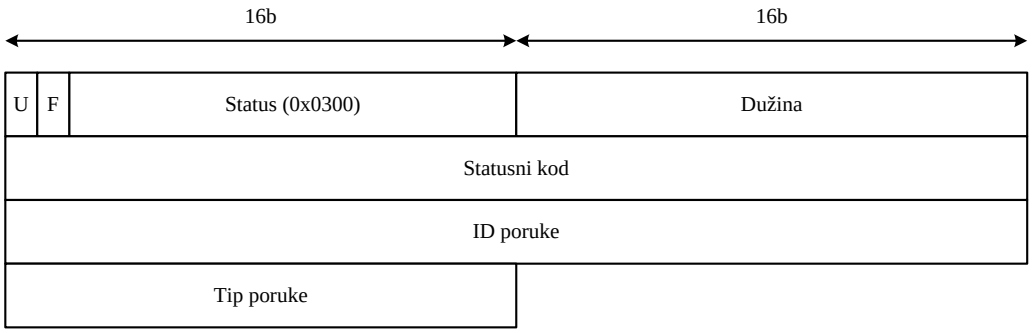


Slika 4.3.8. Struktura parametra broj hopova

Parametar vektor puta se koristi za proces detekcije eventualnih petlji u LSP putu. Vektor puta sadrži spisak svih LSR rutera na putu, pa se na osnovu toga lako može uočiti eventualna petlja. Svaki LSR ruter će ispitivanjem ovog parametra utvrditi da postoji petlja ako se njegova identifikacija nađe u spisku LSR rutera unutar ovog parametra. Struktura parametra vektor puta je prikazana na slici 4.3.9. Parametar vektor puta ređa identifikacije LSR rutera u vidu liste LSR ID polja.



Slika 4.3.9. Struktura parametra vektor puta



Slika 4.3.10. Struktura parametra status

Parametar status se koristi u LDP porukama obaveštenja. Struktura parametra status je prikazana na slici 4.3.10. Statusni kod predstavlja obaveštenje (preciznije nižih 30 bita predstavlja obaveštenje), pri čemu dva najviša bita polja statusni kod predstavljaju bite E i F. E bit označava da li je u pitanju obaveštenje o grešci (E=1) ili regularno obaveštenje (E=0). F bit označava da li se obaveštenje treba proslediti dalje (F=1) ili ne (F=0). ID poruke i tip poruke sadrže vrednosti iz LDP poruke na koju se odnosi dotično obaveštenje (na ovaj način izvor

originalne poruke lako može da detektuje na koju njegovu poruku se odnosi primljeno obaveštenje), a ako se obaveštenje ne odnosi na neku konkretnu poruku onda se ID poruke i tip poruke postavljaju na vrednost 0. Spisak svih 30-bitnih vrednosti statusnog koda (obaveštenja) definisanih u RFC 5036 su prikazani u tabeli 4.3.1.

Tabela 4.3.1 - Vrednosti statusnog koda parametra status

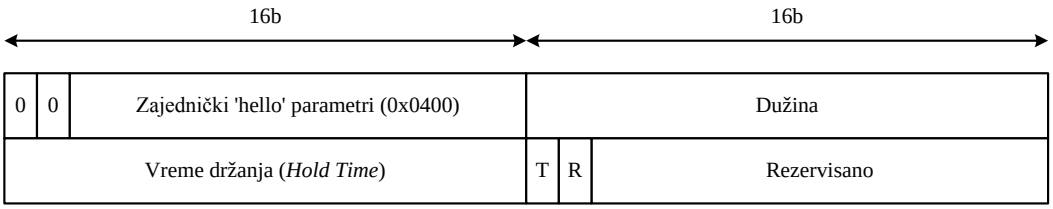
Statusni kod	E bit	Tumačenje
0x0000000	0	*Success*
0x0000001	1	*Bad LDP Identifier*
0x0000002	1	*Bad Protocol Version*
0x0000003	1	*Bad PDU Length*
0x0000004	0	*Unknown Message Type*
0x0000005	1	*Bad Message Length*
0x0000006	0	*Unknown TLV*
0x0000007	1	*Bad TLV Length*
0x0000008	1	*Malformed TLV Value*
0x0000009	1	*Hold Timer Expired*
0x000000A	1	*Shutdown*
0x000000B	0	*Loop Detected*
0x000000C	0	*Unknown FEC*
0x000000D	0	*No Route*
0x000000E	0	*No Label Resources*
0x000000F	0	*Label Resources / Available*
0x0000010	1	*Session Rejected / No Hello*
0x0000011	1	*Session Rejected / Parameters Advertisement Mode*
0x0000012	1	*Session Rejected / Parameters Max PDU Length*
0x0000013	1	*Session Rejected / Parameters Label Range*
0x0000014	1	*KeepAlive Timer Expired*
0x0000015	0	*Label Request Aborted*
0x0000016	0	*Missing Message Parameters*
0x0000017	0	*Unsupported Address Family*
0x0000018	1	*Session Rejected / Bad KeepAlive Time*
0x0000019	1	*Internal Error*

Tabela 4.3.2 - Spisak LDP poruka

LDP poruka	Tip poruke (kod)	Obavezni parametri
Notification	0x0001	Status
Hello	0x0100	Zajednički ’hello’ parametri
Initialization	0x0200	Zajednički parametri sesije
KeepAlive	0x0201	-
Address	0x0300	Lista adresa
Address Withdraw	0x0301	Lista adresa
Label Mapping	0x0400	FEC, labela
Label Request	0x0401	FEC
Label Abort Request	0x0404	FEC, ID Label Request poruke
Label Withdraw	0x0402	FEC
Label Release	0x0403	FEC

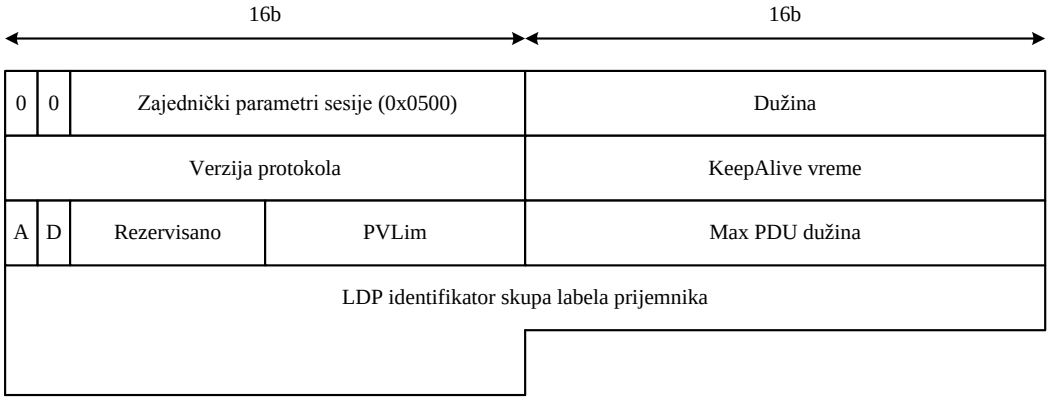
Tabela 4.3.2 sadrži spisak svih LDP poruka definisanih u RFC 5036. Notification poruka se koristi za slanje obaveštenja u toku LDP sesije i mora da sadrži parametar status jer se u njemu nalazi samo obaveštenje. Opciono, Notification poruka može da sadrži i parametre

proširenи status, vraćen PDU, vraćena poruka. Proširenи status dodaje dodatne detalje u odnosu na obaveštenje iz parametra status. Vraćen PDU parametar sadrži deo PDU jedinice (zaglavlje i dovoljan deo korisnog dela PDU jedinice) na koju se odnosi obaveštenje da bi predajna strana mogla lakše da utvrdi problem. Vraćena poruka sadrži dovoljan deo LDP poruke na koju se odnosi obaveštenje da bi predajna strana mogla lakše da utvrdi problem.



Slika 4.3.11. Struktura parametra zajednički ’hello’ parametri

Hello poruke se šalju u već opisanom mehanizmu otkrivanja suseda. Struktura obaveznog parametra zajednički ’hello’ parametri je prikazana na slici 4.3.11. Vreme držanja označava koliko dugo sused treba da drži zapis o primljenoj Hello poruci (u suštini, vrednost ’hello’ tajmera). T bit označava da li je u pitanju Link Hello (T=0) ili Targeted Hello (T=1) poruka. R bit označava da li se zahteva da prijemna strana počne slati periodično Targeted Hello (R=1) poruke ili ne (R=0). Opcioni parametri koji se mogu staviti u Hello poruku su IPv4 transportna adresa, IPv6 transportna adresa, i redni broj konfiguracije. Parametri IPv4 i IPv6 transportne adrese sadrže IPv4, odnosno IPv6 adresu koju treba koristiti za započinjanje LDP sesije (sa tom adresom će biti ostvarena TCP veza i preko nje LDP sesija). Parametar redni broj konfiguracije se može koristiti za praćenje promena konfiguracije predajne strane. Ako se detektuje promena u rednom broju tada se zna da je na suprotnoj strani došlo do promene konfiguracije. Ovaj opcioni parametar je zgodan u slučaju kada se LDP sesija nije uspela uspostaviti. Nakon svakog neuspeha uspostave, vrši se ponovni pokušaj, ali su razmaci između ponovnih pokušaja sve veći. S obzirom da aktivni ruter inicira uspostavu, ovaj opcioni parametar u Hello porukama pasivnog rutera signalizira da je pasivni ruter promenio konfiguraciju i da treba pokušati ponovo uspostaviti LDP sesiju.



Slika 4.3.12. Struktura parametra zajednički parametri sesije

Initialization poruke se šalju u procesu uspostave LDP sesije kao što je već opisano ranije u tekstu. Struktura obaveznog parametra zajednički parametri sesije je prikazana na slici 4.3.12. KeepAlive vreme označava maksimalno vreme između dve uzastopne LDP PDU jedinice za vreme trajanja LDP sesije. Ako KeepAlive tajmer istekne, strana na kojoj je tajmer istekao će generisati odgovarajuću Notification poruku o toj grešci i raskinuti LDP sesiju. A bit označava

tip oglašavanja (A=0 - bezuslovno oglašavanje, A=1 - oglašavanje u uzvodnom smeru na zahtev). D bit označava da li je aktiviran mehanizam za detekciju petlji (D=1) ili ne (D=0). PVLim označava maksimalnu dužinu vektora puta ako je aktiviran mehanizam za detekciju petlji, u suprotnom se postavlja na vrednost 0. Max PDU dužina definiše maksimalnu dužinu LDP PDU jedinice za vreme LDP sesije (dok se ne uspostavi sesija podrazumevana maksimalna dužina je 4096 bajtova). Ako je vrednost ovog polja 255 ili manja onda se zadržava podrazumevana maksimalna dužina od 4096 bajtova. LDP identifikator skupa labela prijemne strane sadrži identifikator iz Hello poruke koju je poslala strana koja prima Initialization poruku, pa na osnovu tog identifikatora, kao i identifikatora predajne strane iz LDP PDU zaglavlja, prijemna strana zna na koju poruku se odnosi Initialization poruka, preciznije na koji skup labela. Opciono se u sklopu Initialization poruke mogu poslati parametri ATM parametri sesije i FR parametri sesije, ako je link preko koga se ostvaruje susedstvo ATM ili FR.

KeepAlive poruka se šalje kao potvrda na Initialization poruku u procesu uspostave LDP sesije, a tokom trajanja LDP sesije se povremeno šalje ako nema drugih LDP poruka za slanje da ne bi istekao KeepAlive tajmer na suprotnoj strani.

Poruka Address se koristi za oglašavanje mrežnih adresa interfejsa uređaja (LSR rutera), a Address Withdraw za oglašavanje nevalidnosti (oglašavanje da se više ne koriste) mrežnih adresa interfejsa uređaja.

Label Mapping poruke se koriste za oglašavanje vezivanja labela na FEC klase, tj. mapiranja labela na FEC klase. Opcioni parametri koji se mogu koristiti su već objašnjeni broj hopova i vektor puta, ali i id poruke zahteva za labelom. Parametar id poruke zahteva za labelom se obavezno mora staviti ako se Label Mapping poruka šalje na zahtev tj. kao odgovor na Label Request poruku da bi suprotna strana znala na koji njen zahtev se odnosi dotična Label Mapping poruka. Label Request poruka se šalje kao zahtev suprotnoj strani da pošalje mapiranje labele na FEC klasu navedenu u poruci. Opcioni parametri ove poruke su broj hopova i vektor puta. Label Abort Request poruka se koristi za poništavanje već poslate Label Request poruke. Label Withdraw poruka se koristi za oglašavanje prestanka važenja mapiranja labele na navedenu FEC klasu. Parametar labela nije obavezan i ako se ne navede onda prijemna strana na osnovu FEC klase zaključuje da su sve labele vezane za dotičnu FEC klasu prestale da važe, a ako se parametar labela navede onda prijemna strana zna da su samo navedene labele prestale da važe (preciznije da su njihova mapiranja prestala da važe). Label Release poruka se koristi za signaliziranje suprotnoj strani da može da raskine mapiranje za navedenu FEC klasu koju je izvršila na ranije poslat zahtev (Label Request). Parametar labela nije obavezan i ako se ne navede onda prijemna strana na osnovu FEC klase zaključuje da sve labele vezane za dotičnu FEC klasu mogu da se oslobode, a ako se parametar labela navede onda prijemna strana zna da samo navedene labele treba da se oslobode.

LDP originalno ne podržava eksplicitne rute, a one su veoma bitne za efikasno i kvalitetno ostvarivanje VPN tunela, QoS servisa, balansiranja saobraćaja i dr. Razlog leži u tome što se LDP oslanja na rad osnovnih protokola rutiranja i samim tim kao putanje vidi jedino najkraće puteve u mreži pa samo njih može i da koristi. Eksplicitne rute mogu da izaberu proizvoljan put kroz mrežu, a ne samo najkraći. Stoga je definisano proširenje LDP protokola u vidu dodavanja podrške za CR (*Constrained based Routing*) putanje tj. gde se prilikom definisanja eksplicitne rute gleda više parametara nego kod klasičnih protokola rutiranja (otuda se moraju definisati i proširenja protokola rutiranja koji bi razmenjivali između rutera i ove dodatne informacije, na primer, OSPF-TE). LDP koji podržava ovo proširenje se često označava

i nazivom CR-LDP protokol i on je definisan u RFC 3212. LSP putanja koja se ostvari primenom CR-LDP proširenja se označava terminom CR-LSP.

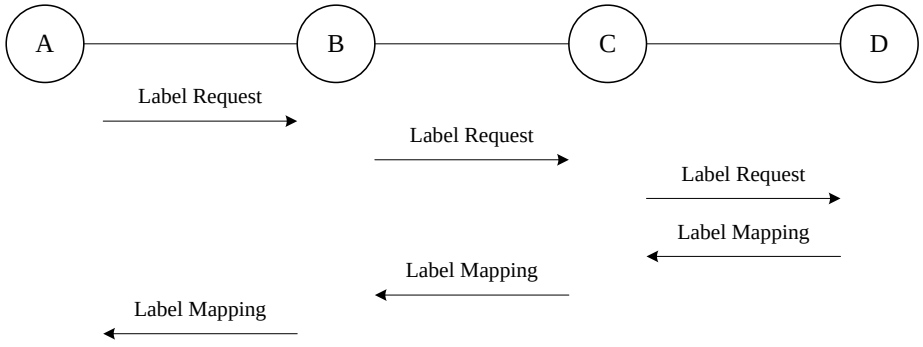
Da bi CR-LDP mogao da funkcioniše, pored samih proširenja u odnosu na originalan LDP potrebno je konfigurisati sledeće funkcionalnosti originalnog LDP protokola:

- Upotreba Label Request i Label Mapping poruka sa vezivanjem labele u uređenom redosledu i sa oglašavanjem u uzvodnom smeru na zahtev
- Upotreba mehanizma za detekciju petlji

CR-LDP dodaje sledeće funkcionalnosti u odnosu na LDP protokol:

- Formiranje eksplicitnih puteva, pri čemu se mogu formirati i striktni i labavi eksplicitni putevi.
- Specifikacija saobraćajnih parametara tokova čime je omogućena QoS podrška u MPLS mreži, ali i utvrđivanje da li je moguće formirati željeni eksplicitni put koji bi podržao saobraćajne parametre toka (za koji se i uspostavlja eksplicitni put), a da se ne naruše postojeći tokovi u mreži.
- Fiksiranje puta omogućava da se, u slučaju labavog rutiranja, delovi puta koji su labavo rutirani ne menjaju tokom vremena. Na primer, ako bi ruteri u tom delu mreže našli novi, bolji put za taj labavi segment LSP puta on se ipak neće iskoristiti ako je labavi eksplicitni put fiksiran.
- Nivoi prioriteta eksplicitnog puta prilikom uspostave i za vreme trajanja puta predstavljaju parametre koji pomažu u utvrđivanju koji eksplicitni putevi smeju da se raskinu, a koji ne. Naime, ako eksplicitni put ne može da se uspostavi na nekoj trasi jer nema dovoljno resursa, tada u slučaju da ima velik prioritet uspostave, on može da izazove raskidanje postojećih eksplicitnih puteva (čiji je prioritet za vreme trajanja puta manji od prioriteta uspostave novog puta) da bi se oslobodili resursi za njega. Slično, prioritet za vreme trajanja puta određuje koji eksplicitni putevi će biti prvi raskinuti u slučaju da dođe do potrebe za oslobađanjem resursa u pojedinim čvorovima mreže.
- Identifikacija LSP puta (LSP ID) je neophodna za identifikovanje eksplicitnih puteva u okviru CR-LDP poruka.

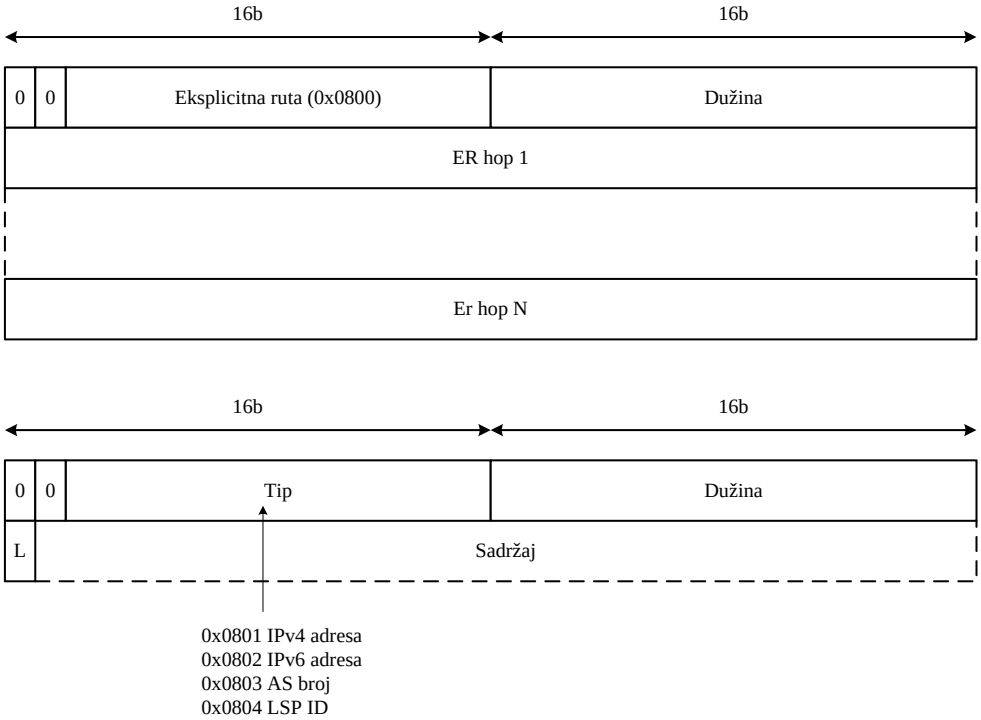
Princip rada CR-LDP proširenja je prikazan na slici 4.3.13.



Slika 4.3.13. Princip rada CR-LDP

CR-LDP prilikom uspostave eksplicitnog puta koristi vezivanje labele u uređenom redosledu i oglašavanje u uzvodnom smeru na zahtev. U primeru sa slike 4.3.13 se uspostavlja striktni eksplicitni put od rutera A do rutera D. Ruter A šalje Label Request zahtev ruteru B da mu pošalje vezivanje (mapiranje) labele za navedenu FEC klasu, pri čemu u Label Request zahtevu navodi striktnu eksplicitnu putanju u vidu niza rutera B, C, D (naravno, ruter A može da navede i labavu eksplicitnu putanju). Pošto ruter B nije izlazni LER ruter, on šalje Label Request zahtev ruteru C, a pošto ni ruter C nije izlazni LER ruter, on šalje Label Request zahtev ruteru D. Ruter D je izlazni LER ruter i on može da izvrši vezivanje labele na navedenu FEC klasu i to mapiranje šalje u vidu Label Mapping odgovora ruteru C. Ruter C sada izvršava svoje vezivanje labele na navedenu FEC klasu i šalje svoje mapiranje ruteru B i na kraju ruter B izvršava svoje vezivanje labele na navedenu FEC klasu i šalje svoje mapiranje rutera A čime je eksplicitni put kreiran. Naravno, vezivanje labele u uređenom redosledu i oglašavanje u uzvodnom smeru na zahtev je moguće i u originalnom LDP protokolu, ali tamo bi kreirani LSP put zavisio od rada protokola rutiranja jer bi svaki čvor ponaosob utvrđivao sledeći hop na putu na osnovu svoje tabele usmeravanja na bazi IP adresa.

CR-LDP proširuje funkcionalnost LDP protokola podrškom za eksplicitne rute. Stoga su uvedeni novi parametri i izmenjene su delimično strukture postojećih poruka i u nastavku teksta ćemo navesti modifikacije koje unosi CR-LDP.

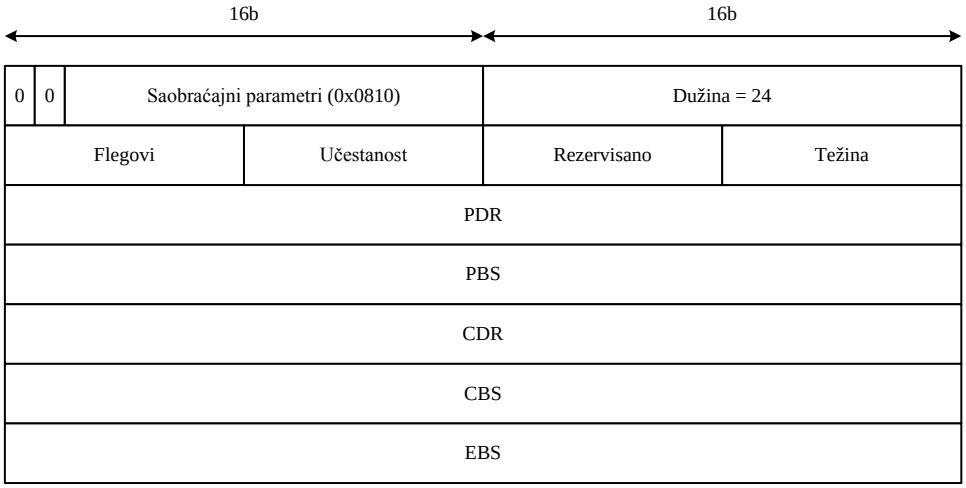


Slika 4.3.14. Parametar eksplicitna ruta

Label Request poruka je doživela modifikacije u vidu dodatnih parametara koje može da sadrži. Parametar LSP ID je obavezan i on predstavlja identifikaciju LSP puta. Opcioni parametri, uvedeni CR-LDP proširenjem, koji mogu da se koriste su eksplicitna ruta, saobraćajni parametri, fiksiranje puta, klasa resursa i prioritet. Label Mapping poruka je takođe doživela modifikacije. Sada je parametar id poruke zahteva za labelom obavezan jer se u uspostavi eksplicitnog puta koristi oglašavanje u uzvodnom smeru na zahtev. Takođe, opcioni parametri

uvedeni CR-LDP proširenjem su saobraćajni parametri i LSP ID. LSP ID omogućava lakše vezivanje uzvodnom ruteru odgovora na svoj poslati zahtev.

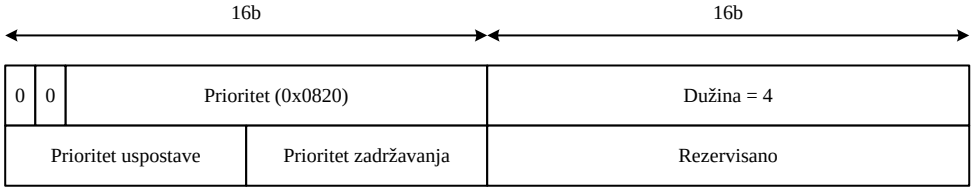
Parametar eksplicitna ruta se koristi za definisanje eksplicitnog puta (striktnog ili labavog). Struktura parametra eksplicitna ruta je prikazana na slici 4.3.14. Kao što se vidi ovaj parametar se sastoji iz liste hopova (ER (*Explicit Routing*) hop), pri čemu je struktura jednog ER hopa prikazana u donjem delu slike. Tip ER hopa ukazuje na tip adresiranja hopa koji može biti u vidu IPv4 ili IPv6 adrese, broja AS (autonomni sistem) domena ili u vidu identifikacije LSP puta (LSP ID). Polje sadržaj zavisi od definisanog tipa i predstavlja adresu/identifikaciju hopa na eksplicitnom putu. L (*Loose*) bit označava da li se koristi labavo (L=1) ili striktno (L=0) rutiranje do navedenog ER hopa.



Slika 4.3.15. Parametar saobraćajni parametri

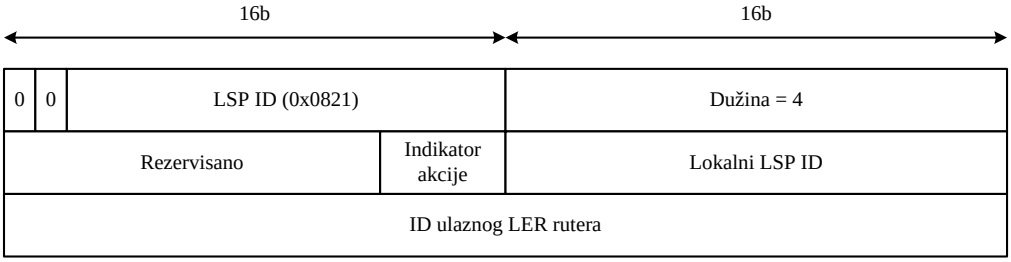
Na slici 4.3.15 je prikazana struktura parametra saobraćajni parametri koji se koriste za opisivanje karakteristika saobraćaja toka za koji se uspostavlja eksplicitna ruta (eksplicitni LSP put). U okviru polja flegovi se nalaze jednobitne indikacije vezane za parametre saobraćaja (PDR, PBS, CDR, CBS, EBS i težina) koje signaliziraju za svaki parametar da li se može pregovarati ili ne tokom uspostave puta. Dva bita ovog polja koja se ne koriste su rezervisana za eventualnu buduću upotrebu. PDR (*Peak Data Rate*) označava vršni protok toka u bajtovima po sekundi. PBS (*Peak Burst Size*) označava maksimalnu veličinu bursta toka. PDR i PBS se koriste kao parametri bušne kofe na ulazu u MPLS domen radi ostvarivanja kontrole korisničkog toka (da li poštuje dogovorene parametre saobraćaja ili ne). CDR (*Commited Data Rate*) označava protok koji je mreža spremna da garantuje toku. CBS (*Commited Burst Size*) označava veličinu bursta toka koji mreža garantuje da može da primi. EBS (*Excess Burst Size*) definiše veličinu prekomernog bursta koji narušava CDR i CBS parametre i koristi se za opsluživanje prekomernog saobraćaja u vidu odbacivanja, obeležavanja kao *best effort* saobraćaj i sl. CDR i CBS se koriste kao parametri bušne kofe koja određuje pakete koji upadaju u garantovane okvire saobraćaja, a iza te kofe se može postaviti kofa za merenje prekomernog saobraćaja (koji izlazi iz okvira garantovanog saobraćaja) i čiji parametri su CDR i EBS. Na osnovu navedene tri kofe se mogu implementirati željeni mehanizmi opsluživanja paketa toka. Na primer, svi paketi koji naruše parametre kofe PDR i PBS mogu biti odbačeni ili odmah označeni sa *best effort* kvalitetom. Paketi koji naruše parametre kofe CDR i CBS se na osnovu dodatnog ispitivanja kofom parametara CDR i EBS mogu označiti sa *best effort* kvalitetom ili se mogu odbaciti i sl. Takođe, može se raditi i uobličavanje toka i dr. Sam protokol ne definiše koji mehanizmi

opsluživanja treba da se koriste već to zavisi od samih proizvođača i operatera, a protokol samo definiše tumačenja saobraćajnih parametara. Polje učestanost definiše sa kolikom učestanosti garantovani CDR protok treba da bude na raspolaganju korisniku. Trenutno su definisane tri vrednosti - nespecificirana učestanost (0), učestano (1), veoma učestano (2). Na primer, veoma učestano označava da na nivou trajanja najkraćeg paketa toka prosečan protok opsluživanja toka mora biti jednak CDR, a učestano označava da na nivou ukupnog trajanja manjeg broja najkraćih paketa toka prosečan protok opsluživanja toka mora biti jednak CDR. Težina određuje težinu toka (u suštini tok je ovde isto što i LSP put). Težina određuje relativni udeo toka u propusnom opsegu koji je slobodan i za koji se bore svi tokovi u čvoru. Dobijeni udeo se koristi za opsluživanje saobraćaja toka koji ne upada u garantovane okvire toka.



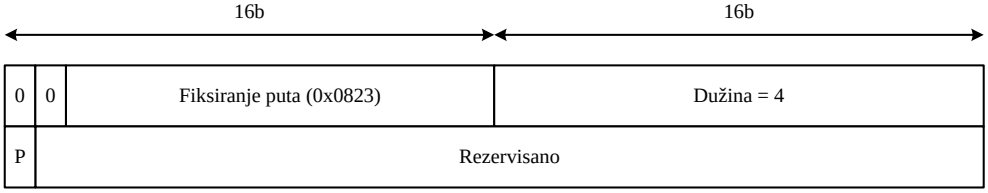
Slika 4.3.16. Parametar prioritet

Na slici 4.3.16 je prikazan parametar prioritet. Polje prioritet uspostave definiše prioritet prilikom uspostave puta. Što je veći prioritet veća je verovatnoća da će eksplicitni put moći da se uspostavi jer će moći da raskine već postojeće manje prioritetne puteve u slučaju nedostatka resursa na pojedinim deonicama puta koji se uspostavlja. Polje prioritet zadržavanja definiše prioritet zadržavanja puta na istoj ruti prilikom uspostave nekog novog puta. Što je veći ovaj prioritet, manja je verovatnoća raskidanja puta usled pojave novog eksplicitnog puta. Raskidanje se svodi na slanje Label Withdraw poruke u uzvodnom smeru, odnosno Label Release poruke u nizvodnom smeru.



Slika 4.3.17. Parametar LSP ID

Na slici 4.3.17 je prikazan parametar LSP ID koji predstavlja identifikaciju LSP puta. Polje indikator akcije označava da li je u pitanju modifikacija postojećeg LSP puta (0001) ili uspostava novog LSP puta (0000). Lokalni LSP ID je lokalna (jedinstvena) identifikacija u ulaznom LER ruteru dotičnog puta. ID ulaznog LER rutera predstavlja identifikaciju ulaznog LER rutera za koju se može koristiti bilo koja IPv4 adresa tog rutera.



Slika 4.3.18. Parametar fiksiranje puta

Na slici 4.3.18 je prikazan parametar fiksiranje puta. U okviru ovog parametra se specificira vrednost bita P (*Pinning*) kojom se signalizira da li se putanja fiksira (P=1) ili ne (P=0). Ovaj parametar ima smisla u slučaju labavog rutiranja. Ako se put fiksira tada se LSP put ne menja u labavim delovima čak i ako u njima dođe do mogućnosti kreiranja boljeg puta, u suprotnom može doći do modifikacije LSP puta u labavim delovima puta.

Tabela 4.3.3 - Vrednosti statusnog koda parametra status - CR-LDP proširenja

Statusni kod	E bit	Tumačenje
0x4000001	1	*Bad Explicit Routing TLV Error*
0x4000002	1	*Bad Strict Node Error*
0x4000003	1	*Bad Loose Node Error*
0x4000004	1	*Bad Initial ER-Hop Error*
0x4000005	1	*Resource Unavailable*
0x4000006	1	*Traffic Parameters Unavailable*
0x4000007	1	*LSP Preempted*
0x4000008	1	*Modify Request Not Supported*

Tabela 4.3.3 prikazuje dodatna obaveštenja (statusne kodove) koja je moguće poslati preko parametra status u okviru Notification poruke za slučaj CR-LDP proširenja. Kao što vidimo iz tabele, u pitanju su uglavnom greške koje se mogu javiti prilikom uspostave eksplicitnog puta.

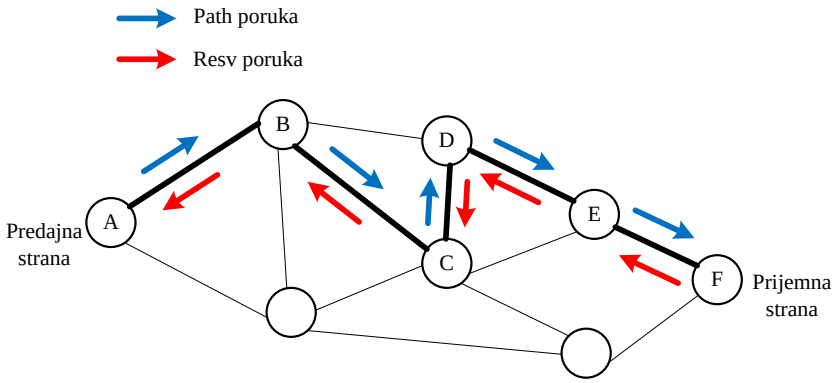
4.4. RSVP-TE

RSVP-TE (*Resource Reservation Protocol - Traffic Enginering*) se koristi za distribuciju MPLS labela. RSVP-TE, definisan u RFC 3209, predstavlja proširenje funkcionalnosti RSVP protokola. RSVP protokol (definisan u RFC 2205) se koristi u sklopu IntServ arhitekture kao signalizacija kojom se obezbeđuje rezervisanje resursa u ruterima za QoS opsluživanje tokova. S obzirom na potrebu QoS implementacije u MPLS domenu, razvijena je ekstenzija RSVP protokola u vidu RSVP-TE kojom je omogućeno uspostavljanje LSP puteva kroz MPLS domen. Pošto je RSVP-TE proširenje RSVP protokola, u okviru ovog potpoglavlja će prvo biti objašnjen RSVP protokol, a potom i RSVP-TE proširenje.

RSVP se koristi u okviru IntServ arhitekture za rezervisanje resursa u mrežnim čvorovima (ruterima) za tokove, pri čemu su podržane sve klase servisa navedene u sekciji 4.1.2. Rezervisanje se vrši u jednom smeru, odnosno tokovi se smatraju jednosmernim. U slučaju dvosmerne komunikacije neophodno je izvršiti dva rezervisanja, po jedno za svaki smer komunikacije. RSVP koristi usluge unikast i multikast protokola rutiranja za određivanje puta kroz mrežu na kom se treba izvršiti rezervacija resursa za dati tok. RSVP je orijentisan na prijemnu stranu, odnosno prijemna strana je ta koja pokreće rezervaciju resursa, što je i logično jer je prijemnik taj koji zna koji kvalitet servisa želi da primi od mreže. Drugi razlog je efikasna podrška za multikast i multipoint (više predajnika šalje, i taj sadržaj prima više prijemnika) komunikacije jer orijentacija na prijemnu stranu omogućava lako priključivanje novih korisnika u komunikacionu sesiju i odlazak korisnika iz sesije (obe operacije se odvijaju na nivou jednog korisnika tj. jednog prijemnika sa stanovišta učesnika u komunikaciji).

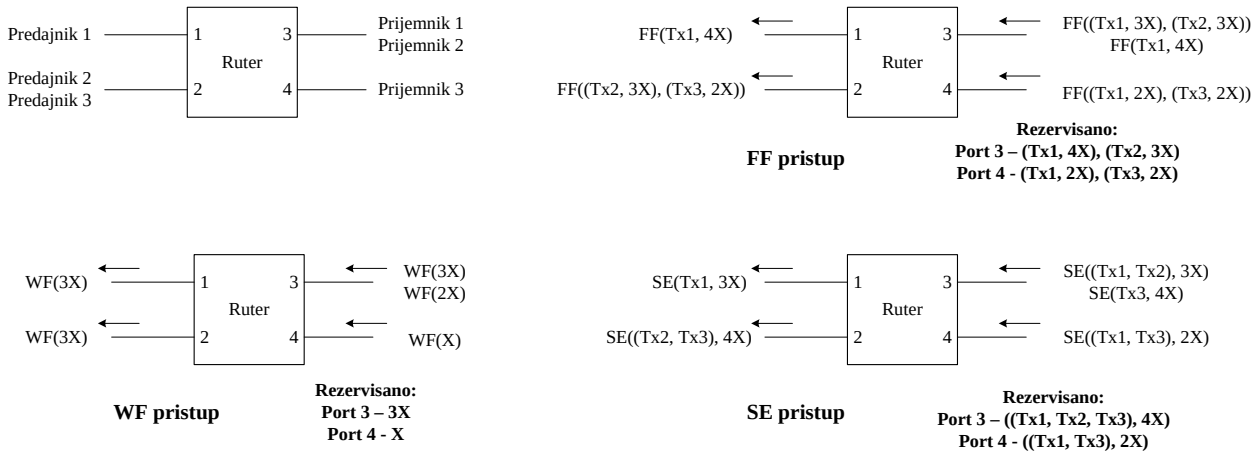
RSVP sesija se opisuje tripletom odredišna IP adresa (unikast ili multikast), transportni protokol i opciono port transportnog protokola. Na osnovu sesije ruteri mogu da prepoznaju da li je u pitanju nova sesija za koju treba izvršiti rezervaciju resursa ili postojeća sesija za koju

eventualno treba modifikovati/osvežiti rezervaciju. Na primer, ako se novi član priključuje u sesiju i priključen je na ruter koji je već rezervisao resurse za tu sesiju zbog drugih članova povezanih (dostupnih) na isti port rutera kao i novi član, ruter će to prepoznati i neće biti potrebe da rezerviše nove ili dodatne resurse (sem ako novi član ne zahteva bolji kvalitet servisa od drugih korisnika pa ruter mora da zauzme dodatne resurse).



Slika 4.4.1. Kreiranje rezervacije

Zahtev za rezervacijom se sastoji od dva dela, specifikacije toka i specifikacije filtera. Specifikacija toka definiše saobraćajne karakteristike toka i željeni kvalitet servisa (TSpec i RSpec specifikacije iz IntServ arhitekture), a specifikacija filtera definiše na koje pakete toka će se odnositi rezervacija (na primer, može se navesti multikast adresa grupe, ili odredišna unikast adresa i TCP port i sl.). Princip kreiranja rezervacije je prikazan na slici 4.4.1. Problem orijentacije na prijemnu stranu da izvrši rezervisanje resursa leži u činjenici da prijemna strana ne zna lokaciju izvorišta tj. predajne strane. Otuda, predajna strana šalje periodično Path poruku koja ide istim putem i smerom kao i korisnički paketi unutar sesije. Svi RSVP ruteri na putu beleže sesiju navedenu u okviru Path poruke. Path poruka unutar sebe nosi opis korisničkih paketa (izvorišna IP adresa i izvorišni transportni port) koje predajna strana generiše unutar sesije (tzv. *sender template*) na osnovu čega ruteri mogu prepoznati dotične korisničke pakete unutar sesije (uz informaciju iz samog IP paketa o odredišnoj adresi). Path poruka ima istu izvorišnu i odredišnu IP adresu kao korisnički paketi unutar sesije čime se obezbeđuje da oni idu istim putem kroz mrežu. Prijemnik na osnovu Path poruke zna adresu izvorišta pa kreira Resv poruku ka izvorištu koja će ići istim putem kao i korisnički paketi unutar sesije samo obrnutim smerom. Resv poruka adresira prvi sledeći uzvodni RSVP ruter u nizu na putu ka izvorištu. Ovaj hop po hop princip rutiranja obezbeđuje da Resv poruka prolazi kroz isti put (preciznije, iste RSVP rutere) u obrnutom smeru kao Path poruka. Resv poruka izvršava rezervaciju resursa u svim RSVP ruterima na putu ka odredištu (RSVP ruter je ruter koji implementira podršku za RSVP). Ukoliko rezervacija bude neuspešna poslaće se poruka o neuspehu prijemnoj strani. Napomenimo da se između RSVP rutera mogu nalaziti ruteri koji ne podržavaju RSVP protokol i koji su transparentni za RSVP pakete i pakete toka, odnosno oni ih obrađuju i prosleđuju kao i sve ostale IP pakete. Naravno, takvi ne-RSVP ruteri mogu da ugroze kvalitet servisa koji obezbeđuju RSVP ruteri, što je i navedeno kao tipičan problem u obe QoS arhitekture (IntServ i DiffServ). Ako za istu sesiju pristigne više Resv poruka od različitih prijemnika u ruter one se spajaju u jednu Resv poruku koja se šalje uzvodno (dodatni uslov je da se sve rezervacije odnose na isti skup predajnika u slučaju kada ima više predajnika u sesiji). Path poruke u sebi nose TSpec specifikaciju, a Resv poruke RSpec specifikaciju tako da na osnovu ovih specifikacija ruter može da proceni kakve resurse treba da rezerviše za dotični tok tj. RSVP sesiju.

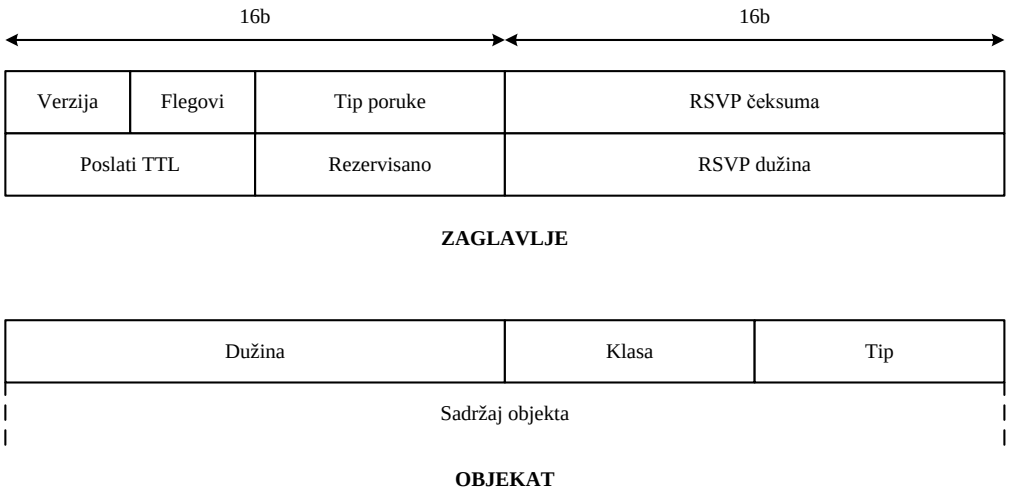


Slika 4.4.2. Tri pristupa u izvršenju rezervacije u ruteru

Kada se vrši rezervacija postoje tri moguća pristupa - WF (*Wildcard Filter*), FF (*Fixed-Filter*) i SE (*Shared-Explicit*) pristupi. WF pristup kreira jednu zajedničku Resv poruku koju šalje ka svim predajnicima (u uzvodnom smeru), pri čemu je generisana Resv poruka dimenzionisana po primljenom Resv zahtevu koji je tražio najveće resurse. Količina rezervisanih resursa, na svakom izlaznom portu preko koga se dolazi do nekog od prijemnika, se dimenzioniše prema prijemniku koji je poslao zahtev za najvećim resursima na dotičnom portu. Kao što se vidi sa slike 4.4.2, ruter na svojim izlaznim portovima 3 i 4 preko kojih su dostupni prijemnici dimenzioniše resurse u skladu sa najvećim rezervacionim zahtevom primljenim preko tih portova, respektivno. Na portove 1 i 2 preko kojih su dostupni predajnici šalje rezervacioni zahtev u WF vidu koji je dimenzionisan prema najvećem zahtevu koji je primio na portovima 3 i 4 (u pitanju je zahtev WF(3X) sa porta 3, pri čemu X predstavlja jedinicu zahtevanih resursa u primeru). FF pristup kreira zasebnu rezervaciju za svaki od predajnika u sesiji (tj. za tokove koji generišu predajnici) na izlaznim portovima rutera, pri čemu se one dimenzionišu prema Resv zahtevu koji je tražio najveće resurse i koji je primljen na dotičnom portu (za svaki predajnik se gleda maksimalan zahtev ponaosob). U uzvodnom smeru se generišu Resv zahtevi FF pristupa, pri čemu se oni dimenzionišu za svaki predajnik ponaosob i to prema najvećim resursima zahtevanim za dotične predajnike ponaosob od svih primljenih Resv zahteva. Sa slike 4.4.2 se vidi da su na port 3 stigla dva zahteva, a na port 4 jedan zahtev. Na portu 4 se rezervišu zasebni resursi za oba navedena predajnika (1 i 3), a na portu 3 se takođe rezervišu resursi za dva predajnika (1 i 2) jer ih je ukupno navedeno 2. Pri tome se na portu 3 resursi vezani za predajnik 1 vezuju za veći zahtev (4X). U uzvodnom smeru se generišu Resv zahtevi prema najvećim zahtevanim resursima iz primljenih Resv poruka. Tako se za Tx1 traže 4X resursi jer je to bio maksimalan zahtev u primljenim Resv porukama. Resv poruke poslate u uzvodnom smeru oglašavaju zahteve takođe u FF pristupu. SE pristup je modifikacija WF pristupa u smislu da se definiše skup predajnika za koje se rezervišu zajednički resursi u vidu jedne rezervacije. Može se videti sa slike 4.4.2 da su rezervisani resursi u ruteru zajednički za skup predajnika, pri čemu su oni dimenzionisani po zahtevu koji je tražio najveće resurse na dotičnom portu. Isto tako, u uzvodnom smeru se šalju Resv poruke kod kojih su zahtevani resursi oglašeni SE pristupom i koji su dimenzionisani po najgorem slučaju (zahtevu koji traži najveće resurse). WF i SE pristup se preporučuju za konferencijske veze u kojima se ne očekuje istovremeno slanje svih predajnika (na primer, telefonska konferencija u kojoj tipično u jednom trenutku priča samo jedan učesnik). FF pristup se preporučuje u slučaju konferencijske veze gde svi (ili većina) predajnici šalju istovremeno podatke u najvećem delu trajanja komunikacije.

RSVP ruter kreira za jednu RSVP sesiju tzv. *path* stanja i *reservation* stanja. *Path* stanje predstavlja zapis o tekućoj RSVP sesiji, a *reservation* stanje predstavlja zapis o tekućoj rezervaciji koju je ruter napravio za dotičnu RSVP sesiju. Ova stanja se održavaju po tzv. *soft* principu, tj. ova stanja su *soft* tipa. *Soft* princip označava da se stanje mora neprekidno osvežavati da bi ostalo aktivno (osvežavanje *path* stanja se vrši periodičnim slanjem Path poruke, a osvežavanje *reservation* stanja periodičnim slanjem Resv poruke). Ako istekne tajmer osvežavanja, stanje se raskida i briše se zapis o njemu u ruteru. Razlog za ovaj pristup leži u načinu slanja RSVP poruka. RSVP poruke se šalju direktno unutar IP datagrama, slično kao ICMP poruke (protokol id unutar IP zaglavlja za RSVP poruke je 46). Pošto se ne koristi pouzdani transportni protokol poput TCP-a, to znači da se RSVP poruke prenose nepouzdano i time nema garancije da bi poruka za raskidanje stigla na odredište čime bi ruter nepotrebno mogao da rezerviše resurse za prijemnik koji je otišao iz sesije. Da bi se takva situacija izbegla uveden je *soft* princip koji prevazilazi navedeni problem nepouzdanog prenosa. I pored upotrebe *soft* principa za održavanje, moguće je i nasilno raskidanje slanjem ResvTear ili PathTear poruke u zavisnosti ko vrši raskidanje - predajna ili prijemna strana (i RSVP ruter može da generiše ove poruke u slučaju da mu istekne tajmer osvežavanja stanja). PathTear poruka putuje u nizvodnom smeru i raskida sva *path* stanja na putu vezana za dotičnu sesiju i sva *reservation* stanja koja su vezana za raskinuta *path* stanja. ResvTear poruka putuje u uzvodnom smeru i raskida sva *reservation* stanja vezana za dotičnu prijemnu stranu tj. koje je prethodno postavila Resv poruka. Preporuka je da se uvek izvrši regularno raskidanje tj. izlazak iz sesije pomoću PathTear/ResvTear poruke da bi se brže obrisala stanja vezana za dotičnu RSVP sesiju u ruterima. Napomenimo i da u slučaju da mreža ne podržava slanje RSVP poruka direktno unutar IP datagrama, RSVP poruke mogu da se enkapsuliraju u UDP pakete (UDP portovi koji se tada koriste su 1698 i 1699).

Napomenimo da se u slučaju uspešne rezervacije šalje poruka ResvConf, ali i dalje stoji napomena da nema garancije da će ta poruka sigurno stići do prijemnika čija se uspešna rezervacija potvrđuje. U slučaju neuspeha u prosleđivanju Path poruke, odnosno Resv poruke ili neuspeha u rezervisanju resursa mogu se poslati RSVP obaveštenja o tim neuspesima/greškama u vidu PathErr ili ResvErr poruka.



Slika 4.4.3. Struktura zaglavlja RSVP poruke i objekta

RSVP poruka se sastoji iz zaglavlja i tela poruke. Telo poruke se sastoji od jednog ili više objekata. Struktura zaglavlja i objekta je prikazana na slici 4.4.3. Zaglavlje se sastoji iz sledećih delova:

- Verzija - Označava verziju RSVP protokola. U RFC 2205 je definisana verzija 1.
- Flegovi - Indikatori. U RFC 2205 nije definisana njihova funkcija.
- Tip poruke - Označava tip RSVP poruke. U RFC 2205 su definisane poruke:
  - Path
  - Resv
  - PathErr
  - ResvErr
  - PathTear
  - ResvTear
  - ResvConf
- RSVP čeksuma - Čeksuma za proveru ispravnosti RSVP poruke sa stanovišta bitskih grešaka. Računa se po istom principu kao IPv4 čeksuma.
- Poslati TTL - U ovo polje je upisana TTL vrednost iz originalno poslatog IP datagrama i koristi se za detekciju rutera koji ne podržavaju RSVP. Ako između dva RSVP rutera postoji takav ne-RSVP ruter doći će do razlike između IP TTL polja i RSVP TTL polja (IP TTL polje će biti manje).
- Rezervisano - Ovi biti su rezervisani za eventualnu buduću upotrebu.
- RSVP dužina - Ovo polje definiše ukupnu dužinu celokupne RSVP poruke (i zaglavlja i tela) u bajtovima.

Objekat se sastoji iz 32-bitnog zaglavlja objekta i sadržaja objekta. Zaglavlje specificira dužinu objekta u bajtovima, pri čemu dužina objekta mora biti celobrojan umnožak 32-bitnih reči. Minimalna dužina objekta je 4 tj. objekat se sastoji samo od zaglavlja. Klasa definiše klasu objekta, a tip definiše tip objekta unutar same klase. Najviša dva bita unutar klase definišu ponašanje rutera u slučaju da ne prepoznaje klasu objekta. Vrednosti 00 i 01 označavaju da se kompletna RSVP poruka odbacuje i generiše se poruka koja nosi obaveštenje o grešci, vrednost 10 označava da se ignoriše dotični objekat i da ga ne prosleđuje dalje (ne generiše se obaveštenje o grešci), vrednost 11 označava da se ignoriše dotični objekat, ali i da se prosleđuje dalje u nemodifikovanom obliku. U slučaju da se prepozna klasa, ali ne i tip objekta unutar te klase, kompletna RSVP poruka se odbacuje i generiše se poruka koja nosi obaveštenje o grešci. Klase objekata definisane u RFC 2205 su (njihova detaljna struktura se može naći u RFC 2205):

- NULL - Prazan objekat čiji se sadržaj ignoriše.
- SESSION - Predstavlja opis RSVP sesije i sadrži odredišnu IP adresu i protokol ID u IP zaglavlju i odredišni transportni port korisničkih paketa.

- RSVP_HOP - IP adresa RSVP rutera (čvora) koji je generisao dotičnu RSVP poruku. Ako je u pitanju nizvodna poruka onda je u pitanju PHOP čvor (*previous hop*), a ako je u pitanju uzvodna poruka onda je u pitanju NHOP čvor (*next hop*).
- TIME_VALUES - Sadrži periodu osvežavanja *path* ili *reservation* stanja (zavisno da li je u pitanju Path ili Resv poruka). Ovaj objekat mora biti prisutan u Resv i Path porukama.
- STYLE - Definiše tip rezervisanja resursa.
- FLOWSPEC - Definiše željeni QoS (nalazi se unutar Resv poruke).
- FILTER_SPEC - Definiše podskup korisničkih paketa sesije koji treba da budu opsluženi QoS kvalitetom zahtevanim u FLOWSPEC objektu Resv poruke.
- SENDER_TEMPLATE - Sadrži IP adresu predajne strane. Ovaj objekat mora da bude prisutan u Path poruci.
- SENDER_TSPEC - Opis karakteristika saobraćaja predajne strane. Ovaj objekat mora da bude prisutan u Path poruci.
- ADSPEC - Sadrži podatke kojima prijemna strana može da proceni kašnjenje s kraja na kraj tako da ove procene može da koristi prilikom kreiranja svojih zahteva za rezervacijom.
- ERROR_SPEC - Predstavlja opis greške unutar PathErr, ResvErr poruke ili potvrdu unutar ResvConf poruke.
- POLICY_DATA - Ovaj objekat nije precizno definisan u RFC 2205 preporuci. Ideja je da se koristi u administratorskom ispitivanju da li je rezervacija moguća ili ne.
- INTEGRITY - Sadrži kriptovane podatke u procesu autentifikacije i verifikacije integriteta RSVP poruke.
- SCOPE - Sadrži eksplicitnu listu predajnika ka kojima RSVP poruka mora da se prosledi. Ovaj objekat se može naći u Resv, ResvErr i Resv Tear porukama.
- RESV_CONFIRM - Sadrži IP adresu prijemne strane koja je zahtevala potvrdu o uspehu rezervacije.

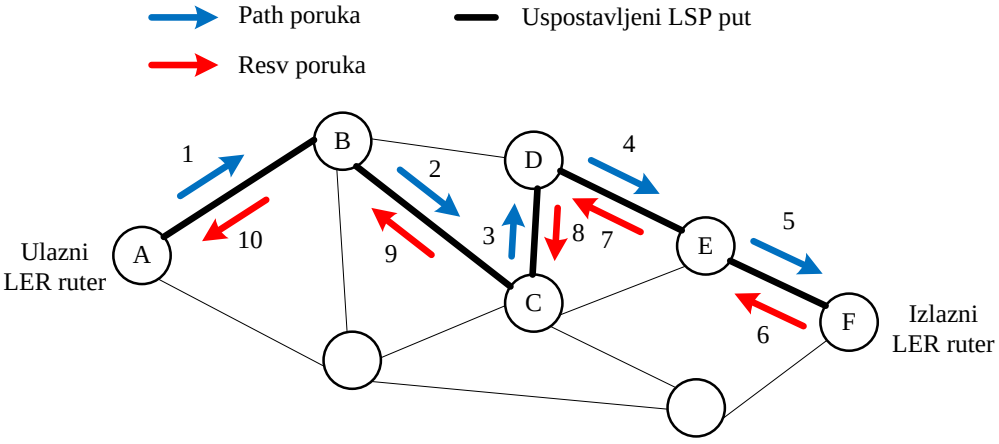
Kao što smo ranije naveli, MPLS ne definiše protokol za distribuciju (oglašavanje) labela već se oslanja na posebne protokole koji će vršiti tu funkciju, pri čemu se u okviru MPLS preporuke predlažu dva načina za kreiranje protokola za distribuciju labela. Prvi način je kreiranje protokola specijalno namenjenog za distribuciju labela, poput LDP protokola. Drugi način je proširenje postojećeg protokola tako da podrži tu funkcionalnost, poput RSVP-TE proširenja RSVP protokola.

RSVP-TE omogućava kreiranje i eksplicitne rute (puta) i hop po hop LSP puta. Zahtevi za labelom i oglašavanje mapiranja labela se integrišu u vidu novodefinisanih klasa objekata unutar RSVP poruka. Skup RSVP poruka je nepromenjen, ali su definisani novi objekti (preciznije nove klase) koji omogućavaju oglašavanje labela, tj. uspostavu LSP puta. RSVP-TE uvodi klase objekata (detaljna struktura ovih klasa se može naći u RFC 3209):

- LABEL_REQUEST(koristi se u Path poruci)
- LABEL (koristi se u Resv poruci)
- EXPLICIT_ROUTE (koristi se u Path poruci)
- RECORD_ROUTE (koristi se u Path i Resv porukama)
- SESSION_ATTRIBUTE (koristi se u Path poruci)

Takođe, u okviru klasa SESSION, SENDER_TEMPLATE i FILTER_SPEC su definisani novi tipovi za podršku LSP putevima. U sve tri klase su definisani tipovi koji reprezentuju ID LSP puta čime je olakšana podrška za LSP puteve tj. njihovo postavljanje i ažuriranje.

U slučaju kada se želi uspostaviti LSP put, LABEL_REQUEST i LABEL klase su obavezne. LABEL klasa predstavlja labelu koja se oglašava i ona se nalazi u okviru Resv poruke, što je i logično jer se labela oglašava u uzvodnom smeru. LABEL_REQUEST klasa predstavlja zahtev za labelom i smešta se u okviru Path poruke, što je takođe logično jer se zahtev šalje u nizvodnom smeru. Takođe, iz ovoga se može zaključiti da se koristi mehanizam oglašavanja u uzvodnom smeru na zahtev. Postoje tri tipa objekta LABEL_REQUEST klase - tip za ATM linkove, tip za FR linkove i tip za ostale linkove (generička labela). Ako se želi koristiti eksplicitna ruta za LSP put onda se mora koristiti i EXPLICIT_ROUTE klasa unutar Path poruke, u suprotnom će biti kreirana LSP putanja na osnovu hop po hop rutiranja. Pri tome, u slučaju eksplicitnog puta podržani su i striktni i labavi eksplicitni put. U okviru objekta EXPLICIT_ROUTE klase se navode čvorovi (ruteri) eksplicitne rute u redosledu pojavljivanja na ruti, pri čemu se navodi IPv4 prefiks ili IPv6 prefiks ili AS broj (uz svaki čvor je definisan L bit koji određuje da li je u pitanju striktna ili labava deonica puta). RECORD_ROUTE klasa se koristi za snimanje puta Path ili Resv poruke jer svaki posredni RSVP čvor dopisuje sebe u listu čvorova kroz koje se prošlo. Ova klasa se može koristiti za detekciju petlji, za definisanje eksplicitnog puta, korisnu informaciju prijemnoj ili predajnoj strani o putu koji se koristi. SESSION_ATTRIBUTE omogućava definisanje prioriteta uspostave i prioriteta zadržavanja koje smo već objasnili u okviru CR-LDP protokola. Takođe, u okviru ove klase se mogu postaviti filtri koji utvrđuju da li su neki kandidati za deonicu LSP puta prihvatljivi ili ne. Kada se kreira LSP put, on se može kreirati i sa QoS podrškom i bez QoS podrške. U okviru RSVP-TE nije dozvoljeno koristiti WF pristup u rezervaciji resursa.



Slika 4.4.4. Uspostava LSP puta pomoću RSVP-TE

Princip formiranja LSP puta pomoću RSVP-TE je veoma jednostavan i prikazan je na slici 4.4.4. Path poruka u sebi nosi LABEL_REQUEST klasu objekta koja predstavlja zahtev za mapiranjem labele od nizvodnog RSVP rutera. Ulazni LER ruter kreira Path poruku i šalje je sledećem RSVP ruteru u nizu koga bira ili po hop po hop principu ili kao prvog u nizu eksplicitne rute. LSR ruteri na putu do izlaznog LER rutera takođe kreiraju Path poruke koje u sebi sadrže zahtev za mapiranjem labele. Kada Path poruka stigne do izlaznog LER rutera, on će izvršiti mapiranje labele i poslaće uzvodno to mapiranje unutar Resv poruke u vidu klase objekta LABEL. Na sličan način, svaki LSR ruter na uzvodnom putu će kreirati Resv poruku sa svojim mapiranjem labele. Kada Resv poruka sa mapiranom labelom stigne do ulaznog LER rutera, LSP put kroz MPLS domen je kreiran. Ukoliko se zahteva i određeni QoS nivo kvaliteta, odgovarajući resursi u LSR ruterima na putu će biti rezervisani za dotični LSP put.

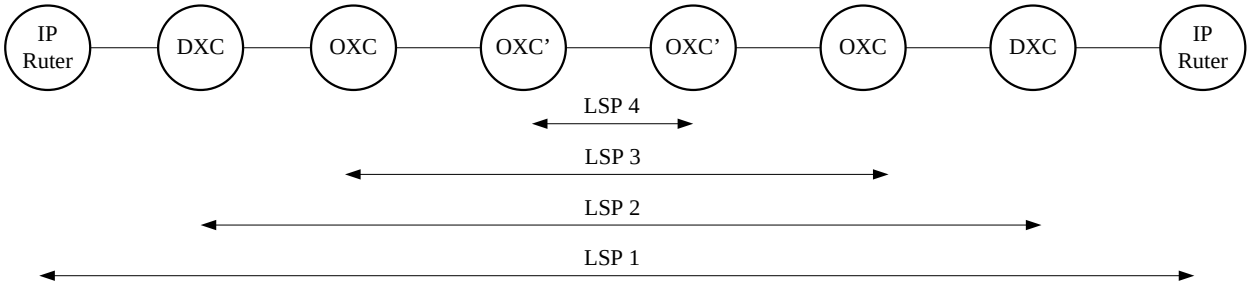
4.5. GMPLS

GMPLS predstavlja proširenje MPLS arhitekture, pri čemu je osnovni okvir GMPLS arhitekture definisan u RFC 3945. MPLS arhitektura je namenjena mrežama baziranim na paketskoj komutaciji, što je i logično jer je MPLS prvenstveno bio namenjen IP mrežama, pri čemu je bio podržan i rad sa ATM, FR i Eternet tehnologijama koje su takođe bazirane na paketskoj komutaciji. Međutim, pored paketski orijentisanih mreža postoji i niz drugih mreža koje su zasnovane na drugačijim principima i koje se tipično koriste kao transportne mreže čije usluge koriste i same IP mreže. Stoga je bilo potrebno omogućiti i rad sa labelama (usmeravanje na bazi labela) i u drugim tipovima mreže. Otuda GMPLS proširuje MPLS arhitekturu podrškom za rad sa TDM mrežama (poput SDH) i sa optičkim mrežama (u suštini i SDH mreže su u fizičkom delu optičke jer koriste optičke linkove u najvećoj meri, ali se komutacija radi u električnom domenu i zasnovana je na TDM principima), pri čemu je u optičkim mrežama podržana i komutacija na nivou talasnih dužina i grupe talasnih dužina, kao i komutacija na nivou fizičkih optičkih portova. Stoga, GMPLS omogućava uspostavu LSP puta i kroz TDM mreže, a takođe i kroz optičke mreže, što znači da GMPLS omogućava konfigurisanje TDM i optičkih svičeva (na primer, u SDH mreži DXC ima ulogu digitalnog (TDM) sviča, a u OTN mreži OXC ima ulogu optičkog sviča).

GMPLS definiše sledeće tipove interfejsa GMPLS LSR čvora koji su navedeni redosledom po nivou hijerarhije od najnižeg nivoa do najvišeg nivoa (hijerarhija sa stanovišta prosleđivanja na bazi labela):

- PSC (*Packet-Switch Capable*) interfejsi - Hijerarhijski najniži nivo hijerarhije. Interfejs preko koga se primaju paketi, poput IP paketa, ATM ćelija, FR okvira, eternet okvira. Praktično ovo je jedini interfejs koji je definisan u MPLS arhitekturi, svi preostali interfejsi su deo GMPLS proširenja.
- TDM (*Time-Division Multiplex capable*) interfejsi - Interfejsi koji vrše prosleđivanje na bazi TDM principa. SDH interfejs pripada ovom tipu.
- LSC (*Lambda-Switch Capable*) interfejsi - Vrše prosleđivanje sa jedne talasne dužine (sa ulaznog interfejsa) na drugu talasnu dužinu (na izlaznom interfejsu). Interfejsi OXC sviča pripadaju ovom tipu.

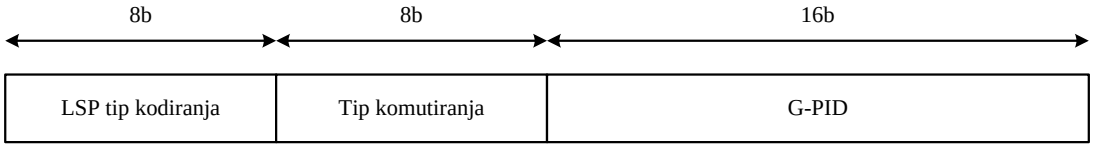
- FSC (*Fiber-Switch Capable*) interfejsi - Hijerarhijski najviši nivo hijerarhije. Interfejsi koji prosleđuju podatke sa jednog (ili više) ulaznog optičkog vlakna na jedno (ili više) izlazno optičko vlakno. Interfejsi OXC sviča koji omogućava optičku komutaciju između više optičkih vlakana spadaju u ovu kategoriju (komutacija nije na osnovu talasne dužine, već na osnovu fizičke lokacije porta).



Slika 4.5.1. Hijerarhije interfejsa u GMPLS

Primer hijerarhijskog odnosa navedenih interfejsa je prikazan na slici 4.5.1. Za sve prikazane čvorove u primeru sa slike 4.5.1 se podrazumeva da podržavaju GMPLS. IP ruter predstavlja ulaz u GMPLS paketski domen gde se formira LSP put 1 koji ide između prikazanih IP rutera. Stoga IP ruter na ulazu u GMPLS domen dodaje labelu na paket (labela nivoa 1). Zatim paket sa labelom nivoa 1 pristiže u DXC uređaj koji, na primer, predstavlja ulaz u SDH mrežu, odnosno u novi GMPLS domen. U okviru ove SDH mreže se formira LSP put 2. Ulazni DXC uređaj ubacuje paket u odgovarajuću TDM strukturu (virtuelni kontejner) koji je dodeljen toku, odnosno LSP putu 2. Napomenimo da se labela nivoa 2 ne dodaje na sam paket, kao što će biti kasnije objašnjeno. OXC prima TDM strukturu (neki od STM-N okvira) i komutira je na jednu od talasnih dužina izlaznog optičkog vlakna, pri čemu je prethodno kreirao LSP put 3. OXC na ulazu ’dodaje’ labelu nivoa 3 (ni ova labela se ne dodaje na same pakete). OXC’ uređaj omogućava komutaciju na nivou više optičkih vlakana, tj. komutira signale između vlakana, pa stoga predstavlja ulaz u novi (hijerarhijski viši) GMPLS domen kroz koji je formiran LSP 4 put. OXC’ na ulazu ’dodaje’ stoga labelu nivoa 4 (ni ova labela se ne dodaje na same pakete). Oznaka OXC’ je korišćena u ovom primeru samo da označi proširene mogućnosti u odnosu na uređaj OXC iz primera (oba uređaja pripadaju klasi OXC uređaja samo različitim skupovima mogućnosti). Nakon toga se u obrnutom redosledu prolaze opisani uređaji i vrše se izlazi iz odgovarajućih GMPLS domena, pri čemu se na svakom izlazu ’skida’ odgovarajuća labela, odnosno terminira odgovarajući LSP put. Na ovaj način se veoma jednostavno može uspostaviti LSP put čak i u slučaju kada put prolazi kroz veoma raznorodne mreže. Treba primetiti da su u suštini LSP putevi tunelovani prilikom prolaska kroz mrežu druge tehnologije (tj. tipa interfejsa) što je i logično jer su ove tehnologije prilično raznorodne da bi funkcionisale po principu steka labela kao MPLS mreže. Ono što je bitno naglasiti jeste da postoji razlika u prenosu labela. Naime, u paketskim mrežama je logično da se labela smesti negde u zaglavlju paketa. Ali u TDM i optičkim mrežama to nije praktično jer te mreže ne vrše procesiranje na nivou korisničkih paketa jer to nisu paketske mreže. Stoga se kod njih labela prenosi van samih korisničkih podataka tj. praktično labela podrazumeva konfiguraciju komutacionih elemenata (TDM i/ili optičkih). Slično važi i za protokole za distribuciju (oglašavanje) labela. U paketskim mrežama se kontrolne (signalizacione) informacije razmenjuju istim putem kao i korisnički paketi, ali to nije slučaj sa TDM i optičkim mrežama gde takve informacije tipično ne idu istim putem kao korisnički podaci (iz istih razloga navedenih za slučaj labela). Na primer, u TDM mrežama se za kontrolne/signalizacione informacije može koristiti jedan zaseban TDM kanal, ili u optičkim

mrežama se može koristiti zasebna talasna dužina i sl. Ovaj pristup gde signalizacija ne ide istim putem kao korisnički podaci se naziva signalizacija van opsega, a u paketskim mrežama se koristi signalizacija u opsegu jer signalizacija ide istim putem kao i korisnički podaci. Očigledno, GMPLS je morao da podrži ovakve specifičnosti u razlikama između paketskih i TDM, odnosno optičkih mreža. Takođe, GMPLS LSP put uopšte ne mora ni da prolazi kroz paketsku mrežu, već može biti definisan samo na nivou TDM mreže ili samo na nivou optičke mreže ili kombinacije TDM i optičkih mreža. Isto tako, GMPLS labele nisu hijerarhijske kao kod MPLS arhitekture u smislu da mogu da kreiraju stek labela. Na primer, ako imamo unutar neke SDH mreže jednog operatera, SDH segment nekog drugog operatera kroz koji prolazi LSP put 1 koji počinje i završava u SDH mreži prvog operatera, tada se u segmentu SDH drugog operatera formira LSP 2 put kroz koji se tuneluje LSP 1 put. Naizgled, ovo je veoma slično MPLS arhitekturi, ali razlika je što sada ne postoji stek labela što je i logično ako se ima u vidu razlika u prirodi prenosa i uloge labela u komutaciji između nepaketskih i paketskih mreža.



Slika 4.5.2. Zahtev za generalizovanom labelom

Pošto u GMPLS ima više tipova interfejsa, a takođe i podaci mogu da se prenose na različit način preko istog fizičkog puta (na primer, u SDH mreži se mogu prenositi generički okviri, ATM ćelije, i dr.), uređaji se moraju dogovoriti ne samo oko vrednosti labela, već i oko svojih karakteristika, kao i tipa saobraćaja. Otuda je definisan tzv. zahtev za generalizovanom labelom prikazan na slici 4.5.2. Ovaj zahtev se sastoji iz tri dela:

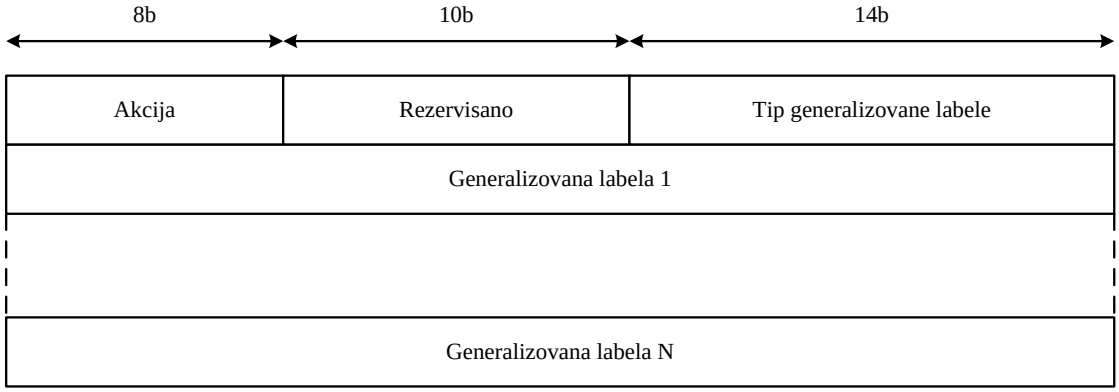
- LSP tip kodiranja (*LSP Encoding Type*) - Definiše kako će podaci koji se prenose biti kodirani. Na primer, neki od definisanih tipova su paket (vrednost 1), ethernet II (vrednost 2), eternet 802.3 (vrednost 10), optički kanal (vrednost 11), optičko vlakno (vrednost 9), itd.
- Tip komutiranja (*Switching Type*) - Definiše tip komutiranja koji će se koristiti. Ovo polje se koristi u slučaju kada je na raspolaganju više načina komutiranja.
- Generalizovani identifikator korisnog saobraćaja (*G-PID - Generalized Payload ID*) - Ovo polje identifikuje tip korisnog saobraćaja koji se prenosi preko LSP puta, pri čemu je vrednost ovog polja bitna samo za krajnje tačke LSP puta što je i logično jer sve LSR tačke na LSP putu će vršiti samo usmeravanje tj. komutiranje bez ispitivanja tipa korisničkog saobraćaja. Na primer, ako se na krajnjim tačkama LSP puta nalazi PE uređaji SDH mreže, onda je samo njima bitno da znaju tip korisničkog saobraćaja jer oni ga moraju pakovati u virtuelne kontejnere na početku LSP puta, odnosno vaditi iz virtuelnog kontejnera na kraju LSP puta. Neke od definisanih vrednosti G-PID su ATM mapiranje u SDH mrežama (TDM interfejs) (vrednost 32), eternet saobraćaj na optičkim linkovima koji podržavaju komutaciju na nivou talasnih dužina ili na nivou optičkih vlakana (LSC, FSC interfejsi) (vrednost 33), SDH saobraćaj na optičkim linkovima koji podržavaju komutaciju na nivou talasnih dužina ili na nivou optičkih vlakana (LSC, FSC interfejsi) (vrednost 34), itd.

GMPLS labela je modifikovana u odnosu na MPLS labelu. Razlog je što se labela može prenositi i van opsega (TDM i optičke mreže) i unutar opsega (paketske mreže) u zavisnosti od same tehnologije. Stoga GMPLS labela, koja se naziva i generalizovana labela, može da predstavlja:

- Generička MPLS labela, ATM labela, FR labela (paketske mreže)
- Skup vremenskih slotova u SDH strukturama, odnosno preciznije bi bilo reći skup virtuelnih kontejnera u SDH strukturama (TDM mreže)
- Jednu talasnu dužinu u skupu talasnih dužina (*waveband*) ili u optičkom vlaknu
- Jedan skup talasnih dužina (*waveband*) u optičkom vlaknu
- Jedno optičko vlakno u skupu (*bundle*) optičkih vlakana

Struktura generalizovane labele zavisi od tipa interfejsa preko koga se razmenjuje generalizovana labela i nju uređaj određuje na osnovu svog tipa interfejsa, pa se otuda u generalizovanoj labeli ne nalazi informacija o tipu interfejsa.

Pošto u nekim tehnologijama uspostava veze traje nezanemarljivo vreme usled nešto većeg vremena potrebnog za konfigurisanje komutatora neophodno je unaprediti proces uspostave LSP puta u odnosu na princip korišćen u paketskim mrežama. Ako bi se koristio princip iz paketskih mreža, LSR čvor bi smeo da izvrši konfiguraciju tek kad primi informaciju o labeli od svog nizvodnog suseda, a pošto se u nepaketskim mrežama koristi princip oglašavanja uzvodno na zahtev to bi trošilo previše vremena jer bi zahtev morao da putuje do izlaznog LER čvora, a tek onda bi se labele počele slati uzvodno i ako se uzme u obzir relativno duže vreme konfigurisanja, uspostava LSP puta bi trajala isuviše dugo. Otuda se koristi princip preporučenih labela. LSR čvor koji šalje zahtev za labelom, unutar zahteva stavlja i preporučenu vrednost labele. Istovremeno LSR čvor izvršava konfiguraciju komutatora prema preporučenoj labeli jer očekuje da će od nizvodnog suseda dobiti tu labelu. Otuda, kada od izlaznog LER čvora krene proces oglašavanja labela, LSR čvorovi će već imati izvršene konfiguracije čime će LSP put znatno brže da se uspostavi. Naravno, ako iz nekog razloga nizvodni sused ne oglasi preporučenu labelu, već neku drugu, LSR čvor će ponovo morati da izvrši konfigurisanje komutatora što će usporiti uspostavu LSP puta.



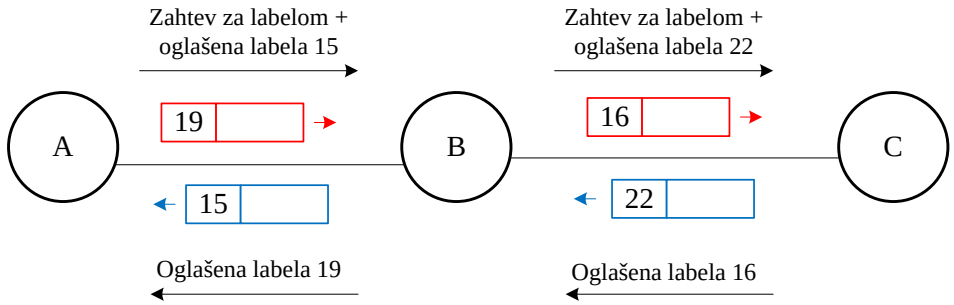
Slika 4.5.3. Skup labela

Takođe, LSR čvor može u zahtevu da definiše i skup labela kojim može ograničiti izbor labele nizvodnog suseda. Ova opcija je zgodna u slučaju kada optički uređaj ne može na primer

da vrši konverziju talasnih dužina pa LSP put mora da zadrži istu talasnu dužinu na izlazu dotičnog uređaja. Takođe, ovim mehanizmom može da se smanji ukupan broj konverzija talasnih dužina na LSP putu kroz optičku mrežu. Struktura definisanja skupa labela je prikazana na slici 4.5.3. Polje akcija definiše način definisanja skupa:

- Lista dozvoljenih labela (polje akcije = 0) - U poljima labela 1 - labela *N* se nalaze labele koji predstavljaju članove liste labela iz kojih nizvodni sused treba da izabere jednu.
- Lista nedozvoljenih labela (polje akcije = 1) - U poljima labela 1 - labela *N* se nalaze labele koji predstavljaju članove liste labela iz kojih nizvodni sused ne sme da izabere labelu koju će oglasiti na poslati zahtev koji sadrži ovu listu.
- Opseg dozvoljenih labela (polje akcije = 2) - U poljima labela 1 - labela *N* se nalazi početak i kraj opsega labela iz kojeg nizvodni sused treba da izabere jednu. Očigledno, u ovom slučaju je *N*=2.
- Opseg nedozvoljenih labela (polje akcije = 3) - U poljima labela 1 - labela *N* se nalazi početak i kraj opsega labela iz kojeg nizvodni sused ne sme da izabere labelu koju će oglasiti na poslati zahtev koji sadrži ovaj opseg. Očigledno, u ovom slučaju je *N*=2.

Polje tip generalizovane labele definiše način kodiranja tj. strukturu generalizovanih labela, dok polje generalizovane labele *i* (*i*=1..*N*) predstavlja generalizovanu labelu. Polje generalizovane labele *i* se označava još i kao potkanal *i* (*sub-channel i*).



Slika 4.5.4. Uspostava bidirekcionog puta

MPLS uspostavlja unidirekcione LSP puteve, pa je za bidirekcione puteve je neophodno izvršiti dve uspostave, po jednu za svaki smer. GMPLS dodaje podršku za kreiranje bidirekcionih puteva. Bidirekcioni LSP putevi se uspostavljaju malom modifikacijom postavljanja unidirekcionih LSP puteva. Naime, u okviru zahteva za labelom poslatom nizvodnom susedu se nalazi i oglašena labela za suprotan smer puta. Na taj način se istovremeno uspostavljaju oba smera puta, kao što je prikazano na slici 4.5.4. U primeru sa slike, čvor A šalje zahtev za labelom u okviru koga oglašava labelu 15 za uzvodni LSP smer. Čvor B potom šalje zahtev za labelom u kom oglašava labelu 22 za uzvodni LSP smer. Ruter C potom oglašava labelu 16, i potom i ruter B oglašava labelu 19. Crvenom bojom su prikazani korisnički paketi u nizvodnom smeru LSP puta, a plavom bojom korisnički paketi u uzvodnom smeru LSP puta.

GMPLS podržava i definisanje tipa zaštite na linku LSP puta koja može biti 1:1, 1+1, 1:N, unapređena (na primer, na nivou bidirekcionog prstena od četiri vlakna), a takođe zaštita se ne mora koristiti (*unprotected* tip zaštite). Pošto se u nekim zaštitama koriste u suštini dva LSP

puta (primarni i sekundarni), GMPLS omogućava identifikaciju koji LSP put je primarni (radni), a koji sekundarni (zaštitni). Očigledno, GMPLS koristi mogućnosti zaštite koju nude TDM i optičke mreže, a koje smo opisali u prethodnim poglavljima. S obzirom na specifičnosti pojedinih mrežnih tehnologija obuhvaćenih GMPLS arhitekturom, definisan je LMP (*Link Management Protocol*) koji omogućava verifikaciju povezanosti između susednih uređaja, kao i detekciju i lociranje grešaka i obaveštavanje o njima. Može se zaključiti na osnovu navedenih LMP funkcionalnosti da su one veoma slične funkcionalnostima transportnih mreža opisanih u prethodnim poglavljima.

GMPLS takođe, kao i MPLS, ne definiše same protokole za oglašavanje labela ili protokole rutiranja već se oni definišu zasebno ili se proširuju postojeći protokoli. Otuda su, na primer, za OSPF i IS-IS protokole rutiranja definisana proširenja koja podržavaju GMPLS. CR-LDP i RSVP-TE su takođe prošireni podrškom za GMPLS. CR-LDP je proširen parametrima: zahtev za generalizovanom labelom, generalizovana labela i skup labela. Slično, RSVP-TE je proširen klasama objekata: zahtev za generalizovanom labelom, generalizovana labela i skup labela.