Univerza v Ljubljani
Fakulteta za elektrotehniko

PODIPLOMSKI ŠTUDIJ
MAGISTRSKO DELO

Navidezna zasebna omrežja na osnovi protokola MPLS

ŠTUDENT: Uroš Hacin
MENTOR: Prof. dr. Sašo Tomažič

Ljubljana, Januar 2010

ZAHVALA

Za nastanek naloge se zahvaljujem mentorju profesorju dr. Sašu Tomažiču za pomoč in predvsem za njegov čas, ki ga je namenil izdelavi moje magistrske naloge.

Prav tako se zahvaljujem podjetju Smart Com d.o.o., ki mi je študij odobrilo in podpiralo ves čas študija.

Zahvaljujem se tudi staršema za moralno podporo in moji novo nastali družini, ki me je podpirala ves čas študija predvsem takrat, ko sem se zaprl v računalniško sobo in tam prebil veliko časa.

KAZALO

SEZNAM SLIK

SEZNAM TABEL

KRATICE

KRATICA - ANGLEŠKO	
ATM	asynchronous transfer mode (asinhroni prenosni način)
ABR	area border router (področni mejni usmerjevalnik)
BGP	border gateway protocol (protokol obrobnega prehoda)
BGP4	BGP version 4 (četrta verzija protokola obrobnega prehoda)
CE	customer edge (robna naprava stranke)
CoS	class of service (kvaliteta storitve)
CR-LDP	constraint based LDP (protokol za distribucijo label z upoštevanjem omejitev)
CPE	customer premises equipment (oprema pri stranki)
DOS	denial of service (zavrnitev storitve)
DLCI	data link connection identifier (identifikator zveze v sloju podatkovne povezave)
EAPS	ethernet automatic protection switching (avtomatično zaščitno preklapljanje v ethernet omrežjih)
EIGRP	enhanced interior gateway routing protocol (Izboljšan protokol za izmenjavo usmerjevalnih informacij v okviru domen)
EBGP	external BGP (zunanji BGP)
EXP	experimental (eksperimentalno)
ERO	explicit route object (objekt eksplicitne smeri)
FEC	forwarding equivalence class (ekvivalentni posredovalni razred)
GRE	generic routing encapsulation (generično ovijanje pri usmerjanju)
GRES	graceful restart (postopni ponovni zagon)
IBGP	internal BGP (interni BGP)
IETF	internet engineering task force (delovna skupina za internetsko inženirstvo)
IS-IS	Intermediate system to intermediate system (vmesni sistem do vmesnega sistema)
IXIA	testing device (preizkusna naprava)
IXOS	IXIA operating system (operacijski sistem preizkusne naprave IXIA)
ISP	internet service provider (ponudnik internetnih storitev)
IP	internet protocol (internetni protokol)
IGP	interior gateway protocol (protokol notranjih usmerjevalnikov)
IPv4	IP version 4 (internetni protokol verzije 4)
IPTv	IP television (televizija preko internetnega protokola)
IPSeC	IP security (varnost v internetnem protokolu)
L2TP	layer 2 tunneling protocol (protokol za tuneliranje v drugem sloju OSI)
LAN	local area network (lokalno omrežje)

LDP	label distribution protocol (protokol za distribucijo label)
LSR	label switched router (labelno komutirani usmerjevalnik)
LSP	label switched path (labelno komutirana pot)
LSA	link state advertisement (obvestilo o stanju povezave)
L3VPN	layer 3 VPN (VPN v tretjem sloju)
MPLS	multi protocol label switching (več protokolna komutacija z zamenjavo label)
MP-BGP	multiprotocol BGP (večprotokolni BGP)
MPLSCP	MPLS control protocol (kontrolni protokol pri protokolu MPLS)
MD5	message digest 5 (izvleček sporočila 5)
MTU	maximum transmission unit (največja prenosna enota)
NG-MVPN	next generation multicast VPN (VPN z oddajanjem več prejemnikom naslednje generacije)
OSI	open system interconnection (medsebojno povezovanje odprtih sistemov)
OSPF	open shortest path first (prva najkrajša prosta pot)
P	provider (ponudnik)
PE	provider edge (ponudnikov rob)
PPP	point to point protocol (protokol točka-točka)
POP	point of presence (točka prisotnosti)
PHP	penultimate hop popping (odstranitev labele na predzadnjem skoku)
PIM	protocol independent multicast (oddajanje več prejemnikom neodvisno od protokola)
PIM-SM	PIM sparse mode (raztreseni način oddajanja več prejemnikom)
PIM-DM	PIM dense mode (zgoščeni način oddajanja več prejemnikom)
PIM-SSM	PIM source specific multicast (Oddajanje več prejemnikom s točno določenim virom)
PPTP	point to point tunnel (tunelski protokol točka-točka)
PDU	protocol data unit (protokolna podatkovna enota)
RP	rendezvous point (točka razvejitve)
RSVP	resource reservation protocol (protokol z rezervacijo virov)
RIB	routing information base (baza usmerjevalnih informacij)
RIP	routing information protocol (protokol usmerjevalnih informacij)
RIPE	Regional Internet Registry for Europe (Evropski omrežni koordinacijski center IP register)
RID	router id (identifikator usmerjevalnika)
RRO	record route object (objekt zapisa smeri)
SM	sparse mode (raztreseni način)

SNAP	Sub network Access Point (dostopovna točka podomrežja)
S bit	stack bit (biti za sklad label)
SDH	synchronous digital hierarchy (sinhrona digitalna hierarhija)
TTL	time to live (življenjska doba)
TCP	transport control protocol (protokol za krmiljenje transporta)
TLV	type length value (tip - dolžina – vrednost)
UDP	user datagram protocol (uporabnikov datagramski protokol)
UHP	ultimate hop popping (odstranitev na zadnjem skoku)
VPI	virtual path identifier (identifikator navidezne poti)
VCI	virtual circuit identifier (identifikator navideznega kanala)
VRF	virtual routing and forwarding (usmerjevalna in posredovalna tabela VPN)
VPN	virtual private network (navidezno zasebno omrežje)
VPLS	virtual private LAN service (storitev navideznega zasebnega LAN omrežja)
VLAN	virtual LAN (navidezni LAN)

1. Povzetek

Omrežja ponudnikov storitev sestavljajo usmerjevalniki in stikala, ki delujejo na osnovi protokola IP (Internet Protocol). Ponudniki storitev si v največji meri prizadevajo izkoristiti svoje omrežje in nuditi največ storitev svojim naročnikom. Primeri takšnih storitev so virtualna privatna omrežja, ki delujejo na osnovi protokola MPLS.

V omrežjih ponudnikov storitev izvajajo osnovne usmerjevalne funkcije usmerjevalni protokoli OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System) ter BGP (Border Gateway Protocol). Protokol OSPF skrbi za dosegljivost povezav med usmerjevalniki in vmesnikov povratnih povezav (Loopback Interface). Po protokolu BGP se prenašajo smeri naročnikov, ki so priklopljeni na ponudnika internetnih storitev ISP (Internet Service Provider). Za potrebe prenosa video vsebin je v omrežjih ponudnikov storitev izveden tudi protokol PIM (Protocol Independent Multicast).

Ponudniki internetnih storitev so v zadnjih letih v svoja omrežja vključili tudi protokol MPLS (Multiprotocol Label Switching), ki zagotavlja dodatne funkcionalnosti, kot je to npr. prometni inženiring, ki omogoča preusmerjanje prometnih tokov po želenih poteh v omrežju.

Protokol MPLS je razdeljen v dva sloja: signalizacijski in podatkovni. Signalizacijska protokola pri protokolu MPLS sta dva: RSVP (Resource Reservation Protocol) in LDP (Label Distribution Protocol). Oba omogočata vzpostavljanje poti LSP (Label Switched Path). Ko se poti vzpostavijo, se jih uvrsti v podatkovni sloj, nato se preko njih posreduje IP pakete.

Trend v razvoju omrežij ponudnikov internetnih storitev je ponudba virtualnih privatnih omrežij VPN (Virtual Private Network) na osnovi protokola MPLS. Obstajata dva tipa storitev VPN in sicer prvi, ki deluje na osnovi protokolov BGP in MPLS, ter drugi, ki deluje samo na osnovi protokola MPLS.

Storitev VPN, ki delujejo na osnovi protokolov MPLS in BGP je več:

- L2VPN (Layer 2 Virtual Private Network),
- VPLS (Virtual Private Lan Service) ter
- L3VPN (Layer 3 Virtual Private Network).

V temeljih se storitve VPN razlikujejo po sloju OSI (Open System Interconnection) v katerem delujejo. Storitvi L2VPN ter VPLS delujeta v drugem sloju OSI, storitev L3VPN deluje v tretjem sloju OSI. Trenutno je najbolj uveljavljena storitev L3VP, ponudniki internetnih storitev pa tudi širijo ponudbo z novo storitvijo VPLS.

Največ izzivov pri storitvah VPN prinaša hkratna oddaja več uporabnikom MVPN (Multicast Virtual Private Network). Omejitve se pokažejo pri skaliranju te rešitve, ker se trenutno v kontrolnem sloju uporablja protokol PIM. Ta protokol za svoje delovanje zahteva vzpostavitev PIM sej za vsak nov MVPN med vsemi robnimi usmerjevalniki, ki sodelujejo pri tej storitvi. To pa predstavlja veliko število sej, ki jih morajo usmerjevalniki vzdrževati v odprtem stanju. Trend razvoja storitve MVPN je v uvajanju protokola BGP v kontrolno ravnino. Ta bi nadomestil protokol PIM. Nova storitev s protokolom BGP se bo imenovala NG-MVPN (Next Generation Multicast Virtual Private Network).

Kot praktični primer storitve VPN so v delu opisani konfiguracija in rezultati meritve storitve L3VPN, ki je bila vzpostavljena v delujočem omrežju pri ponudniku storitev.

Abstract

ISP's (Internet service provider) networks are built with routers and switches that work on the basis of IP protocol. Internet service providers are willing to offer as much as possible services on their network. One example of those services is VPN (Virtual Private Network) that uses protocol MPLS.

Basic routing in ISP's networks is done by routing protocols: OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System) and BGP (Border Gateway Protocol). OSPF is responsible for interconnection between routers. Protocol BGP carries information of customer networks within ISP's network and beyond it towards other ISP's. ISP's have implemented protocol PIM for carrying video traffic.

ISP's are looking for new services that they could offer and that is the reason why MPLS protocol is being implemented into networks. Protocol MPLS also brings out new features like traffic engineering.

MPLS protocol is divided into control and data layer. Two control protocols work in signalization layer: RSVP (Resource Reservation Protocol) and LDP (Label Distribution Protocol). Both protocols are responsible for establishment of LSP (Label Switched Path) paths. After the LSP have been established, it is placed into the data layer and traffic starts to go through it.

New trend in ISP networks is to offer new services on the basis of protocol MPLS. There are two types VPN's that exist now. The first type of VPN works on the basis of two protocols: BGP and MPLS. The second type of VPN works only on the basis of MPLS protocol.

There are several VPN's that work on the basis of BGP and MPLS protocols:

- L2VPN (Layer 2 Virtual Private Network),
- VPLS (Virtual Private Lan Service) and
- L3VPN (Layer 3 Virtual Private Network).

All three VPN's work on different OSI layers (Open System Interconnection). L2VPN and VPLS work on the second OSI layer, L3VPN works on the third OSI layer. Currently L3VPN is the most widespread service. ISP's are introducing new service VPLS.

The most challenging is support for multicast traffic in MVPN (Multicast Virtual Private Network). Scalability is the biggest issue, because PIM (Protocol Independent Multicast) protocol is currently being used in control layer. PIM establishes sessions between all edge routers for every MVPN service, which means a lot of opened sessions that routers need to manage. Future trend of development for this service is in using BGP protocol instead of PIM. New service on the basis of BGP protocol will be named NG-MVPN (Next Generation – Multicast Virtual Private Network).

As a practical example in this theme L3VPN was established in the real network and some measurements were done in this service.

2. Uvod

V omrežjih, ki delujejo na osnovi protokola IP, potuje paket med usmerjevalniki nepovezavno (connectionless). Vsak usmerjevalnik se sam odloča o nadaljnjem usmerjanju IP paketov skozi omrežje. V ta namen vsak usmerjevalnik izvede usmerjevalni algoritem za izračun najboljše poti do cilja. Obstaja več usmerjevalnih protokolov: OSPF, IS-IS, RIP (routing information protocol) in EIGRP (enhanced interior gateway routing protocol). Del teh usmerjevalnih protokolov so algoritmi za izračun najboljše poti. Omenjeni protokoli ne omogočajo ustreznega prometnega inženiringa. V ta namen so pri IEEE (Institute of Electrical and Electronics Engineers) standardizirali nov usmerjevalni protokol MPLS.

Protokol MPLS deluje med drugim in tretjim slojem OSI in je povezavno orientiran. Omrežja, kjer je izveden MPLS, se imenujejo IP/MPLS omrežja. Protokol MPLS je razdeljen v dva sloja: kontrolni in podatkovni.

V kontrolnem sloju delujeta signalizacijska protokola LDP (Label Distribution Protocol) ter RSVP (Resource Reservation Protocol). Protokola omogočata avtomatično vzpostavljanje poti LSP. Poleg tega pa obstaja še možnost statičnega določanja poti LSP. Pri tem načinu vzpostavljanja poti se določi usmerjevalnike, preko katerih bo potekala pot.

Protokol LDP je enostavnejši od protokola RSVP, vendar omogoča manj funkcionalnosti, ko je npr. statično usmerjanje IP prometnih tokov skozi vnaprej določene usmerjevalnike.

Protokol LDP za ustvarjanje povezav s sosedi in prenos informacij uporablja sporočila, ki se prenašajo med usmerjevalniki. V protokolu LDP obstaja avtomatsko zaznavanje sosednjih usmerjevalnikov s pomočjo pozdravnih sporočil (hello message). Uporabljajo se še drugi tipi sporočil, kot npr. naslovno sporočilo, sporočilo za umik naslova, labelno povezovalno sporočilo in še druga. Za vzpostavljanje povezav s sosedi je predvidena avtentikacija sporočil (authentication).

Zaradi različnih potreb po preusmerjanju IP paketov je bilo v omrežjih omogočeno omejevanje usmerjanja po poteh LSP. Pot LSP je mogoče filtrirati na vhodu ali na izhodu iz omrežja. Protokol LDP omogoča tudi deljenje IP prometa med različne poti LSP, katerega cilj je optimalnejša obremenjenost omrežja.

Protokol LDP omogoča postopen ponovni zagon GRES (gracefull restart). Za uspešno izvedbo ponovnega zagona morajo pri postopku sodelovati tudi sosednji usmerjevalniki, ki se v tem primeru imenujejo pomočniki (helper). Usmerjevalnik, ki ga je potrebno zaradi nadgradnje programske opreme ponovno zagnati, mora najprej sporočiti to namero svojim sosedom pomočnikom. Nato pomočniki prevzamejo nase prometne tokove IP paketov in o rezultatu preusmeritve sporočijo usmerjevalniku, ki se bo ponovno zagnal. Ta se lahko nato nadgradi.

Drugi signalizacijski protokol je RSVP, ki omogoča več funkcionalnosti kot protokol LDP. Največja prednost pred protokolom LDP je možnost vzpostavljanja striktno ali ohlapno določenih poti LSP. Protokol RSVP v ta namen uporablja objekta ERO (Explicit Route Object) in RRO (Record Route Object). S pomočjo teh objektov je možno določiti striktne ali ohlapne poti LSP. Striktne poti imajo na celotni trasi vnaprej določene usmerjevalnike. Ohlapne poti so tiste, pri katerih se omrežje samo odloča o poteku poti.

Ena izmed glavnih prednosti protokola MPLS so obhodne poti in hitri preklopi med njimi. Protokol MPLS omogoča definicijo primarnih in obhodnih poti, preklop med njimi pa je mogoč v času manjšem od 50ms, kar je primerljivo s preklopnimi časi v omrežjih SDH.

V zadnjem času se zelo uveljavlja tehnologija »IPTv«, ki mora biti podprta tudi na usmerjevalnikih. Pri protokolu MPLS je bila v ta namen razvita tehnologija poti za hkratno oddajo več uporabnikom (multicast), ki s seboj prinaša boljšo izkoriščenost povezav v omrežju. Pri tej tehnologiji se v omrežje pošlje en tok video podatkov, omrežje pa nato poskrbi za množenje teh paketov. Na ta način vsak uporabnik dobi svojo kopijo IP paketa z video vsebino. To je primerno za prenos IPTv, kjer več uporabnikov istočasno spremlja isti TV program.

Protokol MPLS je ponudnikom internetnih storitev omogočil razširitev ponudbe z virtualnimi privatnimi omrežji, ki so zanimiva predvsem za poslovne uporabnike. Obstaja več vrst virtualnih privatnih omrežij. En primer omrežij VPN je BGP/MPLS L3VPN (RFC 4364) s protokolom BGP (Border Gateway Protocol) v signalizacijskem sloju, drugi pa MPLS L3VPN, ki uporablja protokol LDP (Draft Rosen). Virtualna privatna omrežja obeh tipov so sestavljena iz robnih usmerjevalnikov PE (Provider Edge) in hrbteničnih usmerjevalnikov P (Provider). Na robnih usmerjevalnikih so priključene naročniške povezave in konfiguracija. Hrbtenični usmerjevalniki P skrbijo za prenos podatkov in signalizacije med robnimi usmerjevalniki. Na teh usmerjevalnikih ni shranjene nobene naročniške konfiguracije.

IP naslovni prostori se lahko ponavljajo v vsakem virtualnem privatnem omrežju, kar pomeni, da si naročniki sami izbirajo IP naslovne prostore. V ta namen je bila razvita nova naslovna družina VPN-IPv4 (Virtual Private Network IP version 4). Smerem je potrebno dodati oznako kazalnik smeri. Protokol BGP poskrbi za prenos smeri med robnimi usmerjevalniki skupaj s kazalniki smeri.

3. Usmerjevalni protokoli OSPF, BGP in PIM

3.1. Uvod

Trenutno so v IP omrežjih izvedeni naslednji protokoli za avtomatsko prenašanje smeri med usmerjevalniki OSPF, IS-IS ter BGP. Protokol MPLS je funkcionalni dodatek tem protokolom. Trenutno sta najbolj razširjena protokola OSPF in BGP.

3.2. Usmerjevalni protokol OSPF

OSPF je usmerjevalni protokol, ki skrbi za prenos smeri in je definiran v standardu RFC2328. OSPF deluje znotraj enega avtonomnega sistema, zbira podatke o stanju povezav med usmerjevalniki in shranjuje topologijo omrežja. Osnova zapisa omrežne topologije je usmerjevalna tabela, ki skrbi za zapise naslednjih skokov IP, pomeni izpad določenega ali celotnega omrežja, ker se paketi vrtijo v krogu in obremenjujejo povezave. V primeru zank pride največkrat do popolnega izpada omrežja, ker so povezave 100 % obremenjene in ne prepuščajo ostalega IP prometa.

Omrežje OSPF se lahko razdeli na manjše enote, imenovane področja (area). S tem se poenostavi administracija, optimizira promet ter zmanjša obremenjenost resursov. Področja se identificirajo z 32-bitnim številom, preprosto v decimalni notaciji ali v štirih oktetih, razdeljenih s pikami, kot je to v primeru naslova IPv4. Hrbtenično področje je označeno s številko 0.0.0.0, ostala robna področja pa na primer z 0.0.0.2. Medsebojne povezave med področji, ki niso hrbtenična, niso dovoljene. Povezave med robnimi in hrbteničnimi področji potekajo na meji skozi področne robne usmerjevalnike ABR (Area Border Router). Usmerjevalnik ABR vzdržuje baze stanja povezav za vsa področja na katera meji in skrbi za združevanje smeri, ki prehajajo iz enega področja v drugega.

Protokol OSPF za izmenjavo podatkov o stanjih povezav uporablja svoje mehanizme za varen prenos le teh in ne uporablja transportnega protokola TCP. To je razlika od drugih usmerjevalnih protokolov, npr. BGP, ki prenese funkcijo varnosti in zanesljivosti prenosa na protokol TCP.

Za prenos smeri na povezavah razpršenega oddajanja uporablja OSPF naslov za oddajanje več prejemnikom (multicast). Takšni paketi se razširjajo le do sosednjih. Življenjska doba IP paketov je en skok (one hop). Pri protokolu OSPF je za hkratno oddajo več prejemnikom rezerviran IP naslovni prostor 224.0.0.5 ter 224.0.0.6.

Za medsebojno komunikacijo med usmerjevalniki v omrežjih IPv4 je pri protokolu OSPF možno vklopiti dodatno avtentikacijo. Preko te je omogočeno vključevanje v usmerjanje OSPF samo znanim usmerjevalnikom, ki poznajo gesla. V omrežjih IPv6 ni več uporabljena interna avtentikacija za protokole, uporablja se kar standardno šifriranje IPSeC, ki je že vključeno v varnost protokola IPv6 (IPv6 protocol security - IPSec).

3.3. Usmerjevalni protokol BGP

Protokol BGP je hrbtenični usmerjevalni protokol v internetnem omrežju. Protokol hrani in obvešča o omrežjih IP, ki so dosegljiva med avtonomnimi sistemi AS (Autonomous System). Avtonomni sistem je skupek naprav, ki jih upravlja podjetje. Vsak avtonomni sistem v Evropi ima registrirano svojo številko pri organizaciji RIPE (Regional Internet Registry for Europe).

V internetnih omrežjih je protokol BGP opisan kot protokol vektorja poti. V primerjavi z izračunavanjem najboljše poti pri protokolih IGP (Interior Gateway Protocol), se protokol BGP odloča o najboljših poteh na osnovi parametra pot (path). Ta parameter je zapis avtonomnih sistemov, ki jih je določena smer prepotovala. Manj kot je zapisov v parametru, krajša je pot do cilja. V primeru, da pripotujeta dve smeri do določenega usmerjevalnika po protokolu BGP, ta pogleda parameter pot in izbere tisto smer, v katerem je zapisanih manj avtonomnih sistemov AS.

Od leta 1994 je v uporabi protokol BGP verzije 4, nižje verzije se ne uporabljajo več. BGP je standardiziran kot RFC4271. Glavne prednosti te verzije so podpora usmerjanju CIDR in združevanje smeri. CIDR omogoča boljšo izrabo IP naslovnega prostora z uporabo dodatnih omrežnih mask (na primer 23 ali 25) pri izbiri IP naslovnih prostorov. Združevanje smeri pomeni združitev več manjših smeri v eno večjo, ki se nato oglaša ostalim BGP sosedom. Na ta način pripomoremo k zmanjšanju števila smeri v internetu. Trenutno vsebuje polna BGP tabela (full BGP table) okoli 280 000 smeri. Pri priklopu na dva ponudnika internetnih storitev je v usmerjevalnikih zapis dveh polnih tabel BGP, kar trenutno pomeni 560 000 smeri.

3.4. Usmerjevalni protokol PIM

Protokol PIM je del družine protokolov za hkratno oddajanje več prejemnikom (multicast).

Obstajajo štiri variante protokola:

- **PIM-SM (PIM sparse mode):** Protokol PIM v razpršenem načinu oddajanja več prejemnikom, si pri delovanju izgradi enosmerno večuporabniško drevo, ki je razvejano pri točkah RP (Rendezvous Point) za vsako skupino prejemnikov posebej. V vsaki skupini se lahko nahaja en podatkovni tok oziroma pri storitvi IPTV to pomeni en programski kanal (npr. SLO1). PIM ustvari najkrajše drevo od strežnikov do odjemnikov. PIM-SM je zelo razširljiv in kot tak primeren tudi za prenose preko internetnih povezav. Protokol je standardiziran v RFC 4601.
- **PIM-DM (PIM Dense mode):** Protokol PIM si v strnjenem načinu oddajanja več prejemnikom hkrati izgradi drevo oddajanja po celem omrežju, nato prekine oddajanje v tiste veje, kjer ni prejemnikov. PIM-DM ni najbolj razširljiv. Definiran pa je v standardu RFC 3973.
- **Dvosmeren protokol PIM (Bidirectional PIM):** Dvosmeren protokol PIM izgradi souporabniško dvosmerno drevo. Protokol PIM nikoli ne izgradi najkrajšega drevesa, zato so zakasnitve v omrežju večje. Protokol je zelo razširljiv, ker ne potrebuje informacij o stanju izvora podatkov (strežnik), definiran je v standardu RFC 5015.

- **PIM-SSM (Source Specific Multicast PIM):** Izvorno specifičen protokol PIM izgradi drevesa, ki imajo korenine samo pri enem izvoru. Protokol je zelo razširljiv. Izvore in skupine za oddajo več prejemnikom (multicast group) pri tem načinu protokola PIM poimenujemo izvor S (source) in skupina G (multicast group). Pri protokolu PIM-SSM izvor S oddaja IP pakete ciljnim naslovom za oddajo več prejemnikom G. Sprejemniki se lahko prijavijo v drevo tako, da se vključijo v kanal (S,G). Protokol je standardiziran v RFC 3569.

Med vsemi štirimi načini dela protokola PIM je najbolj razširjen PIM-SM.

4. Protokol MPLS

Protokol MPLS je bil razvit zaradi določenih izboljšav usmerjevalnih protokolov OSPF, BGP in RIP. Glavne prednosti protokola MPLS so:

- prometni inženiring,
- povezavno usmerjene poti,
- ponudba virtualnih privatnih omrežij ter
- usmerjanje z majhno režijo.

S pomočjo prometnega inženiringa je možno preusmerjati prometne IP tokove po optimalnejših poteh po omrežju. Pri tem si pomagamo s povezavno lastnostjo protokola MPLS in tako ustvarjamo povezavno orientirane poti. Drugi usmerjevalni protokoli (OSPF, RIP in BGP) usmerjajo IP pakete v nepovezavnem načinu dela.

Tretja lastnost, ki jo ima protokol MPLS, je ustvarjanje virtualnih privatnih omrežij VPN. Trenutno na trgu prevladujejo omrežja VPN, ki jih nudijo ponudniki storitev (provider provisioned VPN) nad omrežji VPN, ki jih ustvarjajo uporabniki sami.

Četrta lastnost protokola MPLS je usmerjanje z majhno režijo. To je možno zato, ker je glava MPLS velika le 4 oktete.

4.1. Terminologija protokola MPLS

4.1.1. Ekvivalentni razred posredovanja FEC

Ekvivalentni razred posredovanja FEC (Forwarding Equivalence Class) združuje tok podatkov IP paketov, ki se usmerjajo po isti poti LSP. Združevalni mehanizem temelji na ciljnem IP omrežju. Obstajata dva tipa združevalnih mehanizmov: gostiteljski in podomrežni.

Gostiteljski mehanizem združuje IP pakete z omrežnimi maskami dolžine 32 bitov, podomrežni razred pa vsem ostalim maskam v naslovih IP paketov (na primer 24, 25, …).

4.1.2. Labele MPLS

V protokolu MPLS se za usmerjanje uporabljajo vrednosti zapisane v MPLS glavi v obliki label. Labele imajo konstantne dolžine 20 bitov. Za določene storitve, ki temeljijo na protokolu MPLS, se uporablja sklad label (več label naenkrat). Usmerjevalniki, ki delujejo po protokolu MPLS, določijo vsakemu razredu FEC po eno labelo. Izbira vrednosti label ter njihova distribucija je določena v standardu protokola MPLS (RFC 3031).

4.1.3. Labelno komutirana pot

Labelno komutirana pot je skupek usmerjevalnikov, ki se nahajajo na poti paketa do ciljnega omrežja. Prvi usmerjevalnik na poti LSP se odloči o razredu FEC za IP paket in s tem paketu določi prioritete, po katerih ga bodo usmerjevalniki obravnavali na celotni poti po omrežju. Pri labelno komutirani poti se pri vsakem prehodu čez usmerjevalnik zamenja vrednost labele.

4.1.3.1 Distribucija label

Po izbiri vrednosti label je potrebno poskrbeti za prenos informacij o labelah sosednjim usmerjevalnikom. V ta namen sta na voljo dve možnosti za distribucijo label:

- ***Promet proti uporabniku na zahtevo**:* usmerjevalnik v tem načinu dodeli labelo potem, ko dobi prvi IP paket, ki ga mora poslati po poti LSP.
- ***Promet proti uporabniku brez zahteve***: usmerjevalnik dodeli labelo pred prvim IP paketom, ki ga mora poslati po poti LSP.

Po distribuciji label vsem usmerjevalnikom, ki sodelujejo pri protokolu MPLS, si jih morajo usmerjevalniki shraniti v spomin.

4.1.3.2 Shranjevanje label

Usmerjevalnik po protokolu MPLS sam poskrbi za shranjevanje in kontrolo nad labelami. Pri tem sta v standardu RFC3031 definirani dve možnosti za shranjevanje label:

- ***Liberalno shranjevanje label:*** pomeni, da usmerjevalnik obdrži labele tudi, če ni nobenega paketa usmerjanega po protokolu MPLS
- ***Konzervativno shranjevanje label:*** usmerjevalnik obdrži samo tiste labele, ki jih tudi trenutno uporablja. Ostale labele, ki nekaj časa niso v uporabi, odstrani iz spomina.

4.1.3.3 Kontrola nad labelami

Pri odločanju o vrednostih label je pomembno določiti kateri usmerjevalnik odloča o vrednostih label in o distribuciji le teh. Na voljo sta dve možnosti:

***Neodvisna kontrola nad labelami**: U*smerjevalnik določi razred FEC ter sam izbere labelo za povezovanje labele z razredom FEC.

***Urejena kontrola nad labelami**:* Pri urejeni kontroli izhodni usmerjevalnik (zadnji na poti LSP) poskrbi za razdelitev label vsem ostalim usmerjevalnikom, ki sodelujejo pri nastanku poti LSP.

4.1.3.4 Operacije z labelami

Usmerjevalniki, ki delujejo po protokolu MPLS podpirajo naslednje operacije, ki se izvajajo nad labelami:

- dodajanje labele (push),
- odvzem labele (pop),
- zamenjava labele (swap),
- večkratno dodajanje label (multiple push) ter
- zamenjava in dodajanje label (swap and push).

Opisi posameznih procesov

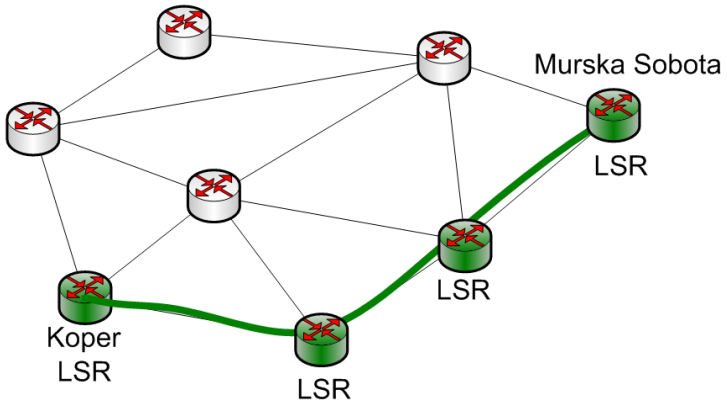
- ***Dodajanje label:*** Proces dodajanja labele v MPLS glavo vpiše novo vrednost labele. Vrednosti TTL, sklad label in CoS polje (Class Of Service) usmerjevalnik prepiše iz IP glave v MPLS glavo paketa.
- ***Odvzem label:*** Pri operaciji odvzema labele iz paketa se le ta odstrani in se paket usmerja na osnovi normalnih usmerjevalnih tabel. Vrednost TTL se iz MPLS glave paketa prepiše v IP glavo. Vrednost TTL se pri potovanju paketa na poti LSP

zmanjšuje. V primeru sklada label se odvzame le vrhnja labela, ostane pa spodnji sklad label.

- ***Zamenjava label:*** Pri operaciji zamenjave labele se vrhnja labela zamenja z novo. V labeli je zapisana tudi vrednost S (Stack), ki označuje prisotnost sklada label. S in CoS biti se pri zamenjavi labele prepišejo iz prejšnje labele. Vrednost TTL se pri zamenjavi zmanjša za 1.
- ***Večkratno dodajanje label:*** Proces dodajanja label pomeni vpisovanje večjega števila label (maksimalno 3) v MPLS glavo.
- ***Zamenjava in dodajanje label:*** Ta proces pomeni zamenjavo vrhnje labele v skladu label in dodajanje nove labele.

4.1.4. Usmerjevalniki, ki sodelujejo pri komutiranju label

Vsak usmerjevalnik, na katerem je bil konfiguriran protokol MPLS, sodeluje pri zamenjavi label. Ti usmerjevalniki imajo posebno ime in sicer labelno komutirani usmerjevalniki LSR (Label Switched Router) in sodelujejo pri izgradnji oziroma sestavljanju poti LSP. Protokol MPLS se lahko vključi samo na nekaj usmerjevalnikih v IP omrežju, ostali usmerjajo na podlagi drugih usmerjevalnih protokolov. Poti LSP pa se lahko vzpostavljajo le preko vmesnikov na usmerjevalnikih, na katerih je vklopljen protokol MPLS.



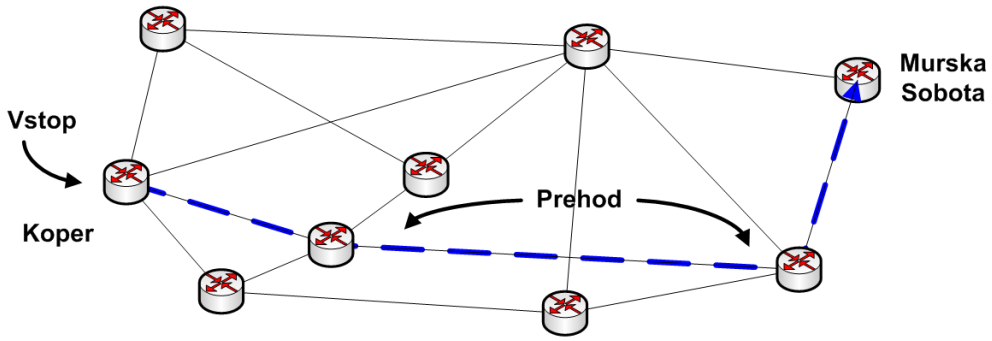
Slika 1: Usmerjevalniki LSR, ki sodelujejo pri komutiranju label

4.1.5. Funkcije usmerjevalnikov MPLS

Usmerjevalniki imajo v MPLS omrežju različne funkcije, glede na lokacijo na poti LSP. Usmerjevalnik na začetku poti je vhodni. V sredini poti LSP so prehodni usmerjevalniki, na koncu poti pa se nahaja izhodni usmerjevalnik.

4.1.5.1 Vhodni usmerjevalnik

IP paketi na vhodnem usmerjevalniku vstopajo v LSP pot (Slika 2). Ta usmerjevalnik se zato imenuje "head end" in deluje kot navzgornji usmerjevalnik (upstream router) ostalim sosedom. Ko usmerjevalnik po pregledu usmerjevalne tabele ugotovi, da je potrebno paket usmeriti na pot LSP, mu doda labelo. V primeru, da gre za omrežje VPN, doda dve labeli v MPLS glavo.



Slika 2: Vhodni usmerjevalnik

4.1.5.2 Prehodni usmerjevalnik

Prehodni usmerjevalnik posreduje IP paket z MPLS glavo naprej po poti LSP. Ta usmerjevalnik zmanjša vrednost TTL za 1, zamenja labelo v MPLS glavi, nato paket pošlje naprej sosednjemu usmerjevalniku na poti LSP.

4.1.5.3 Izhodni usmerjevalnik

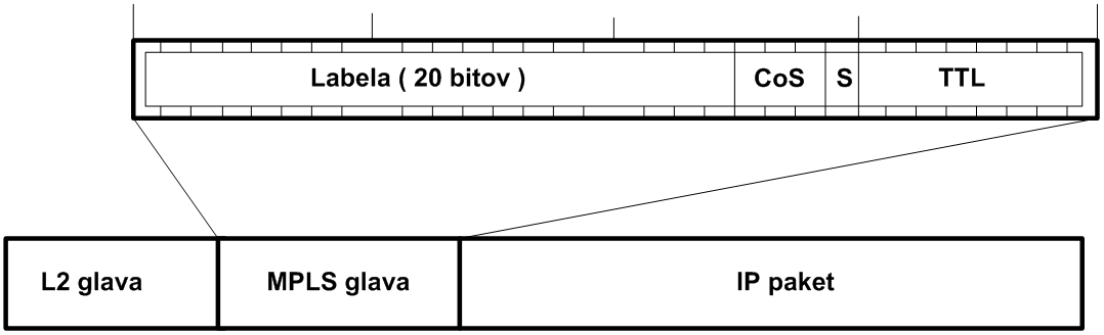
Funkcija izhodnega usmerjevalnika je, da IP paketu odvzame MPLS glavo in ga usmeri naprej na podlagi ciljnega IP naslova. V angleškem prevodu se imenuje tudi "tail-end" usmerjevalnik in ker je zadnji v vrsti, se imenuje navzdolnji usmerjevalnik (downstream router).

4.1.6. Glava MPLS

Na vhodnem usmerjevalniku IP paket vstopi v pot LSP. Na tem mestu se IP paketu doda MPLS glava velikosti 32 bitov. Dodajanje MPLS glave se imenuje tudi ovijanje IP paketa po protokolu MPLS.

Slika 3: Dodajanje 32 bitne MPLS glave

IP paketu se MPLS glava odstrani na koncu LSP poti. V IP omrežjih se uporablja MPLS glava tipa SHIM.



Slika 4: Glava MPLS – SHIM

4.1.6.1 Polje labela

V 20 bitno polje je vpisana vrednost labele.

4.1.6.2 Polje za kakovost storitev COS

V polje za določanje kakovosti storitev COS (Class Of Service) so vpisane tako imenovane EXP biti. S tem poljem je zagotovljena podpora kakovosti storitev in razdelitvi paketov v različne razrede storitev (CoS).

4.1.6.3 Skladovno polje S

S (Stack) bit ponazarja sklad label. V primeru, da ima S bit vrednost 1, pomeni, da imamo samo eno labelo. Če je v S bit vpisana vrednost 0, pomeni, da je prisotna še vsaj ena labela in torej lahko govorimo o skladu več label. V primeru sklada label, se paketu doda več MPLS glav in se zato dolžina paketa poveča za n-krat 32 bitov (n pomeni število glav).

4.1.6.4 Polje življenjske dobe paketa – TTL

Vrednost TTL (Time To Live) pomeni število usmerjevalnikov, ki jih lahko IP paket prepotuje, preden se mu življenjska doba izteče. Vsak usmerjevalnik zmanjša vrednost TTL za 1, ko vrednost pade na 0 usmerjevalnik izbriše paket. Vrednost TTL se v MPLS glavo pri vhodu v pot LSP prepiše iz IP glave.

4.1.6.5 Rezervirane vrednosti label

- **Vrednost 0** je eksplicitna 0. Usmerjevalnik, ki prejme paket z labelo 0 odstrani MPLS glavo in paket usmerja po protokolu IP. Ta način dela se imenuje UHP (Ultimate Hop Popping).
- **Vrednost 1** je uporabljena kot alarm. Vsak usmerjevalnik, ki prejme paket s to labelo, jo mora upoštevati, tudi če ni končni LSR usmerjevalnik. Trenutno ni napisane nobene aplikacije, ki bi upoštevala labelo z vrednostjo 1.
- **Vrednost 2** je vrednost 0 za IP verzije 6 in je ekvivalentna labeli 0 za IPv4. To vrednost se lahko uporabi le, kadar ni prisotnega sklada label. Usmerjevalnik mora glavo MPLS odstraniti in usmerjati paket na osnovi IP glave.
- **Vrednost 3** je implicitna vrednost 0. Uporabljena je lahko tudi v skladih z večjo globino kot 1. Ta labela ni nikoli dejansko vpisana v sklad label. V primeru, da je bila usmerjevalniku signalizirana labela z vrednostjo 3, pomeni, da mora odstraniti sklad

label preden posreduje paket naslednjemu skoku. Usmerjevalnik na naslednjem skoku nato usmerja promet na osnovi IP naslova. Ta način dela se imenuje odstranitev na predzadnjem skoku PHP (Penultimate Hop Popping).

- **Vrednosti 4 - 1048575** se lahko uporabijo po želji proizvajalca opreme in niso standardizirane.

4.2. Signalizacija pri protokolu MPLS

Protokol MPLS je razdeljen v dve ravnini: signalizacijsko in podatkovno. V signalizacijski ravnini se odvija vzpostavljanje poti LSP. V tej ravnini se iščejo najboljše poti po omrežju, ki določajo vrednosti label na LSP poteh. Nato se izvaja obveščanje vseh usmerjevalnikov o vzpostavljenih LSP poteh.

V podatkovni ravnini usmerjevalniki posredujejo dejanski promet (IP pakete), ki vsebujejo podatke. Ker je MPLS povezavno orientiran protokol, se poti vzpostavljajo med končnimi usmerjevalniki.

IETF je podprl več standardov za signalizacijo pri MPLS protokolu in sicer LDP, RSVP ter CR-LDP.

Glavne značilnosti protokolov LDP, RSVP in CR-LDP so:

LDP:

- delovanje po skokih,
- izbira iste fizične poti kot IGP,
- podpora manjši kompleksnost LSP poti.

CR-LDP

Ta varianta je razširjen protokol LDP z lastnostmi:

- razširitev protokola LDP s podporo eksplicitno določenim smerem,
- enaka funkcionalnost kot protokol RSVP.

RSVP

Glavne prednosti protokola RSVP so:

- razširljivost na eksplicitno določene smeri,
- uporaba s strani ponudnikov omrežnih storitev NP,
- je dobro poznan signalizacijski protokol.

4.3. Protokol LDP

Protokol LDP deluje v signalizacijski ravnini in skrbi za vzpostavljanje LSP poti. Poti LSP, ki jih ustvari protokol LDP, temeljijo na protokolu IGP. Najboljše poti, ki jih izbere protokol IGP, so posledično tudi najboljše poti za protokol LDP. Ta omogoča paketom, namenjenim v enako ciljno omrežje, da si delijo isto pot, kar pomeni, da uporabijo isto labelo. Protokol LDP vključi ciljno omrežje in LSP pot v razred FEC (RFC 3031) in razredu pripiše

določeno labelo. Posredovalne poti LSP, ki jih ustvari protokol LDP, so posredovalne poti za oddajo enemu uporabniku (unicast).

Avtomatičnemu vzpostavljanju poti LSP lahko dodamo določene omejitve. V ta namen je bil razvit razširjen protokol CR-LDP (Constraint based Label Distribution Protocol). Omejitve so lahko v obliki barv, s katerimi administrativno obarvamo povezave med usmerjevalniki LSR. Povezavam pa nato dodamo lastnost vzpostavljanja LSP poti le po povezavah z določeno barvo.

Protokol LDP uporablja za komunikacijo več različnih LDP sporočil. Vsa sporočila pa imajo skupno LDP glavo.

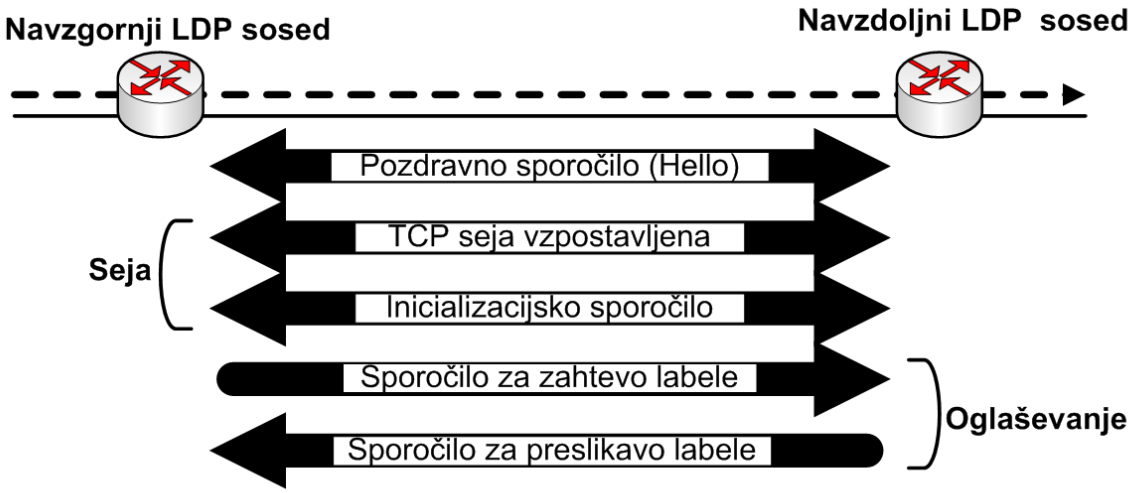
4.3.1. Pregled tipov sporočil po protokolu LDP

Komunikacija med usmerjevalniki poteka po protokolu LDP na osnovi naslednjih sporočil:

- **Pozdravno sporočilo**: Odkrivanje potencialnih LDP sosedov,
- **Sejna sporočila:** Nadzor nad TCP sejami ter inicializacijsko sporočilo,
- **Oglaševalna sporočila**: Ustvari, zahtevaj, preslikaj/zamenjaj ali izbriši labele, oglaševanje in brisanje LDP vmesnikov,
- **Sporočila za objave**: Svetovalne informacije za ostale usmerjevalnike.

4.3.1.1 Tipi LDP sporočil

Pri protokolu LDP je uporabljenih več tipov sporočil za vzpostavitev ali brisanje povezave label z razredom FEC ter za zapisnike o napakah pri komunikaciji.



Slika 5: Tipi sporočil LDP

Pozdravno sporočilo

S pomočjo pozdravnega sporočila se periodično oglašuje in vzdržuje informacije o prisotnosti usmerjevalnikov v omrežju. Pozdravno sporočilo je vpisano v UDP paket, ki ima vpisan ciljni naslov 224.0.0.2 za hkratno oddajo več naslovnikom. To sporočilo nato prejmejo vsi sosednji LDP usmerjevalniki.

Sejno sporočilo

S pomočjo sejnega tipa sporočila usmerjevalniki odpirajo, vzdržujejo ter zapirajo seje med LDP sosedi. Za vzpostavljanje seje med usmerjevalniki se uporabi TCP transport. Usmerjevalnik z višjim IP naslovom pa je odgovoren za pravilno vzpostavitev TCP seje.

Oglaševalno sporočilo

S pomočjo oglaševalnih sporočil se vzpostavljajo, spreminjajo ter brišejo povezave med labelami in razredi FEC.

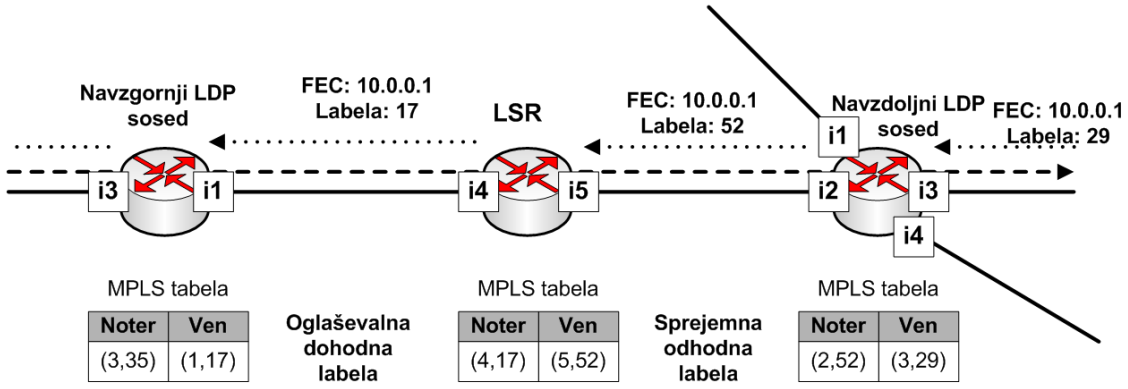
Objavno sporočilo

S pomočjo sporočil za objavo usmerjevalniki svetujejo ter sporočajo o napakah na povezavah med usmerjevalniki. Ko usmerjevalnik dobi sporočilo o takšni napaki zaključi TCP sejo z LDP sosedom in umakne vse povezave med labelami in razredi FEC, ki se jih je od tega soseda naučil.

4.3.2. Izbira in povezovanje label

4.3.2.1 Izbira MPLS label

Za izbiro label je odgovoren zadnji usmerjevalnik na poti LSP. Vsak usmerjevalnik višje na poti vpiše dve labeli v MPLS tabelo, ki jih prejme od LDP soseda. V tej tabeli so zapisane informacije o labelah in vmesnikih, preko katerih poteka pot. Na sliki spodaj so vmesniki označeni z oznakami: i1, i2, … i5. Razred FEC vključuje ciljni IP naslov 10.0.0.1.



Slika 6: Dodeljevanje label LDP razredom FEC

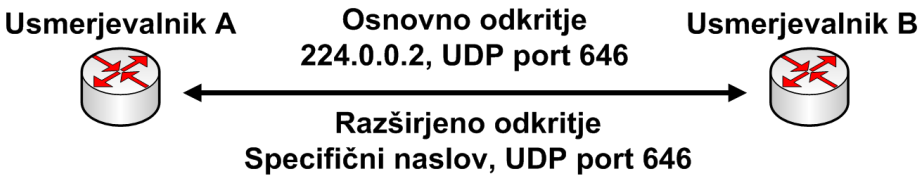
4.3.2.2 Povezovanje LDP Label z razredi FEC

Sporočila za dodeljevanje ter sporočila z zahtevami po dodeljevanju label se uporabljajo za povezovanje label z razredom FEC. V zgornjem primeru (Slika 6) ima usmerjevalnik na desni informacije o omrežju 10.0.0.1. Usmerjevalnik na sredini dobi preko vmesnika i5 informacijo o povezavi razreda FEC (naslovni prostor 10.0.0.1) z labelo vrednosti 52. Ta usmerjevalnik nato pošlje informacijo o tem razredu z svojemu upstream sosedu in temu razredu dodeli labelo 17. Proces se nadaljuje, dokler ne zmanjka usmerjevalnikov, ki morajo izvedeti za ta naslovni prostor.

4.3.3. Zaznavanje sosedov s pozdravnimi sporočili

4.3.3.1 Odkrivanje sosedov po protokolu LDP

Med procesom odkrivanja usmerjevalniki pošiljajo pozdravna sporočila na naslov 224.0.0.2 ali na točno določen naslov, ki pripada določenemu usmerjevalniku.



Slika 7: Odkrivanje sosedov po protokolu LDP

V obeh primerih se uporablja protokol UDP ter vrata z vrednostjo 646. V primeru, da usmerjevalnik pošlje paket na ciljni naslov 224.0.0.2, prejmejo ta paket vsi usmerjevalniki na tem podomrežju, kot je to definirano v standardu RFC 1112. Če postaja odgovori na pozdravno sporočilo, se predvideva, da je LDP usmerjevalnik pripravljen na vzpostavitev LDP sosedstva z usmerjevalnikom, ki je poslal pozdravno sporočilo.

4.3.3.2 Transportni naslov

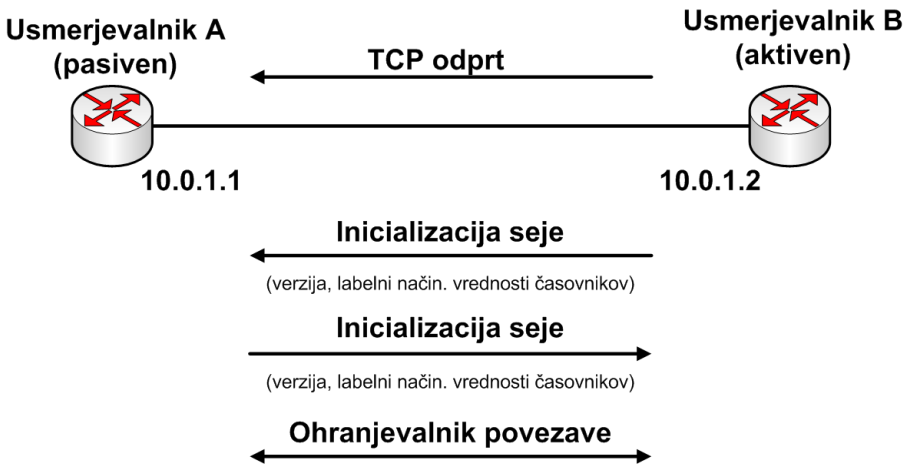
Za komunikacijo pri protokolu LDP se v seji TCP uporablja transportni naslov. Ta naslov se vpiše v pozdravno sporočilo kot objekt. Transportni naslov je lahko definiran ročno ali izbran avtomatsko s strani usmerjevalnika.

4.3.3.3 Pozdravno sporočilo LDP

Po vklopu protokola LDP začne usmerjevalnik pošiljati pozdravna sporočila na vseh delujočih vmesnikih. Pozdravna sporočila se naslavljajo na standardni naslov 224.0.0.2/32 po protokolu UDP z vrati 646. Pozdravna sporočila, kot tudi ostala LDP sporočila, so strukturirana v obliki TLV (Time Length Value).

4.3.3.4 *Vzpostavljanje transportne povezave*

Vozlišče, ki poseduje numerično večji IP naslov, je odgovorno za vzpostavitev TCP seje. Po uspešni vzpostavitvi seje TCP se lahko začne vzpostavljati seja LDP.



Slika 8: Vzpostavljanje transportne povezave

4.3.3.5 *Inicializacijsko sporočilo*

Najprej se med dvema sosedoma izmenjajo informacije o naslovnem prostoru ter transportnem naslovu z uporabo pozdravnih sporočil. Nato se vzpostavi seja LDP med sosedoma. Ta seja se uporablja za oglaševanje IPv4 naslovov od vmesnikov, label in omrežij dosegljivih preko LSP poti. Za zanesljivost seje LDP skrbi protokol TCP.

4.3.3.6 *Sporočilo ohranjevalnika povezave LDP*

Vsak usmerjevalnik izračunava in intervalno pošilja sporočila za ohranjevanje povezav. Čas ohranjevanja povezave (dead timer), ki ga usmerjevalniki izberejo po pogajanjih, je običajno 40 sekund. Ta čas se nato razdeli na tretjine in tako dobimo 10- sekundni čas ohranjevalnika povezave. V primeru uspešne dospelosti sporočila, se časovnik ponastavi na vrednost 0 in takoj nato začne naraščati. V primeru, da časovnikova vrednost naraste na 40 (4 x 10s), se sosedstvo prekine. »LDP soseda« se obravnava kot mrtvega.

4.3.4. Izmenjava informacij v seji LDP

Po vzpostavitvi LDP seje se začnejo prenašati omrežne informacije med usmerjevalniki. Med omrežne informacije spadajo naslovi usmerjevalnika ter labele za označevanje poti LSP. Vsak skupek informacij vsebuje svoj format sporočila in unikatne informacije.

4.3.4.1 *Oglaševanje naslova vmesnikov*

Prve informacije, ki se oglasijo LDP sosedu, so IPv4 naslovi za vmesnike, ki sodelujejo po protokolu LDP. To omogoča usmerjevalnikom, da poveže labele z naslovi naslednjih skokov. Naslovi se oglašujejo preko “oglaševalnega sporočila”.

4.3.4.2 Sporočilo za umik naslova

Če eden od sosedov prekine delovanje protokola LDP na določenem vmesniku ali ta postane neaktiven, se morajo prejšnji naslovi umakniti iz baz podatkov. To se izvede s pomočjo sporočila za umik naslova, ki je del oglaševalnih sporočil. V polje za tip sporočila za umik naslova se vpiše vrednost 0x0301.

4.3.4.3 Sporočilo za povezave label LDP

Izhodni usmerjevalnik oglašuje informacije o razredu FEC z določeno labelo svojemu navzgornjemu sosedu. Ta nato pošlje informacijo o razredu FEC z novo labelo svojemu navzgornjemu sosedu in sam postane tranzitni usmerjevalnik. Zadnji usmerjevalnik nato prevzame funkcijo vhodnega. Oglaševanje razreda FEC se izvrši s pomočjo oglaševalnega sporočila za povezave label LDP.

4.3.4.4 Sporočilo za umik LDP labele

V primeru, da mora usmerjevalnik umakniti določeno labelo iz razreda FEC, to sporoči sosedu s pomočjo sporočila za umik LDP labele. Razlika med sporočiloma za povezavo in umik LDP labele je v tem, da je tu vpisana vrednost za tip sporočila: 0x0402.

4.3.5. Vzdrževanje LDP seje

Usmerjevalniki si pošiljajo pozdravna sporočila v 10 sekundnih intervalih. Ti intervali so nastavljivi, zato v primeru, da ima usmerjevalnik vzpostavljenih več sej, za vsako vzdržuje drugačen pozdravni interval. Vsaka stran lahko pošlje prekinitveno sporočilo (shutdown message) in s tem prekine sejo med sosedoma.

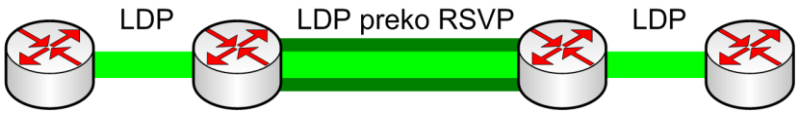
4.3.6. Izbira transportnega naslova

Transportni naslov se uporablja za TCP sejo, preko katere se zanesljivo prenašajo LDP sporočila. V primeru, da je med sosedoma več povezav, izbira transportnega naslova ni mogoča. Razlog za to omejitev je dejstvo, da je potrebno za pošiljanje LDP sporočila istemu sosedu uporabljati vedno isti transportni naslov.

4.3.7. Tuneliranje protokola LDP

Protokola LDP in RSVP omogočata medsebojno tuneliranje. Na ta način se lahko tunelirajo seje LDP preko protokola RSVP. Na ta način se lahko vzpostavi med robnimi usmerjevalniki protokol LDP, v hrbteničnem omrežju pa protokol RSVP. Pri vzpostavljanju tunelov usmerjevalniki dodajo še eno labelo poleg LDP labele in tako ustvarijo sklad label.

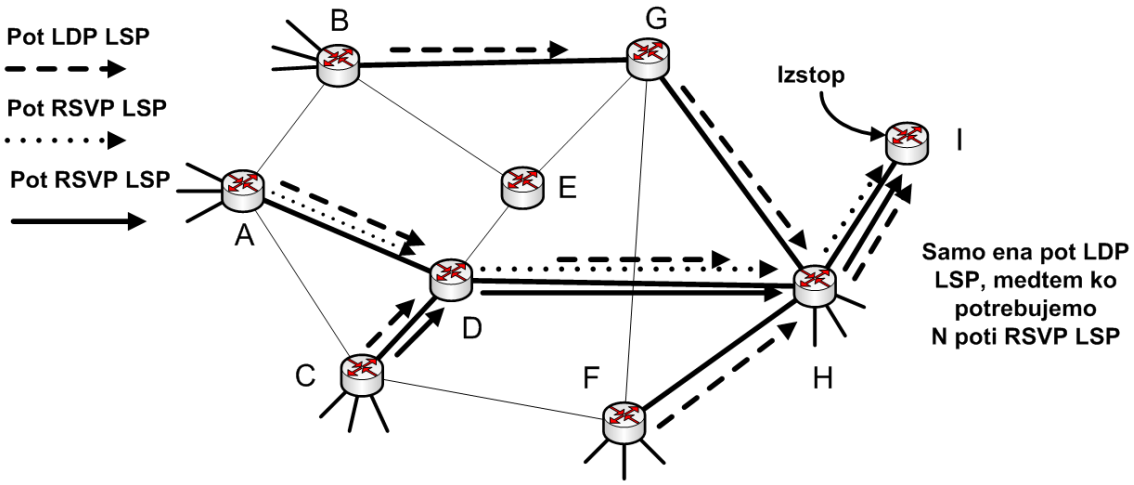
Pogoj za tuneliranje protokola LDP je vzpostavitev funkcionalnosti prometnega inženiringa pri protokolu IGP. Vsi usmerjevalniki v omrežnem jedru, kjer se izvaja prometni inženiring morajo pripadati istemu področju OSPF ali istemu nivoju IS-IS, odvisno kateri protokol se uporablja. V primeru neupoštevanja tega pravila protokol IGP ni sposoben izračunati naslednji skok.



Slika 9: Tuneliranje protokola LDP

4.3.8. Združevanje poti po protokolu LDP

Protokol LDP omogoča funkcionalnost združevanja LSP poti, če se te združijo na eni fizični poti. Protokol RSVP te funkcionalnosti nima. Slika 10 prikazuje primerjavo med številom label na posameznih fizičnih povezavah. LSP poti signalizirane s pomočjo protokola RSVP med A in I usmerjevalnikom ter C in I usmerjevalnikom imata različne labele na poti med D in H.

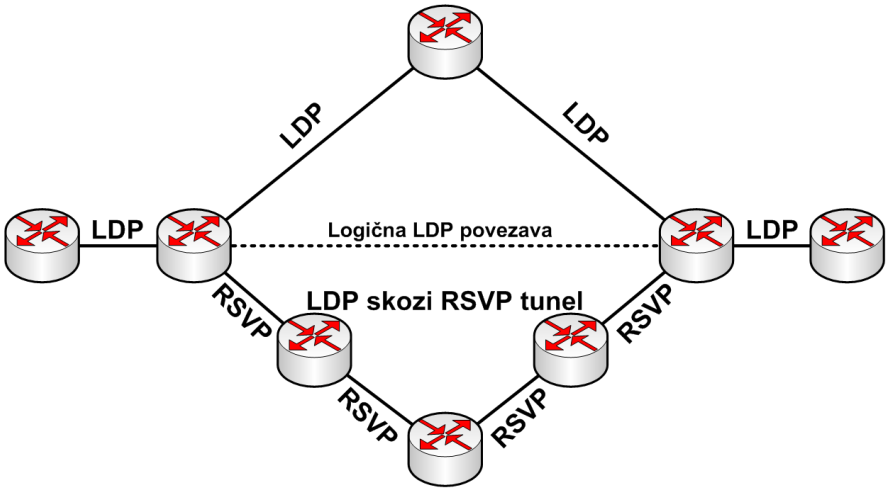


Slika 10: Operacije protokola LDP

Protokol LDP za razliko od protokola RSVP združuje poti LSP. Poti, ki potekata od usmerjevalnikov A in C do usmerjevalnika I, se na usmerjevalniku D združita v eno pot. Rezultat je ena pot na linku med D in H. To je prednost protokola LDP pred protokolom RSVP in pomeni mnogo večjo razširljivost protokola LDP.

4.3.9. Prometni inženiring protokolov LDP in RSVP

Poleg prometnega inženiringa, protokola IGP, poznamo prometni inženiring tudi pri protokolu MPLS. Slika 11 prikazuje LSP pot po protokolu LDP, ki je tuneliran preko protokola RSVP. Prometni inženiring deluje na RSVP tunelu. Po privzetem bi LDP pot potekala po poti izbrane s strani protokola IGP, torej po zgornjih usmerjevalnikih na skici. S pomočjo prometnega inženiringa protokola RSVP pa je bila pot preusmerjena na spodnje usmerjevalnike.



Slika 11: Prometni inženiring v protokolih LDP in RSVP

4.3.10. Politike filtriranja label

MPLS labele je pri protokolu MPLS možno filtrirati. S pomočjo politik filtriranja se kontrolira vzpostavljanje poti LSP ter razdruževanje razredov FEC. Pri protokolu LDP obstaja vhodno / izhodno filtriranje ter izhodne politike.

Kratka razlaga politik filtriranja je sledeča:

- *Vhodno filtriranje:* kontrola nad sprejemom razredov FEC, ki jih bo protokol LDP sprejel,
- *Izhodno filtriranje:* kontrola nad oglaševanjem razredov FEC
- *Izhodna politika:* kontrola nad razredi FEC, katerim je usmerjevalnik izhodni LSP usmerjevalnik (egress router).
- *Cilj* je oglaševanje direktno povezanih smeri, katerim je ta usmerjevalnik izhodni LDP usmerjevalnik.

4.3.10.1 Vhodna politika filtriranja

Splošno lahko z uporabo politik preprečimo vzpostavitev poti LSP, ni pa kontrole nad njihovim usmerjanjem. V primeru obstoja več enakovrednih poti med dvema usmerjevalnikoma, lahko s pomočjo politik filtriranja izključimo določeno pot iz izbire vzporednih poti.

4.3.10.2 Izhodna politika filtriranja

Izhodna politika se uporablja za filtriranje izhodnih LDP label. S to politiko se negira privzeta izhodna politika oglaševanja label, s katerimi se po protokolu LDP oglašuje usmerjevalnikov "loopback" naslov.

4.3.10.3 Izhodna politika usmerjanja

Z izhodno LDP politiko usmerjanja je možna kontrola nad oglaševanjem podomrežij po protokolu LDP. Usmerjevalnik tako postane izhodni usmerjevalnik za poti LSP, ki so namenjene do ciljnih podomrežij.

4.3.10.4 Razdruževanje razredov FEC

Pri hkratnem oglaševanju več podomrežij, vzpostavi usmerjevalnik povezavo vseh z eno labelo in vsa združi v en razred FEC. Razred nato poveže z eno potjo LSP, ki jo vodi skozi omrežje. Združevanje deluje v skladu s pričakovanji, dokler ne pridemo do potrebe po porazdeljevanju prometnih tokov (load balance) po več fizičnih poteh. To se zgodi v primeru, kadar imamo na voljo več poti, ki niso enakomerno obremenjene.

Da bi dosegli porazdeljevanje prometa, je potrebno razdružiti en razred FEC v več razredov in vsakemu dodeliti svojo labelo ter svojo LSP pot. Poti LSP nato vzpostavljamo s pomočjo prometnega inženiringa po več fizičnih poteh.

4.3.11. Avtentikacija sej LDP

IP paketi pri vzpostavljanju LDP sej potekajo na istih povezavah kot internetni promet, zato je bila zaradi večje varnosti razvita avtentikacija sej LDP. Avtentikacija poteka pri TCP protokolu, ki je uporabljen kot transportni protokol. Pri iskanju LDP sosedov se ne uporablja avtentikacija, za vzpostavitev seje pa se vklopi avtentikacija po algoritmu MD5 (Message Digest 5).

4.3.12. Postopni ponovni zagon seje LDP

Postopni ponovni zagon usmerjevalnika omogoča ugasnitev in ponovno vključitev usmerjevalnika brez izgube paketov. Zagon je opisan v standardu RFC 3478 "Graceful Restart Mechanism for Label Distribution Protocol". V primeru ugasnitve usmerjevalnika morajo vsi sosednji usmerjevalni protokoli podpirati ta način dela, drugače lahko pride do izgube paketov. Postopni ponovni zagon podpirajo tudi protokoli RSVP ter OSPF. Mehanizem postopnega ponovnega zagona po privzetem na usmerjevalnikih ni vključen.

Mehanizem poteka po naslednjem vrstnem redu:

- usmerjevalnik pred ustavitvijo delovanja oglasi svojo zmožnost za postopni ponovni zagon tako, da vključi TLV za občutljivost na napake v inicializacijsko sporočilo,
- po ponovnem zagonu usmerjevalnik signalizira sosedom, da se njegova posredovalna tabela ni spremenila. Sosedi, ki so bili v načinu pomoči, ohranijo vse labele poslane sosedu, ki se je ponovno zagnal.

Seveda lahko mehanizem deluje le v omrežju, v katerem ni težav z usmerjanjem. Uporabi se ga v primeru, ko želimo omrežje nadgraditi z novimi funkcionalnostmi, programskimi

verzijami ali strojnimi nadgradnjami. V primeru, da omrežje ne deluje, ni izpolnjen pogoj za delovanje mehanizma postopnega ponovnega zagona.

4.4. Protokol RSVP

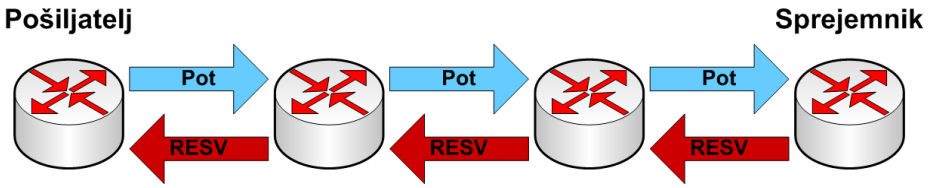
Druga različica signalizacije je protokol RSVP (RFC 2205), ki je bil načrtovan za rezervacijo resursov v omrežjih in nudi rezervacije za oddajanje enemu ter več prejemnikom. Rezervacije so pomemben del prometnega inženiringa in omogočajo podporo:

- eksplicitnemu definiranju poti,
- oštevilčevanju poti ter
- shranjevanju smeri.

CR-LDP je podoben protokolu LDP z dodanim prometnim inženiringom. CR-LDP in RSVP sta zelo podobna po zmogljivostih, vendar se protokol CR-LDP malo uporablja, zato ga ne bomo obravnavali.

4.4.1. Signalizacija poti po protokolu RSVP

Protokol RSVP zahteva resurse za enosmerne prometne tokove. Sporočila za poti in rezervacije se izmenjujejo dvosmerno od pošiljatelja k sprejemniku.



Slika 12: Signalizacija poti RSVP

Ko usmerjevalnik dobi zahtevo po vzpostavitvi poti, lahko to zavrne zaradi pomanjkanja resursov ali vzpostavi mehko stanje. To je komplementarno stanje k trdi vzpostavitvi poti, pri kateri se vzpostavljajo virtualne povezave, ki ostanejo odprte v času pretoka podatkov.
Mehka vzpostavitev poti pa pomeni, da se kontrolni podatki prenašajo drugje, kot sami podatki iz podatkovne ravnine.

4.4.1.1 Objekt za eksplicitno določeno smer (ERO)

Operaterju omrežja omogoča objekt ERO vpis vozlišč, ki jih mora LSP nujno prepotovati. V protokolu LDP tega objekta ni in se zato prometni inženiring ne more izvajati.

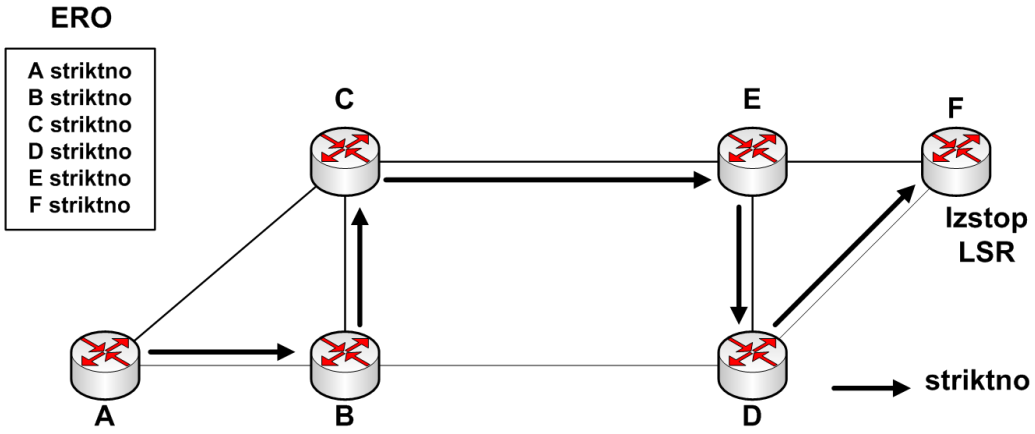
Eksplicitni objekt smer se uporablja za ohlapno določanje ali striktno določanje LSP poti. Ohlapno določene smeri temeljijo na klasičnih usmerjevalnih tabelah, ki določajo vozlišča, preko katerih bo potekal LSP. Pri striktno določenih LSP poteh administrator vpiše, katera vozlišča mora LSP prepotovati.

LSP je lahko na določenem odseku poti določen striktno, na drugem ohlapno.

4.4.1.2 Striktno določena pot

Pri striktno določenih poteh je potrebno vpisati vsakega izmed usmerjevalnikov, ki se nahajajo na LSP poti. Na tej poti niso dovoljene izjeme. Slika 13 prikazuje striktno določeno

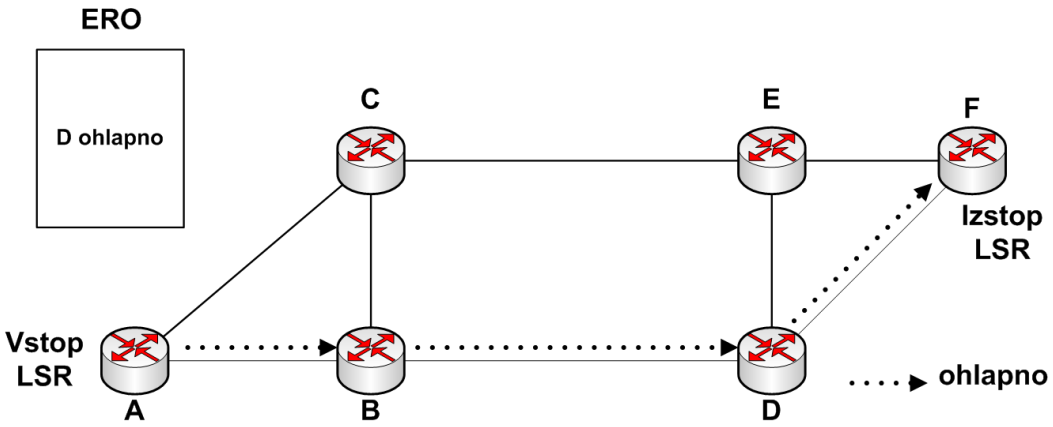
pot, ki gre skozi usmerjevalnike v naslednjem vrstnem redu: A, B, C, E, D in F. Konfiguracija za striktno določeno pot se vpiše v usmerjevalnik A, ki nato poskrbi za prenos informacije o poti vsem ostalim usmerjevalnikom.



Slika 13: Striktno določena smer

4.4.1.3 Ohlapno določena pot

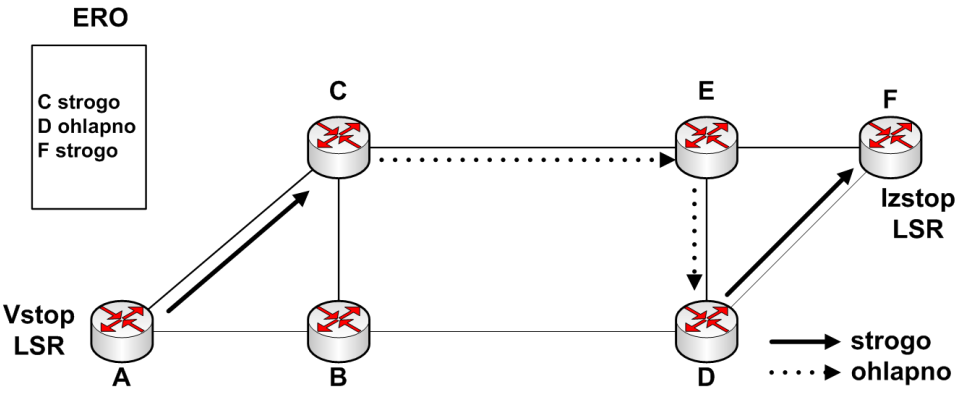
Pri ohlapno določeni poti si usmerjevalniki sami izgradijo LSP. Kot pomoč za določanje naslednjih skokov usmerjevalniki pregledajo usmerjevalne tabele protokola IGP in te informacije uporabijo za vzpostavljanje nove poti LSP. Slika 14 prikazuje vpis usmerjevalnika D v konfiguracijo poti LSP. To pomeni, da mora LSP potekati skozi usmerjevalnik D, ostale skoke usmerjevalniki določijo avtomatsko na osnovi usmerjevalnih tabel IGP. Usmerjevalniki imajo dva odseka za izračun: odsek med usmerjevalnikoma A in D ter segment D - F.



Slika 14: Ohlapno določene smeri

4.4.1.4 Kombinacija striktno in ohlapno določenih smeri

Mogoča je tudi kombinacija striktno ter ohlapno določenih smeri; primer - na začetku ter na koncu je striktno določena pot, vmes pa usmerjevalniki sami izberejo pot na osnovi protokola IGP. Slika 15 prikazuje zapis na usmerjevalniku A, kjer je vpisan usmerjevalnik C kot strogo (striktno) določen zapis, kar pomeni, da mora pot potekati po fizičnem linku med A in C. Nato je ohlapno zapisan D, kar pomeni, da se bo usmerjevalnik oprl na informacije iz protokola IGP. Pot mora nato potekati strogo do F in sicer po fizičnem linku med D in F.



Slika 15: Kombinacija strogo in ohlapno določene smeri

4.4.1.5 Objekt smeri

Preko objekta smeri RRO (Record Route Object), dodanega k sporočilu o poti (path message), vhodni usmerjevalnik LSR izve o poteku poti LSP. To je povratna informacija o točni poti LSP, ki jo morajo izvedeti vsi usmerjevalniki, ker pri sami vzpostavitvi ne vedo, kakšna bo točna pot.

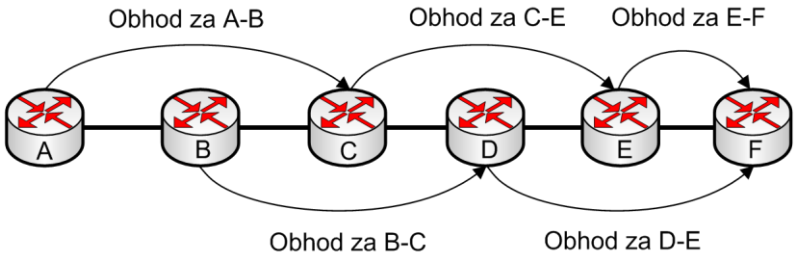
RRO je odgovoren tudi za zaznavanje možnih zank v omrežju, ki nastanejo v primeru težav. Zanke nastopijo, če se določen usmerjevalnik dvakrat pojavi v zapisu LSP poti.

4.4.2. Obhodne poti pri protokolu MPLS

Zaščita poti LSP se izvaja s preklopi med primarnimi in obhodnimi potmi. Mehanizem "fast reroute" opisuje vzpostavitev obhodnih poti še v času delovanja primarne poti. Vzpostavljajo se poti, ki potekajo mimo naslednjega skoka in zaobidejo eno vozlišče. Ker klasični izračun nove poti zahteva kar nekaj časa (razred sekund), je «fast-reroute« boljši način izračunavanja poti.

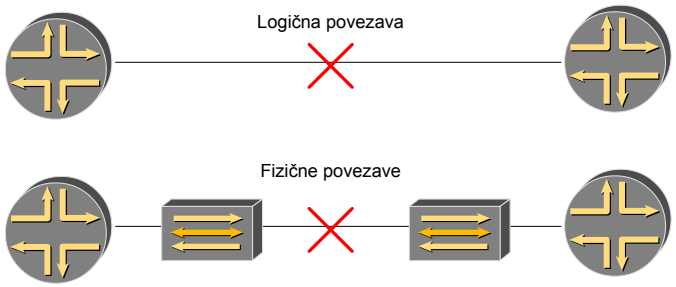
4.4.2.1 Hitra obhodna pot

Pri mehanizmu se hitre obhodne poti (fast-reroute) vzpostavijo vnaprej. V primeru težav s povezavami se aktivirajo poti, ki služijo kot obhodna pot za določene povezave (vozlišča). Povezave lahko potekajo preko več usmerjevalnikov, pogoj je, da ti delujejo po protokolu MPLS. Ta način je dober za primere, ko se pojavi enojna napaka. V primeru več nedelujočih povezav obstaja možnost, da ta način ne bo zagotavljal obhodne poti.



Slika 16: Hitra obhodna pot

Pogoj za hitri preklop med primarnimi in obhodnimi potmi je zaznavanje izpada povezav. Klasičen problem zaznavanja izpadov povezav je, če na povezavo med dvema usmerjevalnikoma vključimo dva stikala (Slika 17).



Slika 17: Izpad povezave med usmerjevalnikoma

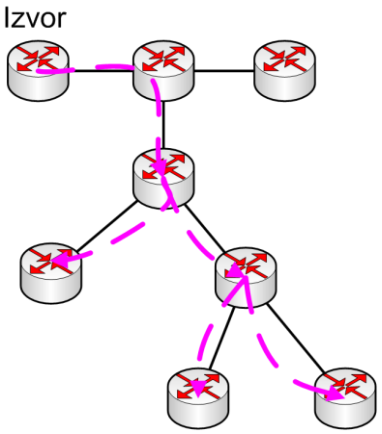
Slika 17 prikazuje logično povezavo med usmerjevalnikom, zgrajeno iz dveh stikal in povezav med njima in usmerjevalnikoma. Pri izpadu povezave med stikaloma ta po trenutnih standardih ne sporočita izpada naprej usmerjevalnikoma. Usmerjevalnika morata zato sama ugotoviti, da povezava ne deluje več. To se lahko zgodi najprej v okviru nekaj sekund, ko se iztečejo določeni časovniki. Primer protokola za zaznavanje izpadov je BFD (Bidirectional Forwarding Detection). Takoj ko usmerjevalniki izvedo za izpad prometa, lahko eden sporoči ostalim usmerjevalnikom, predvsem vhodnemu, da je postala pot LSP nedelujoča. Vhodni usmerjevalnik nato preklopi iz primarne poti na obhodno pot.

V primeru, da so usmerjevalniki povezani z direktnimi povezavami (brez vmesnih stikal), se lahko preklopi izvedejo v času pod 50 ms. Če so na poti med usmerjevalniki priklopljena še »ethernet« stikala, se časi preklopov drastično povečajo (razred nekaj sekund).

4.4.3. Poti za oddajo več prejemnikom

Protokol RSVP omogoča konfiguriranje poti LSP za oddajo več prejemnikom (multicast). Prenos video signalov preko IP je primer aplikacije, ki potrebuje takšne poti. Brez uvedbe poti za oddajo več uporabnikom se v omrežju do vsakega ciljnega uporabnika, ki zahteva prenos

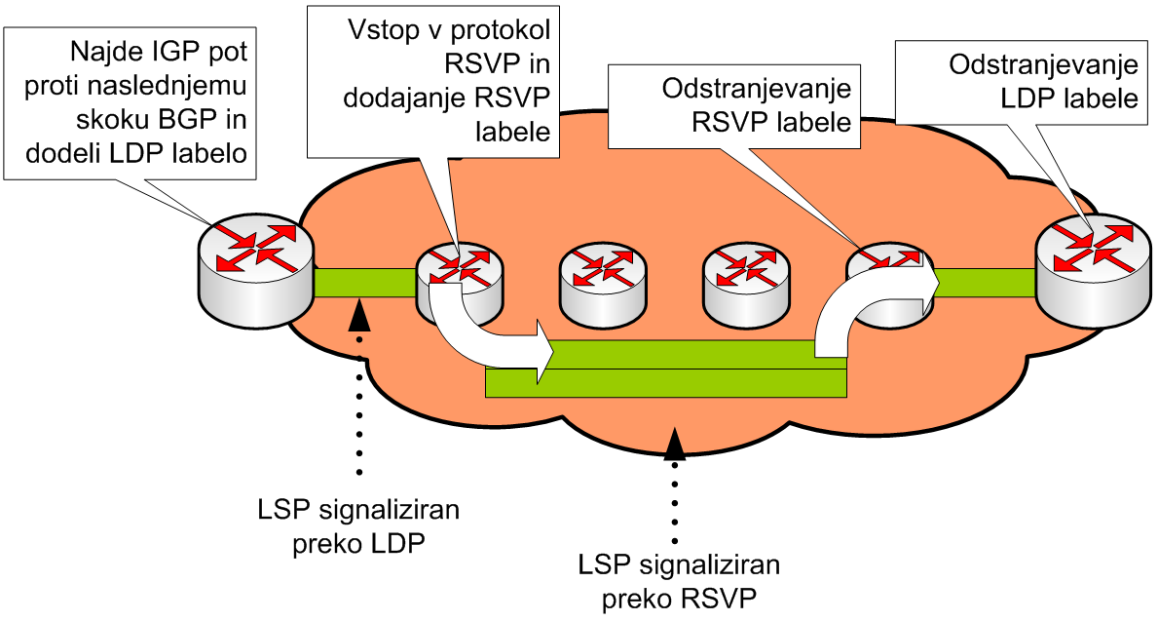
video paketov, prenese svoj tok podatkov (packet stream). Če več uporabnikov hkrati spremlja isti TV kanal, je smiselno v omrežju prenašati samo en tok podatkov do razvejitev (
Slika 18). Nato usmerjevalniki na teh razvejitvah podvojijo isti tok podatkov in ga pošiljajo po več vejah naprej. S tem dosežemo manjšo obremenjenost omrežja.



Slika 18: Poti LSP za oddajo več prejemnikom

4.4.4. Skladi label

V primeru, da imamo jedro omrežja (Slika 19), ki je signalizirano s pomočjo protokola RSVP, lahko prenašamo protokol LDP skozi RSVP tunel.



Slika 19: Skladi label

Za potrebe vzpostavljanja tunelov uporabimo funkcionalnost sklada label. MPLS sklad zgleda tako, da je v MPLS glavi LDP labela, ki ji je dodana še RSVP labela. Na prvem usmerjevalniku se doda prva labela (protokol LDP), na drugem pa se ustvari sklad label z

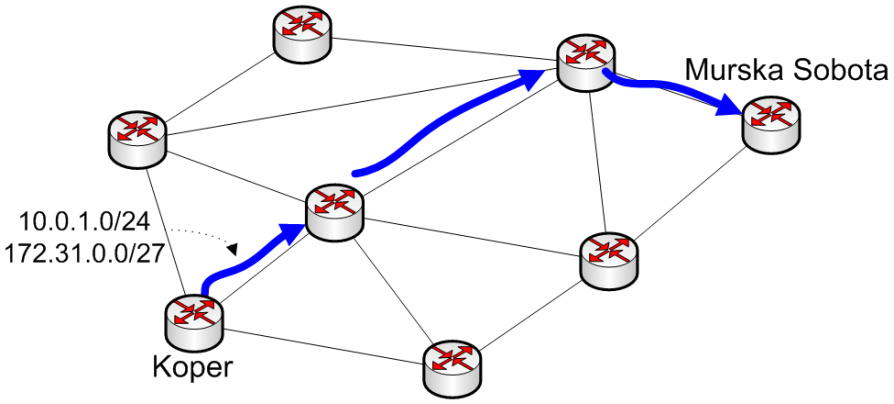
dodajanjem druge labele (protokol RSVP). Tretji in četrti usmerjevalnik na poti samo posredujeta pakete na osnovi zgornje RSVP labele. Peti usmerjevalnik odstrani RSVP labelo, šesti, zadnji usmerjevalnik na našem primeru nato odstrani labelo in usmeri paket na osnovi IP usmerjevalne labele.

4.5. Prometni inženiring na osnovi protokola MPLS

Kadar se v omrežju zapolnijo določene povezave oziroma so te preobremenjene, je potrebno prometne tokove preusmeriti. To se lahko doseže s pomočjo prometnega inženiringa pri protokolu MPLS.

4.5.1.1 Usmerjanje s pomočjo protokola IGP

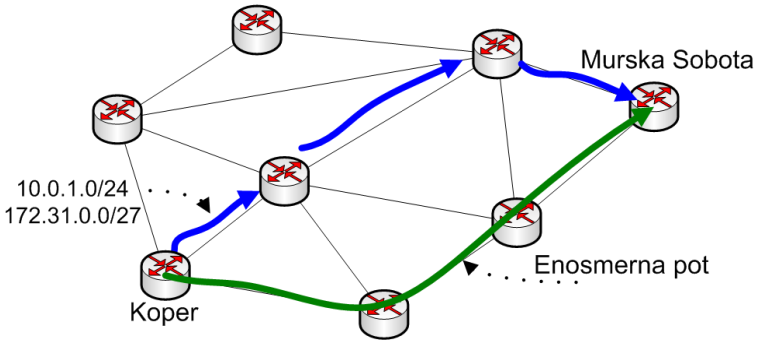
Protokol IGP je eden izmed usmerjevalnih protokolov, ki prenašajo smeri med usmerjevalniki. Protokol IGP izbere najbližjo pot do cilja glede na hitrost in število povezav. Na odločitev, katera pot je najboljša, je težko vplivati. Ta vrsta izračunavanja in usmerjanja je vezana le na naslednji fizični skok (next-hop). Slika 20 prikazuje najbližjo pot iz Kopra do Murske Sobote za omrežja 10.0.1.0/24 in 172.31.0.0/27, ki poteka po modri liniji. Na spremembo poti lahko vplivamo z nastavljanjem določene metrike na povezavah, vendar to potem velja za vse izračunane poti.



Slika 20: Klasično usmerjanje vezano na fizični skok

4.5.1.2 Vzpostavitev dodatne poti s pomočjo protokola MPLS

Enosmerne poti skozi omrežje pri protokolu MPLS se lahko vzpostavijo brez uporabe poti, izračunanih s pomočjo protokola IGP. Enosmerne poti LSP se vzpostavljajo s pomočjo prometnega inženiringa statično ali dinamično z uporabo prometnega inženiringa. V tem primeru je omogočena večja kontrola nad prometnimi tokovi in usmerjanjem. Slika 21 prikazuje vzpostavitev poti LSP iz Kopra do Murske Sobote (zelena linija) skozi druge usmerjevalnike, kot je to v primeru IGP (modra linija).

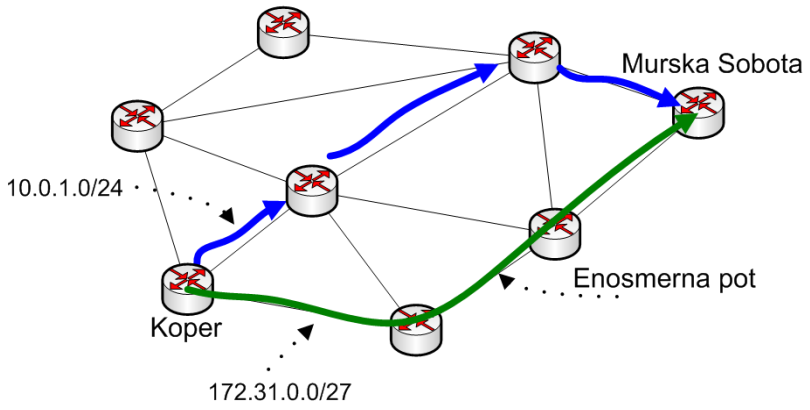


Slika 21: Prometni inženiring s pomočjo protokola MPLS

4.5.1.3 Preusmeritev prometnih tokov na nov LSP

Prometni tok preusmerimo skozi LSP, tako, da vanj usmerimo IP podomrežje 172.31.0.0/27. S tem vplivamo na promet, ki je namenjen do tega ciljnega omrežja.

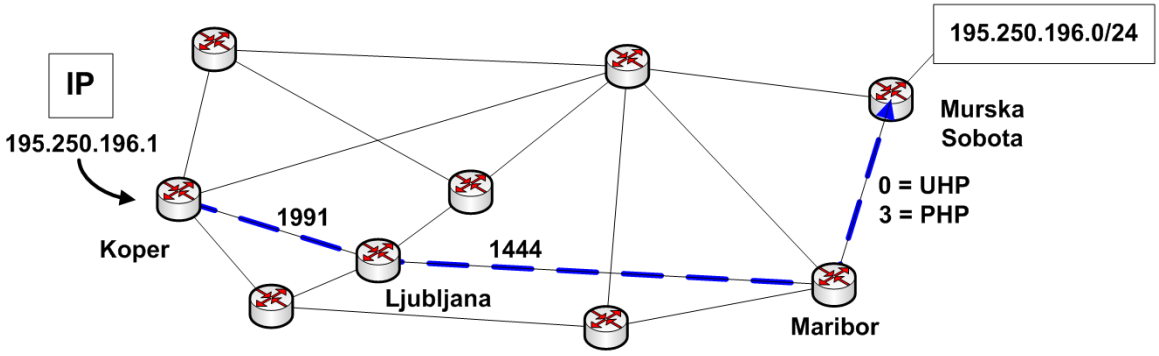
To je enosmerna rešitev, v drugo smer je potrebno vzpostaviti nov LSP.



Slika 22: Poti MPLS na osnovni prometnega inženiringa

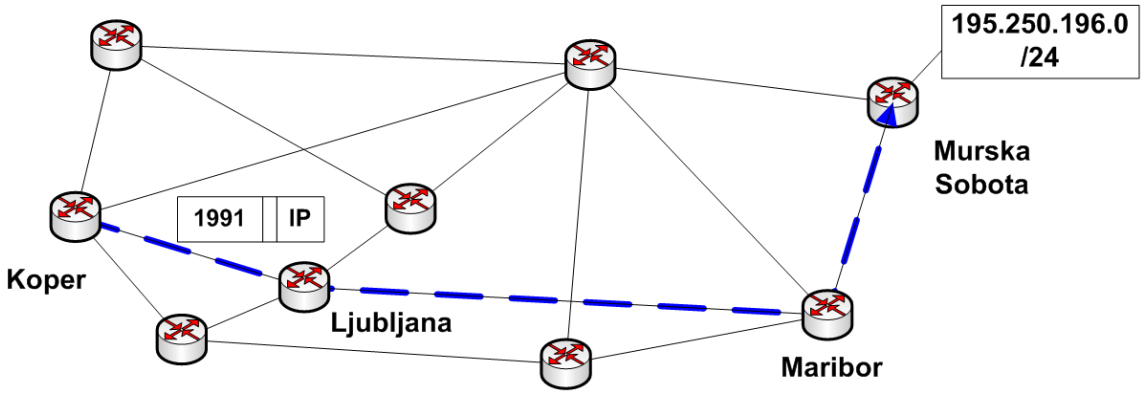
4.6. procesiranja v podatkovni ravnini MPLS

Kot primer je navedeno posredovanje IP-paketa v omrežju MPLS iz usmerjevalnika v Kopru do usmerjevalnika v Murski Soboti. V koprski usmerjevalnik prispe IP paket v katerega je vpisan ciljni IP naslov 195.250.196.1.



Slika 23: Primer procesiranja v MPLS

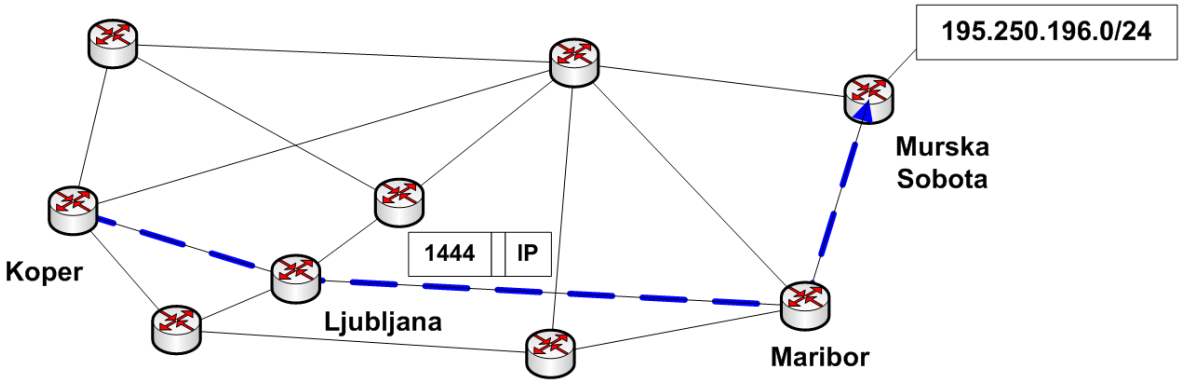
Ciljno omrežje je konfigurirano v Murski Soboti in se nahaja na koncu LSP poti za oddajo enemu uporabniku (unicast). O tem je obveščen tudi koprski usmerjevalnik, ki ta paket usmeri po poti LSP do Murske Sobote. Torej je koprski usmerjevalnik vhodni usmerjevalnik na LSP poti in IP paketu doda MPLS glavo z labelo vrednosti 1991.



Slika 24: Prvi usmerjevalnik na poti LSP

S tem je bil narejen prvi korak na poti posredovanja MPLS paketa do Murske Sobote. Usmerjevalniki na poti nato ne usmerjajo IP paketa na osnovi ciljnega omrežja, temveč posredujejo paket na osnovi label MPLS.

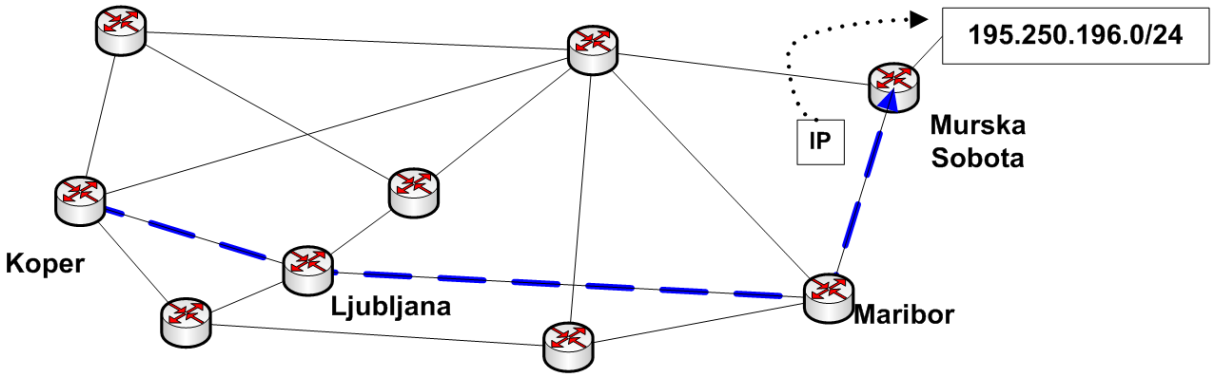
Tranzitni usmerjevalnik najprej pregleda MPLS labelo in ugotovi zapisano vrednost 1991.



Slika 25: Drugi usmerjevalnik na poti LSP

Nato pogleda v MPLS posredovalno tabelo, v kateri je zapisano, na katerem vmesniku je potrebno poslati paket naprej po LSP poti. V tabeli je vpisano tudi, katero novo vrednost labele mora vpisati usmerjevalnik v MPLS glavo paketa. V našem primeru je to nova vrednost 1444. Podobno naredi tudi usmerjevalnik v Mariboru.

Izhodni usmerjevalnik v Murski Soboti odreže glavo MPLS in usmeri paket na osnovi informacije iz IP glave.



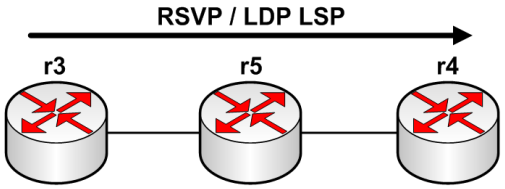
Slika 26: Izhodni usmerjevalnik v LSP

Tu je zapisano, da je ciljni IP naslov 195.250.196.1 in usmerjevalnik poišče naslednji skok v IP usmerjevalni tabeli.

4.7. MPLS ping

MPLS ping (Slika 27) omogoča preverjanje posredovanja in s tem delovanje poti LSP. Preden je bil standardiziran MPLS ping, je bilo potrebno uporabljati BGP smeri za preizkus delovanja poti LSP. Torej se je posredovalna raven testirala s pomočjo usmerjevalne ravni.

MPLS ping deluje podobno kot navaden ping, vendar po protokolu MPLS.



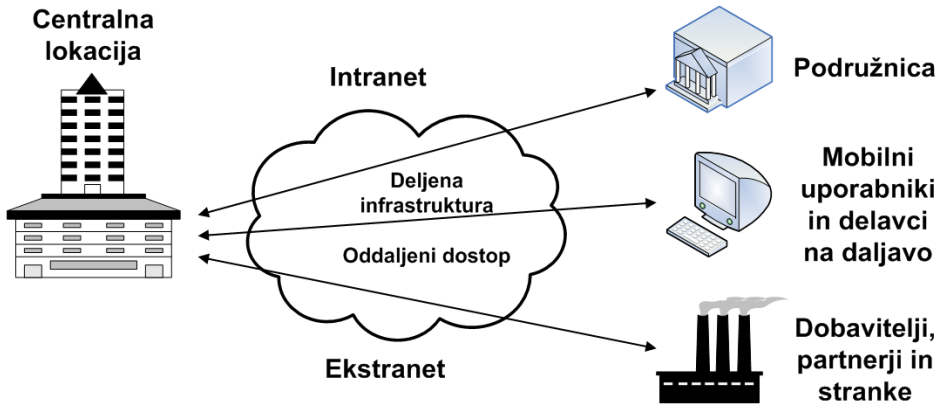
Slika 27: MPLS ping

5. IP MPLS VPN

V prejšnjih poglavjih so bili opisani vsi protokoli, ki jih potrebujemo za vzpostavitev nove storitve IP MPLS VPN. S tem se približamo cilju čim večjega izkoriščanja IP omrežja. Ta storitev omogoča naročnikom, da si ustvarijo svoje omrežje, ki ni vidno ostalim uporabnikom. To privatno omrežje pa jim nudi kar ponudnik storitev. Pristopne točke POP (Point Of Presence) k storitvi IP MPLS VPN se lahko zagotavljajo na vseh lokacijah, kjer se razprostira omrežje ponudnika storitev.

5.1. Sodobno omrežje VPN

Internetno omrežje zagotavlja povezavo vseh IP omrežij preko javnega naslovnega prostora. To je odprt medij za komunikacijo, kar pa je omejitev, ki jo poslovni svet ne sprejema preveč dobro. Zato se je pojavila potreba po virtualnih omrežjih, ki bi bila zaprta za internet. V ta namen je bila razvita storitev IP MPLS VPN. Na ta način lahko uporabniki uporabijo deljeno infrastrukturo za zagotavljanje intraneta kot tudi ekstraneta. Intranet je interno IP omrežje v podjetju, ki zagotavlja dostop do internih informacij. Ekstranet pa zagotavlja dostop do informacij, ki jih podjetje nudi svojim poslovnim partnerjem.



Slika 28: Sodobno omrežje VPN

5.2. Primeri storitev VPN

Obstajata dve vrsti storitev VPN in sicer tiste, ki jih zagotavljajo uporabniki sami imenovani CPE VPN (Customer Premises Equipment) in tiste, ki jih zagotavlja ponudnik storitev imenovane PP (Provider Provisioned).

Primeri omrežij CPE VPN so naslednji:

- **PPTP in L2TP** sta tehnologiji, ki omogočata ustvarjanje tunelov tipa točka-točka. Tuneli se vzpostavljajo med naročnikovim usmerjevalnikom in se zaključujejo na ponudnikovem usmerjevalniku.
- **IPSeC** je virtualno privatno omrežje tipa točka-točka in se uporablja za zagotavljanje privatnosti in šifriranja skozi internetno omrežje.

Ponudniki omrežij pa trenutno zagotavljajo naslednja VPN omrežja:

- **L2VPN:** Vse povezave v tem omrežju so na nivoju OSI 2 oziroma se ponudnikovo omrežje obnaša kot stikalo z dvema priključkoma.
- **VPLS:** Pri tej storitvi se ponudnikovo omrežje obnaša kot pravo ethernet stikalo z več priključki.
- **L3VPN:** Omrežje se obnaša kot usmerjevalnik z več priključki. Vse tri omenjene rešitve temeljijo na protokolu MPLS in so zelo razširljive v velikostnem redu 1000 VPN omrežij.
- **Virtualni usmerjevalniki:** Pri tem načinu se vsak usmerjevalnik razdeli v več logičnih usmerjevalnikov, ki se nato med seboj povežejo v novo logično omrežje. Ta rešitev ne temelji na protokolu MPLS. Ker ta način zavzame veliko resursov usmerjevalnika, je rešitev razširljiva samo do nekaj deset virtualnih usmerjevalnikov.

6. Virtualno privatno omrežje L3VPN

Dober primer za razlago delovanja virtualnih privatnih omrežij tipa BGP/MPLS je omrežje L3VPN. Protokoli IGP, BGP ter MPLS, ki se uporabljajo za zagotavljanje storitve L3VPN, so enaki tudi pri storitvah L2VPN ter VPLS.

6.1. Kontrolna in podatkovna ravnina pri L3VPN

Virtualno privatno omrežje L3VPN je razdeljeno na dve ravnini: kontrolno in podatkovno. Kontrolna ravnina poskrbi za vzpostavljanje poti MPLS LSP ter za prenos smeri po protokolu MP-BGP (Multi Protocol Border Gateway Protocol), podatkovna pa za prenos podatkov preko poti LSP.

6.1.1. Kontrolna ravnina

Kontrolna ravnina zavzema več mest v standardu RFC 2547. V tej ravnini se nahajajo usmerjevalni protokoli med PE in CE usmerjevalniki. PE usmerjevalniki posredujejo smeri ostalim PE usmerjevalnikom po protokolu MP-BGP. Signalizacija LDP ali RSVP za vzpostavljanje poti LSP se tudi nahaja v tej ravnini.

6.1.2. Podatkovna ravnina

Ko kontrolna ravnina poskrbi za vzpostavitev poti LSP, se le te nato uporabijo v podatkovni ravnini. Preko njih se prenašajo IP paketi, ki potujejo med lokacijami določenega omrežja VPN.

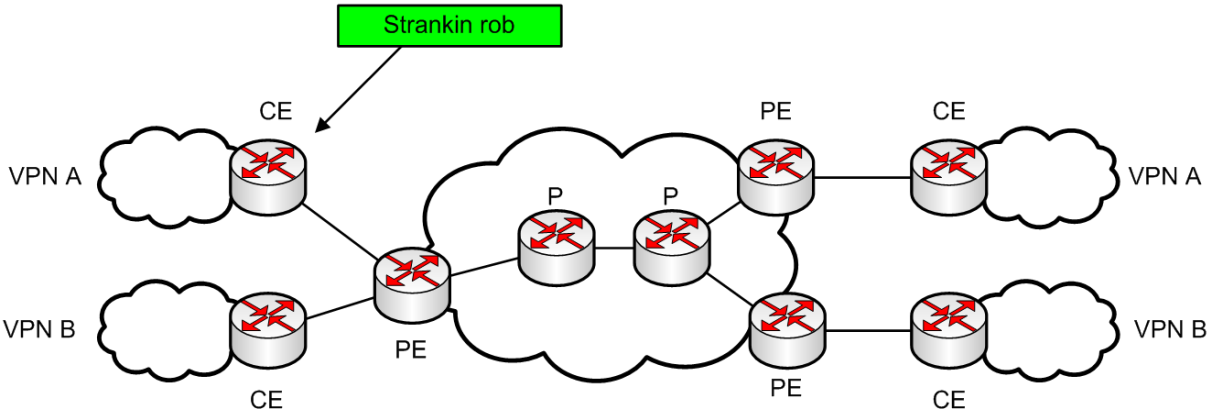
6.2. Poimenovanje usmerjevalnikov v omrežju VPN

Usmerjevalniki, ki sodelujejo pri ustvarjanju omrežij VPN, imajo različne vloge. Obstajajo tri vrste usmerjevalnikov:

- uporabniški robni CE (Customer Edge),
- ponudnikov robni PE (Provider Edge) ter
- ponudnikov usmerjevalnik P (Provider).

6.2.1. Uporabniški robni usmerjevalniki

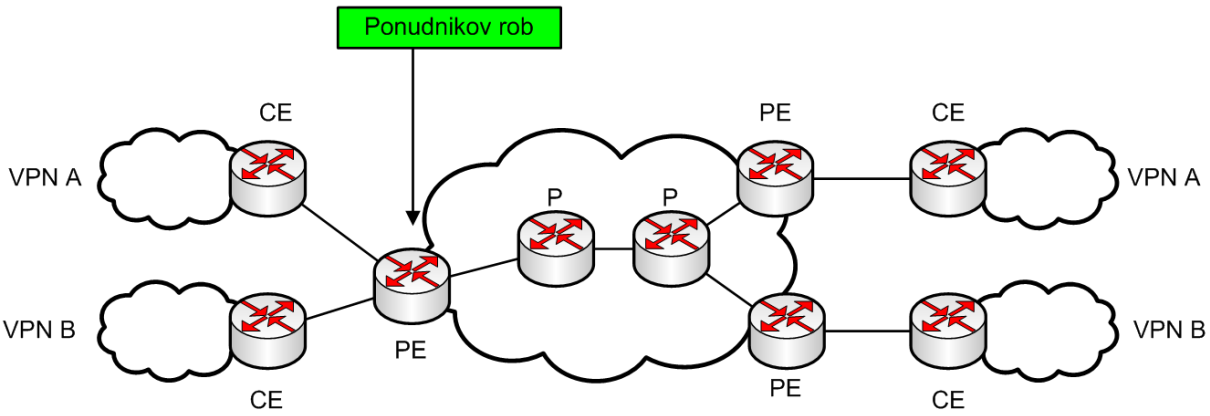
Uporabniške robne usmerjevalnike CE (
Slika 29) nadzorujejo uporabniki sami. Bistveno je, da so ti usmerjevalniki lahko preprosti, ker jim ni potrebno podpirati protokola MPLS.



Slika 29: Uporabniški robni usmerjevalniki CE

6.2.2. Ponudnikovi robni usmerjevalniki

Ponudnik storitve VPN ima na robu svojega omrežja vgrajen robni usmerjevalnik PE (Slika 30). To je demarkacijska točka med ponudnikom in uporabnikom te storitve. Na tem usmerjevalniku se zaključujejo povezave uporabniških robnih usmerjevalnikov. Tu so shranjene vse informacije v zvezi z uporabniki in zapisane informacije o povezavah do uporabnika, kakšen je njegov naslovni prostor, preko katerih usmerjevalnih protokolov bo usmerjevalnik komuniciral z usmerjevalnikom CE.



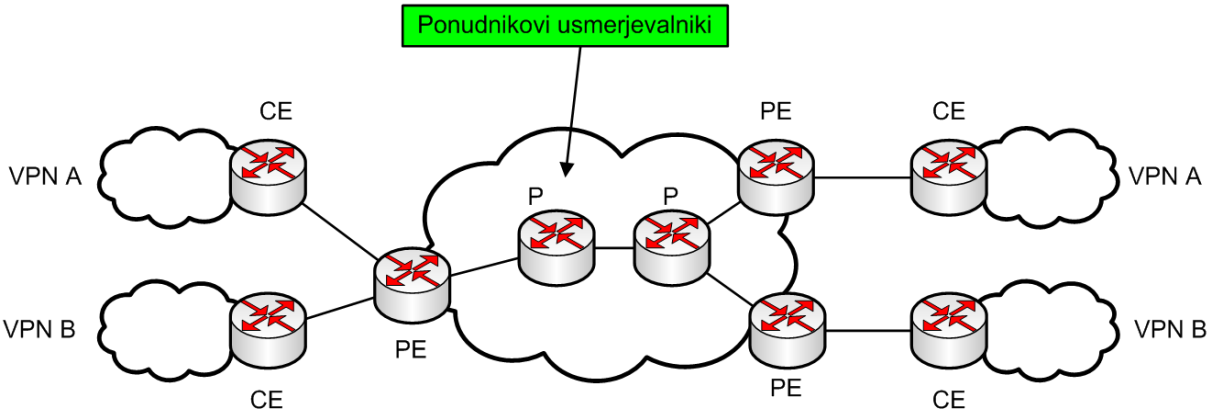
Slika 30: Ponudnikovi robni usmerjevalniki

Osnova za delovanje usmerjevalnika je zapis usmerjevalne tabele. Poleg te se na usmerjevalniku PE za vsak VPN posebej ustvari ločena tabela za usmerjanje in posredovanje

imenovane VRF (VPN Routing and Forwarding). Tabele VRF spadajo v kontrolno ravnino omrežja VPN.

6.2.3. Ponudnikovi usmerjevalniki

Ponudnikovi usmerjevalniki se nahajajo v ponudnikovem hrbteničnem omrežju (Slika 31). Njihova vloga je hitro posredovanje podatkov med usmerjevalniki PE in ne vzdržujejo posebnih zapisov o omrežjih VPN. V primeru komunikacije med dvema lokacijama omrežja VPN se podatki prenašajo skozi hrbtenične usmerjevalnike P.

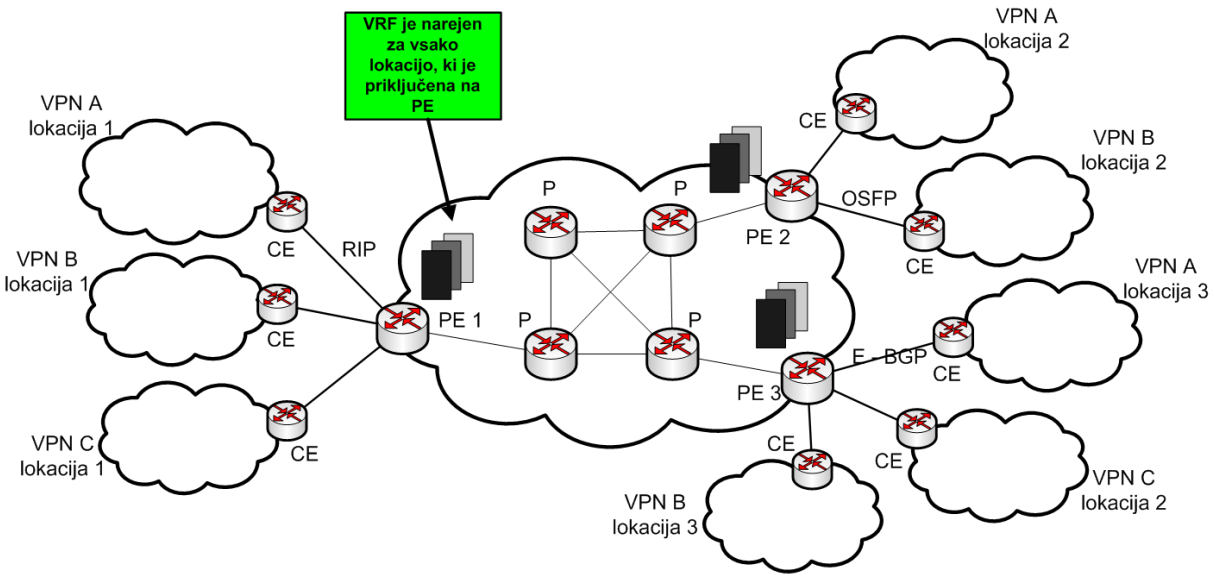


Slika 31: Ponudnikovi usmerjevalniki

6.3. Usmerjevalne in posredovalne tabele

Pri omrežjih VPN se na OSI nivoja 3 shranjujejo tabele VRF za vsako stranko posebej. To pomeni, da se naslovni prostor IP lahko prekriva oziroma podvaja.

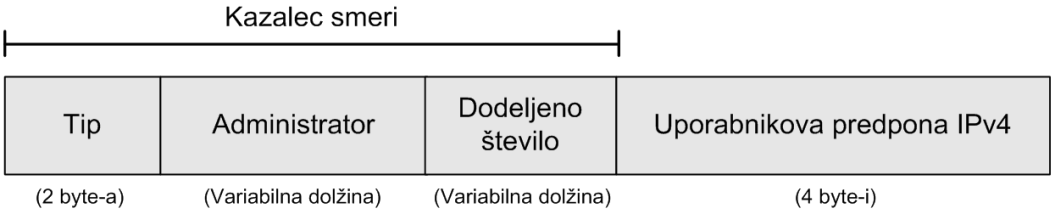
Slika 32 prikazuje tri VPN stranke: A, B in C, ki so priklopljene na omrežje MPLS na več lokacijah. Z omrežjem L3VPN so stranke povezane preko različnih usmerjevalnih protokolov (BGP, OSPF, statične smeri in RIP) za izmenjavo usmerjevalnih informacij na relaciji PE CE. Preko teh protokolov se prenašajo informacije o omrežjih, ki so prisotna na različnih lokacijah VPN strank. Na ta način lahko lokacije medsebojno komunicirajo.



Slika 32: Tabele VRF

6.3.1.1 Nova družina naslovov IPv4

Za omrežja VPN je bil ustvarjen nov naslovni prostor VPN IPv4. Naslovni prostor ima dodan kazalec smeri, ki določa kateremu VPN omrežju pripada (Slika 33).



Slika 33: Družina naslovov IPV4 VPN

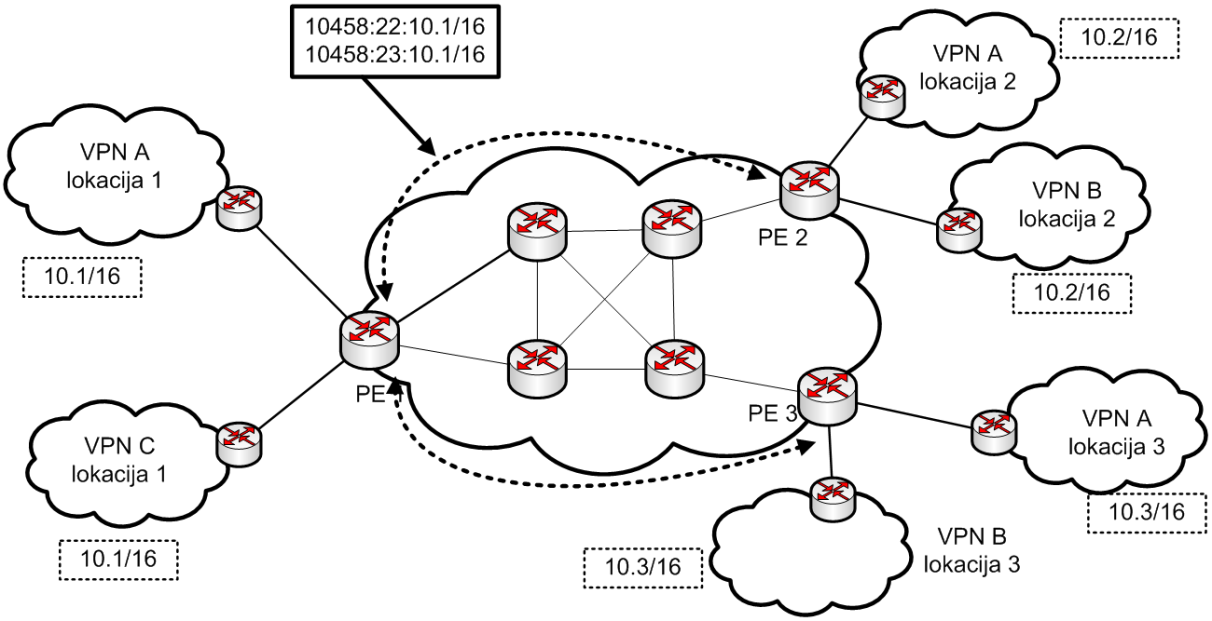
Družina naslovov podpira uporabo privatnega naslovnega prostora IP in tudi prekrivanje uporabnikove predpone. To v praksi pomeni, da lahko naročniki storitve sami izbirajo med javnimi ali privatnimi naslovnimi prostori. Več naročnikov ima lahko tudi isti naslovni prostor.

Za prenos smeri je tu uporabljen razširjen protokol BGP z imenom MP-BGP (RFC 2283). Nov naslovni prostor je uporabljen samo v kontrolni ravnini, uporabnik storitev ne čuti teh dodatkov. V podatkovni ravnini se prenašajo normalni IP paketi.

6.4. Uporaba kazalnikov smeri

Prekrivanje IP naslovov

V omrežjih VPN je omogočeno prekrivanje naslovov IP. To dosežemo z uvedbo kazalnikov smeri, ki jih uporabljajo usmerjevalniki PE. Na ta način ločimo smeri med omrežji VPN. Slika 34 prikazuje prekrivanje IP naslovov posameznih VPN strank. Smerem so dodane vrednosti kazalnikov: 10458:22 in 10458:23, zato lahko VPN A uporablja na lokaciji 1 enak naslovni prostor kot VPN C. Tudi v primeru, da so naslovni prostori različni, se smerem še vedno dodajo različni kazalniki.



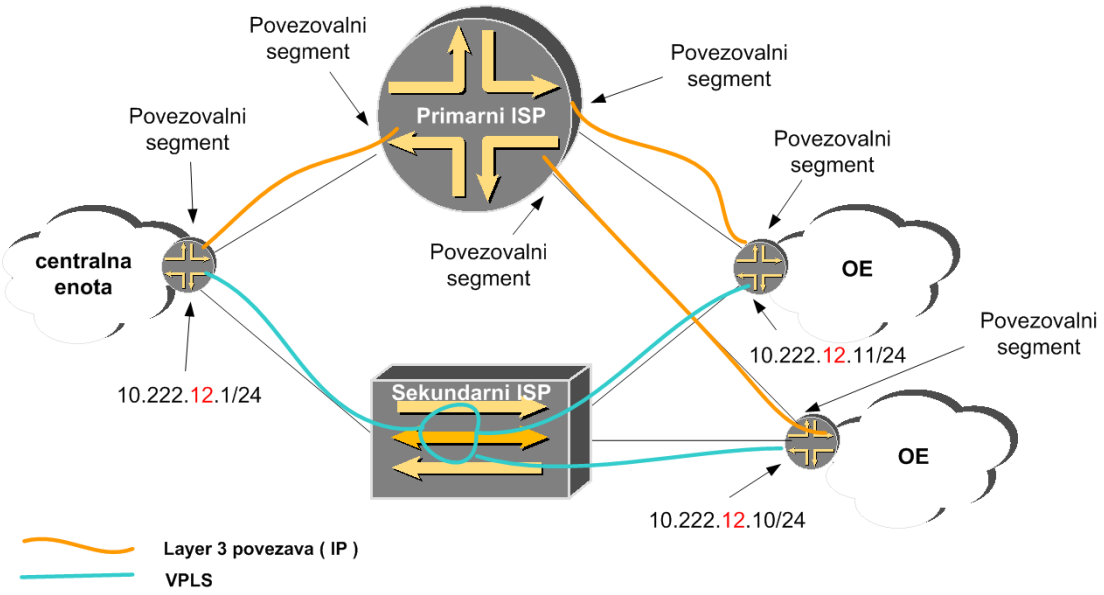
Slika 34: Uporaba kazalnikov smeri

6.5. VPLS

Za delovanje omrežja z dvema ali več usmerjevalniki je potrebno imeti delujoč protokol IGP. Na osnovi tega protokola deluje protokol BGP, ki ga je potrebno razširiti v večprotokolni BGP in vključiti protokol MPLS. Vsi ti protokoli so nato osnova za konfiguriranje storitve VPLS. Ravno tako na tej osnovi delujejo druge storitve, kot je na primer L3VPN.

Kot že kratica VLS (Virtual Private LAN Service) pove, je to virtualno omrežje, vendar za razliko od L3VPN na OSI nivoju 2. Torej se na usmerjevalnikih PE konfigurirajo pristopne povezave v to storitev. Največkrat so pristopne povezave tipa ethernet, ki so virtualno razdeljene v lokalna omrežja VLAN. Omrežje VLAN je delitev ethernet povezave v več navideznih povezav. V glavo ethernet paketa se doda še vrednost VLAN-ID v velikosti 4 oktetov. Naprave na obeh straneh povezave nato preko vrednosti ID ugotovita, kateremu omrežju VLAN pripada paket in s tem tudi, v kateri VPLS je ethernet paket namenjen.

Omrežje se proti naročniku obnaša kot ethernet stikalo, ki se razteza na več koncev omrežja operaterja. Slika 35 prikazuje storitvi L3VPN in VPLS, ki jih nudita dva ponudnika internetnih storitev.



Slika 35: Primer uporabe omrežij VPN

Razlika med storitvama je v tem, da se omrežje ponudnika storitev obnaša kot virtualni usmerjevalnik. Pri storitvi VPLS se ISP proti stranki predstavlja kot virtualno stikalo. Pri L3VPN se morata tako ISP kot tudi njegov naročnik domeniti za povezovalne segmente. To so lahko kakršnikoli naslovi IP, tudi privatni. Pri storitvi VPLS pa ima naročnik proste roke pri izbiri naslovov IP.

Kot dodatno storitev, ki je trenutno dostopna na trgu, lahko omenimo še storitev nudenja ethernet povezav z omrežjem VLAN. Ta omrežja so osnovana na stikalih, ki se nahajajo na celotnem omrežju ponudnika in preko katerih se lahko konfigurirajo obročno zaščitene ethernet storitve.

Potrebno se je zavedati razlik med storitvami, ki jih prikazuje spodnja tabela:

Storitev	L3VPN	VPLS	VLAN
OSI	3	2	2
MPLS	DA	DA	NE
Zaščita <50ms	DA, MPLS	DA, MPLS	DA, EAPS
QoS	DA	DA	DA
Prometni Inženiring	DA	DA	NE
Zaščita pred zankami	DA	NE	NE
Infrastruktura	Usmerjevalniki	Usmerjevalniki	Stikala
Preverjanje delovanja	MPLS ping, L3 tabele	MPLS ping	Na vmesnikih

Tabela 1: Primerjava storitev: L3VPN, VPLS in VLAN

Vrstica OSI govori o nivoju, na katerem je storitev nudena stranki. Druga vrstica pove, ali storitev za svoje delovanje kot osnovo uporablja protokol MPLS. Storitve so lahko zaščitene z

različnimi obročnimi tehnologijami, ki omogočajo izpadne čase pri preklopih pod 50 ms, kar je primerljivo s tehnologijo SDH. Prometnega inženiringa ne omogoča le storitev VLAN, kar v praksi pomeni, da ni mogoče zadovoljivo preusmerjati določenih prometnih tokov. Zaščito pred zankami (Loop) omogoča le storitev L3VPN.

7. Trendi razvoja protokola MPLS in storitev VPN

7.1. Naslednja generacija storitve MVPN

7.1.1. Uvod

Aplikacije za oddajanje več prejemnikom potrebujejo navidezna omrežja. Omrežje je potrebno virtualno razdeliti za potrebe ponudbe različnih poslovnih modelov. Ponudniki storitev uvajajo nov pristop k implementaciji omrežja VPN za oddajanje več prejemnikom. Zato izvajajo nadgradnjo obstoječih omrežij VPN z naslednjo generacijo omrežij NG-MVPN (Next Generation Multicast VPN).

Količina prometa za oddajanje več prejemnikom se je v zadnjem času povečala zaradi uporabe aplikacij, ki temeljijo na video prometu. Video promet pa zahteva storitev L3VPN, ki omogoča hkratno oddajo več prejemnikom. Trenutno dobro delujejo le omrežja L3VPN, ki pa omogočajo promet le za oddajo enemu prejemniku. Standard za to storitev je RFC2547, v zadnjem času ga nadomešča standard RFC 4364.

Trenutno se za zagotavljanje storitve prenosa video prometa uporabljajo storitve na OSI nivoju 2, kot je na primer VLAN. Ti dve storitvi pa nista razširljivi. Tudi v finančnem sektorju se tudi pojavlja potreba po prenosu vsebin za oddajo več prejemnikom. Na primer borzni posredniki po vsem svetu želijo vsi istočasno (z zakasnitvijo nekaj ms) prejeti informacije o spremembah borznih podatkov.

Ponudniki storitev nudijo še druge storitve, ki tudi temeljijo na protokolu MPLS: L2PVN, VPLS, L3VPN, IPv4, IPv6, unicast ter multicast. Tu se pojavi izziv, kako poleg teh storitev, brez vnosa dodatnih kontrolnih protokolov in nivojev dodatno zagotoviti še omrežja MVPN (Multicast VPN) za hkratno oddajo več prejemnikom.

7.1.2. Osnovni model delovanja MVPN

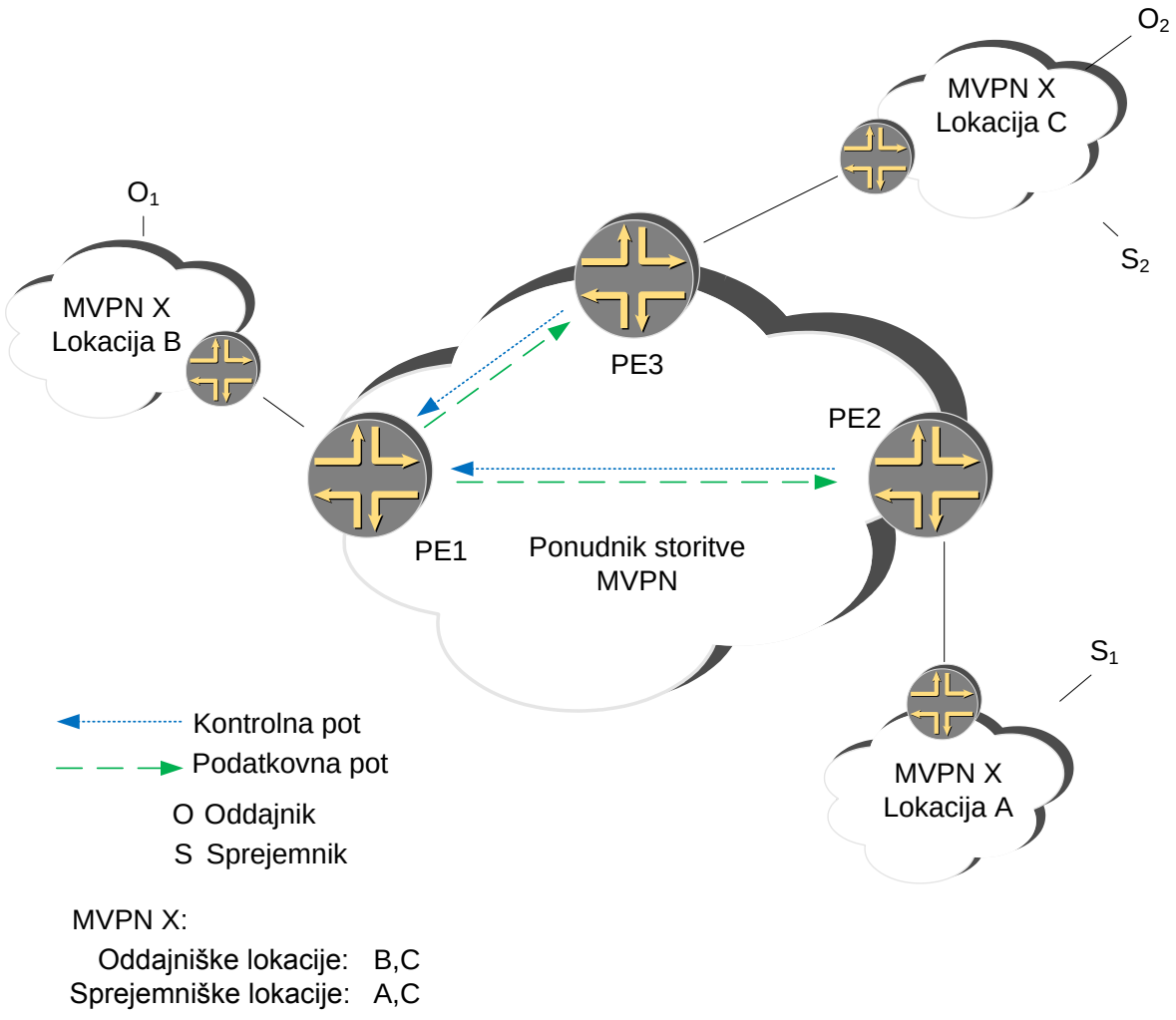
Pri virtualnih omrežjih MVPN je potrebna nova kontrolna ravnina za prenos usmerjevalnih informacij za hkratno oddajo več prejemnikom. Te informacije se prenašajo od izvorov do prejemnikov podatkov, pri čemer so oboji priklopljeni na usmerjevalnike PE.

Prav tako je potrebna podatkovna ravnina za prenos samih video podatkov (video stream). Te informacije se prenašajo od usmerjevalnikov PE, kjer so priklopljeni izvori do usmerjevalnikov PE, kjer se nahajajo prejemniki. Podatki se torej prenašajo od izvora skozi omrežje do prejemnikov.

Različna omrežja MVPN lahko pri svojem delovanju uporabljajo enak naslovni prostor, ki je definiran v standardu RFC 1918, vključno z naslovnim prostorom za oddajanje več prejemnikom. Najbolj elegantno bi bilo, če bi za ločevanje smeri uporabljali enak mehanizem ločevanja usmerjevalnih smeri (route distinguisher), kot je to na primer pri RFC 2547.

7.1.3. Primer delovanja omrežja MVPN

Slika 36 prikazuje primer storitve MVPN. Kontrolna ravnina poteka od usmerjevalnikov PE povezanih na sprejemnike (lokacija A in C) do usmerjevalnikov PE, kjer so priključeni oddajniki (lokacija B in C). Podatkovna ravnina poteka od usmerjevalnikov PE, povezanih na oddajnik (lokacija B in C), do usmerjevalnikov PE, povezanih na prejemnike (lokacija A in C). Na lokaciji C se nahajata tako sprejemnik kot oddajnik.



Slika 36: Primer modela MVPN

7.1.4. Izzivi obstoječih omrežij VPN

Standard Draft Rosen (D-ROSEN) za storitev L3VPN za oddajo več prejemnikom temelji na delitvi v virtualne usmerjevalnike. Model uporablja PIM-SM za izmenjavo informacij v kontrolni ravnini. Če uporabnik omrežja VPN uporablja protokol PIM za storitev oddaje več uporabnikom (multicast), se uporabniška sporočila PIM (join/prune) prenašajo med usmerjevalniki CE in PE. Nato usmerjevalnik PE sporočila prenese znotraj omrežja VPN do ostalih usmerjevalnikov PE s pomočjo sej PIM tipa točka-točka oziroma PE-PE. Za prenos informacij vzpostavljajo usmerjevalniki PIM seje do vsakega usmerjevalnika PE, ki je

vključen v omrežje MVPN, kar predstavlja velik problem pri razširljivosti rešitve. Na primer pri 1000 omrežjih MVPN na enem usmerjevalniku PE s 100 lokacijami, bi bilo potrebno na vsakem usmerjevalniku PE vzpostaviti 100.000 povezav s sosedi. Rezultat tega bi bil, da bi vsak usmerjevalnik PE moral procesirati 3300 pozdravnih sporočil PIM na sekundo.

V primeru, da ponudnik vzpostavi protokol P-PIM (Provider PIM), se podatkovni promet posreduje preko tunelov GRE. Enkapsulacija GRE omogoča ustvarjanje tunelov v omrežjih IP. Po teh tunelih se lahko vzpostavljajo povezave različnih usmerjevalnih protokolov, kot so na primer OSPF, BGP in drugih. Normalno preko omrežja IP ni možno vzpostavljati teh povezav. V glavi tunela GRE je uporabljen naslovni prostor za oddajo več uporabnikom in ta prostor določi ponudnik storitve.

Vzpostavljanje storitev VPN na takšen način prinaša s seboj omejitve oziroma probleme pri skaliranju rešitve. Ponudnik mora vzdrževati dva mehanizma za vzpostavljanje storitev VPN: unicast in multicast. Pri organizaciji IETF zato trenutno potekajo pogajanja o naslednji generaciji privatnih omrežij: NG-MVPN.

7.1.5. Princip delovanja NG MVPN

V standardu za NG MVPN je v kontrolni ravnini uporabljen protokol BGP, enako je pri obstoječih omrežjih VPN za oddajo enemu prejemniku. Pri storitvi NG MVPN so od omrežij VPN za oddajo enemu prejemniku prevzeli dve bistveni lastnosti:

1. Za vzpostavljanje storitev oddaje več prejemnikom in prenos usmerjevalnih informacij je uporabljen protokol BGP. To omogoča ponudnikom storitev, da uporabijo obstoječe znanje od omrežij VPN za oddajo enemu prejemniku,
2. Za prenos uporabniških smeri C (Customer multicast routes) je uporabljen protokol BGP. Na ta način je lahko kontrolna ravnina fizično ločena od podatkovne. To omogoča uporabo novih tehnologij, kot so poti LSP za oddajo več prejemnikom PTMP (Point To Multipoint).

Kontrolna ravnina NG MVPN podpira fleksibilne topologije kot je »hub and spoke«, ter novo verzijo IP protokola IPv6. IPv6 NG MVPN nudi možnost podpore enkapsulaciji MPLS za vzpostavljanje oddaje več uporabnikom za protokol IPv6. Pri IPv6 NG MVPN je uporabljen enak model kot pri IPv6 VPN za oddajo enemu uporabniku RFC 4659 (RFC4659). Na tak način obstaja možnost enostavnega prehoda med omrežji IPv4 in IPv6 VPN za oddajo več uporabnikom. Omrežja BGP MVPN nudijo možnost priklopa več izvornih strežnikov za oddajo več uporabnikom (multi homing multicast) na različne usmerjevalnike PE. V primeru odpovedi enega strežnika, je preklop na redundantni strežnik v času pod 1 sekundo. Avtomatično zaznavanje sosedov MVPN deluje prav zaradi pristopa s protokolom BGP in omogoča enostavno dodajanje usmerjevalnikov PE ter avtomatično vzpostavljanje ponudnikovih tunelov za podatkovni prenos MVPN med usmerjevalniki PE.

	DRAFT-ROSEN	NG MVPN
Transport	PIM-SM GRE	Uporabi se lahko različne tunelske tehnologije (P2MP MPLS ali PIM-SM GRE)
Signalizacija	PIM	BGP, enak model kot pri L3VPN za oddajo enemu uporabniku. Podpira avtomatsko zaznavanje smeri.
Signalizacijske seje PE-PE	V vsaki storitvi VRF potrebuje vsak PE ločeno sosedstvo PIM z vsakim oddaljenim usmerjevalnikom PE.	Vsak PE uporablja že obstoječe interne seje BGP med usmerjevalniki PE.
Združevanje VPN prometa	Ni možnosti združevanja storitev MVPN v en tunel med usmerjevalniki PE.	Z uporabo poti P2MP LSP je možno združiti oddaj več uporabnikom tipa (S,G).

Tabela 2: Primerjava storitev VPN

7.2. Naslednja generacija storitve VPLS

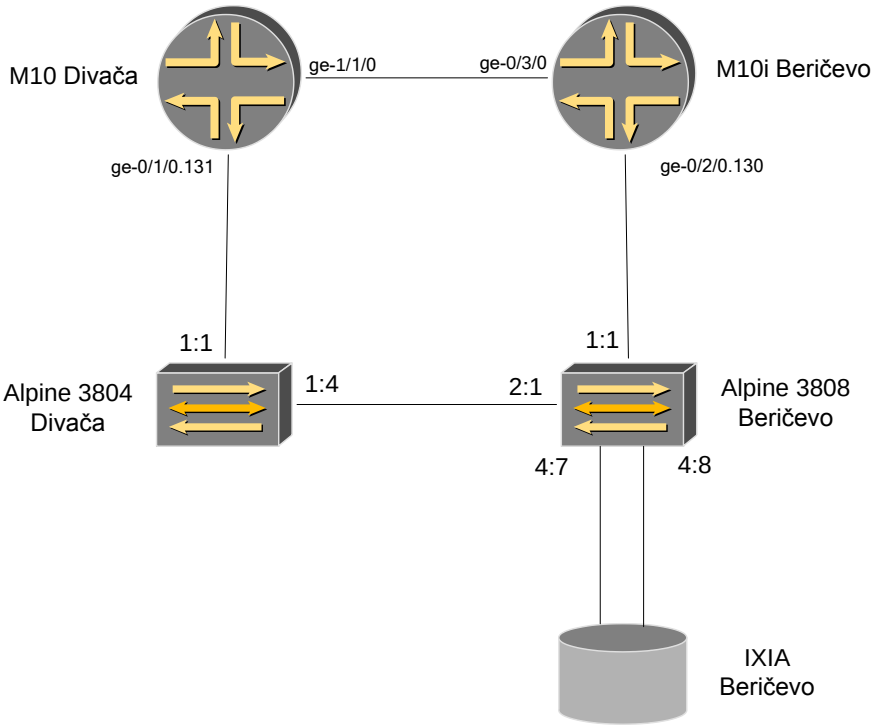
VPLS je ključna storitev, ki se trenutno trži s strani ponudnikov storitev. Nujno mora torej ta storitev podpirati prenos oddaje več uporabnikom. Delitev IP paketov se izvaja pri storitvi VPLS na vhodu v omrežje. To ni najbolj optimalna rešitev, ker se po omrežju VPLS prenašajo podvojeni paketi. Uporaba poti P2MP LSP v omrežjih BGP VPLS dovoljuje delitev v notranjosti omrežja na začetku vej drevesa za oddajo več uporabnikom. Na ta način se skozi omrežje ne prenašajo podvojeni paketi.

8. Merjenje zakasnitve storitve L3VPN

8.1. Opis preizkusnega omrežja

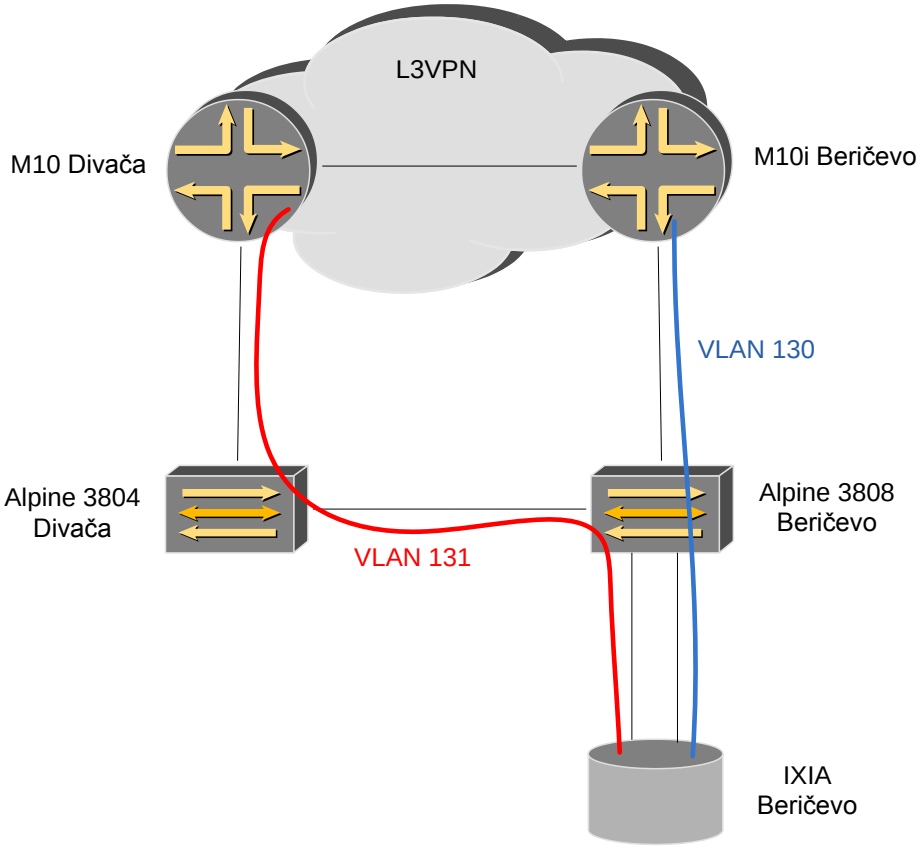
Preizkusno omrežje (Slika 37) je bilo sestavljeno iz dveh stikal ter dveh usmerjevalnikov. Stikala Extreme Networks Alpine 3808 se je uporabilo kot pristop do usmerjevalnikov Juniper M10 ter M10i. Fizične povezave so bile tipa ethernet in vzpostavljene s hitrostjo 1 Gbit/s. Med Ljubljano in Divačo so se uporabili štirje optični vodniki, po dva za vsako ethernet povezavo. Vzpostavili sta se dve storitveni povezavi:

- M10i Beričevo – M10 Divača
- Alpine 3808 Beričevo – Alpine 3808 Divača



Slika 37: Vzpostavljanje transportne povezave

Na usmerjevalnikih je bil vzpostavljen L3VPN (RFC2547). Stikala so zagotavljala posredovanje ethernet paketov preko omrežij VLAN (130 in 131) do L3VPN (Slika 38). Na usmerjevalnikih Juniper se je usmerjalo IP pakete skozi L3VPN omrežje. Omrežje se je raztezalo od Ljubljane do Divače. Merilna oprema IXIA se je nahajala v Ljubljani.



Slika 38: Logična shema preizkusnega omrežja

8.2. Spisek merilne opreme

V preizkusu so bile uporabljene naslednje naprave in moduli:

- Merilna naprava IXIA
- Šasija IXIA 400T (SN: 400T-1241148)
- Modul LM1000STXS4 (SN: 033554)
- Programska oprema: IXOS 4.10.250.28, strežnik: 4.10.250.28, HAL: 2495
- Usmerjevalnik Juniper Networks model M10 (Divača)
- Stikalo Extreme Networks model Alpine 3804 (Divača)

8.2.1. Opis ter konfiguracija usmerjevalnika Juniper M10 in M10i

Usmerjevalnik M10 je deloval z različnimi protokoli z usmerjevalnikom M10i, ki so osnova za vzpostavitev L3VPN in sicer:

- OSPF,
- BGP in

- MPLS.

Vzpostavljanje sejnih povezav teh protokolov zagotavlja transportno osnovo za vzpostavitev storitve L3VPN. VPN se konfigurira kot usmerjevalna instanca, ki ima svojo usmerjevalno in posredovalno tabelo VRF ustvarjeno samo za ta VPN. Del konfiguracije omrežja VPN na usmerjevalniku M10, ki je podobna tudi na M10i:

```
sc@DIVRTPR1> show configuration routing-instances L3VPN-test
instance-type vrf;
interface ge-0/1/0.131;
route-distinguisher 65000:401;
vrf-import L3VPN-test-imp;
vrf-export L3VPN-test-exp;
sc@DIVRTPR1>
```

Tip instance v zgornji konfiguraciji je VRF, kar pomeni usmerjanje in posredovanje za virtualno privatno omrežje (VPN routing and forwarding). V ta VPN (Slika 37) je vključen vmesnik ge-0/1/0.131, ki je tipa gigabit ethernet v reži 0, kartica je na prvem mestu in uporabljena so vrata 0 (0/1/0). To je fizični vmesnik, iz katerega je uporabljen VLAN 131 in samo v ta VLAN je vključen omenjeni L3VPN. Vrednost kazalnika smeri je 65000:401. Kot vhodna politika je uporabljena politika z imenom »L3VPN-test-imp«, izhodna politika je »L3VPN-test-exp«.

8.2.2. Opis in konfiguracija stikala Extreme Alpine 3808

Na obeh stikalih sta bila konfigurirana omrežja z vrednostmi VLAN-id 130 in 131. Stikala sta v tem primeru zagotavljala posredovanje ethernet paketov, ki jih je na eni strani generirala IXIA, na drugi pa usmerjevalnika JUNIPER.

8.2.3. Merilna naprava IXIA

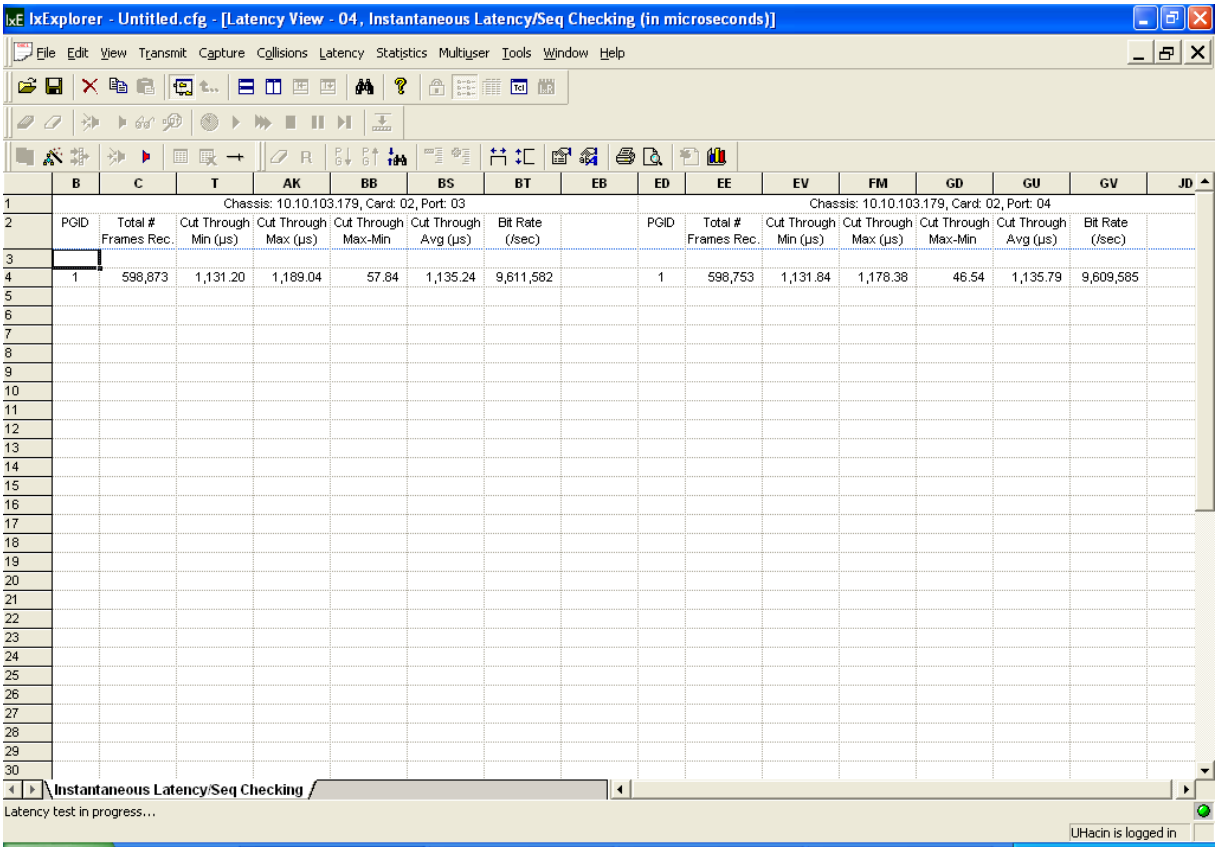
Merilna naprava IXIA omogoča generiranje prometnih tokov IP in analizo različnih parametrov dospelih IP paketov. Med glavne lastnosti spadajo vmesniki oziroma hitrosti s katero lahko generira in analizira vsak IP paket. V merilno napravo IXIA se lahko vgradi vmesnike hitrosti 1Gbit/s. Pri tem lahko vsakemu paketu oziroma toku paketov nastavljamo različne parametre kot so: naslovi IP, naslovi MAC, bite TOS, dodajamo jim sekvenčne in časovne vrednosti. IXIA nato s pomočjo vgrajenih procesorjev tipa FPGA v realnem času analizira vrnjene IP pakete.

8.3. Rezultati meritve

Kot rezultat meritve je podana povprečna zakasnitev IP paketa skozi celotno preizkusno omrežje, merjena v času 5 minut pri prometnem toku 10Mbit/s z velikostjo paketov 500 oktetov. Dodatno je izmerjena razlika med največjo ter najmanjšo zakasnitvijo.

Rezultati meritve (Slika 39: Izpisek iz merilne naprave IXIA):

- Zakasnitev na celotni poti: **1,135 ms**.
- Razlika med največjo in najmanjšo zakasnitvijo: **57,84 µs**.



Slika 39: Izpisek iz merilne naprave IXIA

Te vrednosti kažejo na zelo majhen vpliv usmerjevalnikov, stikal in optičnih povezav na sam prometni tok. Za primerjavo lahko te vrednosti primerjamo z zahtevami za VoIP, pri katerem se mora časovna zakasnitev na prenosu gibati znotraj področja 200ms.

9. Sklep

V praksi se je protokol MPLS že izkazal za zelo uporabnega in ga v polni meri uporabljajo ponudniki internetnih storitev. Uporablja se za storitve L3VPN in VPLS. Poleg tega se lahko uporabi tudi za preusmerjanje vsega prometa, kot je internetni, VoIP ter VIDEO preko IP. V tem primeru se MPLS uporabi kot varovanje primarnih poti in hitrih preklopov (< 50ms) na obhodne poti v primeru izpadov primarnih. Pri praktičnem primeru merjenja storitve L3PVN se je izkazalo, da vnos približno 1ms dodatne zakasnitve in ne prevelikega trepetanja IP paketov ne vnaša prevelikih sprememb v paketna omrežja.

10. Literatura

[CSCO] Cisco Systems, Inc., (2007). Cisco RAN Optimization Solution for GSM and UMTS Backhaul Optimization: Apps. [online]. [citirano 17. dec. 2009; 12:21]. Dostopno na spletnem naslovu: http://www.cisco.com/en/US/solutions/collateral/ns341/ns523/ns675/ns329/net_brochure0900aecd8032c191.html

[JNPR] Juniper Networks, Inc. (2008).JUNOS™ Software.[online].[citirano 12. okt 2009; 17:20] Dostopno na spletnem naslovu: http://www.juniper.net/techpubs/software/junos/junos91/swconfig-vpns/frameset.html

[JNPRDOC] Juniper Networks, Inc. (2008). JUNOS 9.1 : Software Documentation. [online]. [citirano 11. sep 2009; 17:20]. Dostopno na spletnem naslovu: http://www.juniper.net/techpubs/software/junos/junos91/index.html

[MPLSEA] Lucek, Julian in Minei, Ina: MPLS-Enabled Applications, 1. Ponatis. Apr. 2006, Anglija : John Wiley@ Sons, Ltd, 2005

[MPLSRFC] Rosen, E., Viswanathan, A. in Callon, R. (2001): RFC 3031: Multiprotocol Label Switching Architecture.[online].[citirano 17. dec. 2009; 13:26]. Dostopno na spletnem naslovu: http://www.ietf.org/rfc/rfc3031.txt.

[JNCIP] Reynolds, Harry: JNCIP Juniper Networks Certified Internet Professional : Study Guide, Anglija : Sybex Inc., 2003.

[JNCIS] Soricelli, Joseph: JNCIS Juniper Networks Certified Internet Specialist : Study Guide, Anglija: Sybex Inc., 2004.

[D-ROSEN] Rosen, Eric, Cai, Yiqun in Wijnands, Ijsbrand (2004): Multicast in MPLS/BGP IP VPN's.[online].[citirano 29.12.2009;10:24].Dostopno na spletnem naslovu: http://tools.ietf.org/html/draft-rosen-vpn-mcast-08.

[RFC4659] Clercq,J.,Ooms,D.,Carugi,M. in Faucheur,F.(2006): RFC 4659: BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN.[online].[citirano 29. dec. 2009;10:30].Dostopno na spletnem naslovu: http://www.ietf.org/rfc/rfc4659.txt.

11. Izjava

Izjavljam, da sem magistrsko nalogo samostojno izdelal pod vodstvom mentorja Prof. dr. Saša Tomažiča. Izkazano pomoč drugih sem v celoti navedel v zahvali.