UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

ALJAŽ VAJDA

PROTOKOL MULTICAST V NAVIDEZNEM ZASEBNEM OMREŽJU Z VIDIKA INTERNETNEGA PONUDNIKA

DIPLOMSKO DELO VISOKOŠOLSKEGA STROKOVNEGA ŠTUDIJA

MENTORICA: DOC. DR. MOJCA CIGLARIČ

LJUBLJANA, 2009

ZAHVALA

Zahvaljujem se vsem, ki so v kakršni koli obliki pripomogli k nastanku moje diplomske naloge.

Zahvalo za pomoč in nasvete bi prvo namenil mentorici doc. dr. Mojci Ciglarič ter delovnem kolektivu – IP oddelku na Telekomu Slovenije. Zahvaljujem se sodelavcem: šefu mag. Alešu Vodopivcu, Petru Grošlju, mag. Matjažu Pučku, Mitju Jenčku, Saši Vukomanoviču, Miroslavu Đošiću, Boštjanu Jakiju, mag. Tomislavu Bercetu ter ostalim.

Posebna zahvala gre mojim staršem – mami Adrijani ter očetu Bojanu za finančno podporo in spodbujanju k dokončanju študija. Zahvaljujem se še prijateljem: Heleni Žagar, Mihi Colnerju, Mateju Hočevarju, Janezu Bartolo, ter ostalim.

KAZALO / CONTENTS

KAZALO SLIK

POVZETEK

V diplomski nalogi bom predstavil izvedbo oddajanja več prejemnikom hkrati (v nadaljevanju multicast) z vidika internetnega ponudnika, ki implementira in omogoči svojim klientom (poslovnim strankam) možnost uporabe protokola multicast v njihovem navideznem zasebnem omrežju (VPN) preko hrbtenice svojega omrežja.

Po uvodnem poglavju, v katerem bom pojasnil problem, bom v drugem poglavju na hitro predstavil tri načine prenosa podatkov skozi omrežje s prednostmi in slabostmi uporabe vseh treh načinov. V tretjem poglavju preletimo IP-naslavljanje. Četrto poglavje bo malenkost bolj obsežno od prvih treh. V njem bomo spoznali zgradbo omrežja MBone, metodo RPF, zgradbo distribucijskih dreves (souporabniška drevesa, drevesa najkrajših poti, točko stičišča, drevo točke stičišča) in uporabo le-teh. Peto poglavje zajema usmerjanje multicast. Tukaj bom predstavil vse variante protokola PIM: PIM-Dense Mode, PIM-Sparse Mode, PIM-Source Specific Multicast in Bidirectional-PIM. Predstavil bom metodi poplavljanja (flooding) in obrezovanja (pruning) ter kje in kdaj se uporabljata. V šestem poglavju spoznamo internetni protokol za upravljanje skupin – IGMP. Predstavil bom strukturo protokola IGMPv3. Sedmo poglavje predstavlja protokol mejnih usmerjevalnikov – BGP, tukaj spoznamo strukturo omenjenega protokola (glavo paketa BGP, tipe sporočil). V osmem poglavju spoznamo multiprotokolno komutacijo z zamenjavo oznak – MPLS, zgradbo, usmerjanje protokola in prednosti njegove uporabe na omrežju internetnega ponudnika. V devetem poglavju bom predstavil navidezna zasebna omrežja – VPN, zgradbo in njihovo uporabo. Tukaj bomo spoznali uporabo VRF, ki je ključni protokol v VPN-tehnologiji, usmerjevalnik razločevalne smeri-RD, cilj usmerjanja-RT. Deseto poglavje zajema nadgradnjo VPN – Multicast VPN oziroma mVPN. Tu bom predstavil uporabo tega protokola v omrežju internetnega ponudnika, zakaj je smiselna implementacija protokola pri ponujanju storitev multicast klientom v njihovem VPN. Spoznali bomo izpeljavo VRF v multicast VRF – mVRF ter distribucijsko drevo multicast – MDT, ki je pomemben parameter znotraj protokola mVRF.

V praktičnem preizkusu bom implementiral mVRF na MPLS-omrežju. Uporabil bom dva računalnika, od katerih bo eden služil kot strežnik, na drugem pa bom simuliral omrežje hipotetičnega internetnega ponudnika. Omrežje bo zajemalo tri ponudnikove usmerjevalnike ter enega klientovega. Drugi računalnik bo tudi služil kot odjemalec. Po implementaciji in preizkusu delovanja bom predstavil razliko delovanja tehnologije multicast na ponudnikovem omrežju z uporabo mVRF ter brez njega. Spoznali bomo, zakaj je implementacija mVRF na ponudnikovem omrežju primerna, da ne rečem potrebna, če želimo ponujati to storitev podjetjem (*enterprise)*, ki imajo svojo navidezno privatno omrežje speljano preko hrbtenice omrežja internetnega ponudnika.

Ključne besede: multicast, unicast, PIM, MPLS, VPN, VRF, mVPN, mVRF, MDT.

ABSTRACT

In this diploma thesis I will present the implementation of multicast, from a point if view of the service provider, who implements and enable its clients (business customers) the possibility of using multicast protocol in their own virtual private network (VPN) through provider network backbone.

After the first chapter, in which I will introduce us with basis of this thesis, the second section will briefly present three methods to transfer data through the network with the advantages and disadvantages of all three methods. The third chapter overflies IP and multicast addressing. In fourth chapter we will learn about MBone network architecture, RPF method, building distribution trees (shared trees, shortest path trees, rendesvouz point, rendesvouz point tree) and use them. The fifth chapter covers the multicast routing. Here I will present all the variants of PIM protocol: PIM-Dense Mode, PIM-Sparse Mode, PIM-Source Specific Multicast and Bidirectional-PIM. I will introduced the flooding and pruning methods and where and when to apply them. In the sixth chapter we will get know Internet Group Managing Protocol - IGMP. I will introduce the structure of IGMPv3 protocol. The seventh section presents the border gateway protocol - BGP, here we get to know the structure of the mentioned Protocol (BGP header package, the types of messages). In the eighth chapter we will get known Multiprotocol Label Switching – MPLS protocol, its architecture, routing of the protocol and the advantages of its use on the Internet service providers network. In the ninth chapter I will present Virtual Private Networks - VPN, it's architecture and their use. We will learn about the use of Virtual Routing Forwarding -VRF, which is a key protocol in VPN technology, router-Route Distungusher – RD, Route Target-RT and so on. The tenth chapter covers upgrade of VPN into Multicast VPN - mVPN. Here I will present the usage of this protocol in the service provider's network, for a meaningful implementation of the protocol for providing multicast services to clients in their VPN. We will get to know the derivation of the VRF into multicast VRF - mVRF and multicast distribution tree - MDT, which is an important parameter within mVRF Protocol.

In practical test I will implement mVRF the MPLS network. I will use two computers, one of which will be used as server, and the second computer will simulate the hypothetical service provider. The second computer will also serve as a client. After the implementation and operation of the test, I will present the difference of multicast technology on service providers network with or without using mVRF. We will get to know why the implementation of mVRF on service provider network is adequate if we want to offer multicast VPN to the enterprises, which would run their multicast VPN over service provider backbone.

Keywords: Multicast, unicast, PIM, MPLS, VPN, VRF, mVPN, mVRF, MDT.

1 UVOD

V zadnjem desetletju smo bili priča drastičnem porastu pasovne širine, kar je pripeljalo k razširitvi ponudbe internetnih storitev in omogočilo ponudnikom, da se poleg interneta pričnejo ponujati tudi druge storitve, kot je na primer televizija na osnovi internetnega protokola ali IPTV. Skoraj vsi poznamo paketne ponudbe internetnih ponudnikov, kot so tako imenovani trojčki (internet, telefonija, televizija). Te storitve se največkrat ponujajo glavnini uporabnikov, ki jih imenujemo zasebni ali rezidenčni uporabniki.

Velik del zaslužka pa internetnim ponudnikom prinašajo poslovni uporabniki, ki imajo bistveno večje zahteve kot rezidenčni uporabniki. Veliki poslovni sistemi prek omrežja ponudnika internetnih storitev povezujejo svoje razpršene lokacije med seboj. Na primer: veliko trgovsko podjetje s sedežem v Ljubljani ima skoraj v vsakem večjem kraju svoje poslovalnice in te poslovalnice komunicirajo z glavno poslovno enoto preko navideznega zasebnega omrežja (v nadaljevanju VPN). Ta VPN se izvaja preko ponudnikovega internetnega omrežja. Ponudnik zagotavlja povezljivost, kot tudi usmerjanje (če imamo VPN na tretji plasti ali IP VPN), tako da je z vidika uporabnika to omrežje vidno kot veliko lokalno omrežje (LAN). Želja stranke je, da ji ponudnik zagotovi vse potrebne pogoje in tehnologije za normalno poslovanje. Ena izmed teh tehnologij je multicast. Slednje je tehnologija, na kateri med drugim deluje storitev IPTV zato jo ponuja vsak resni internetni ponudnik.

Stranka pa si morda želi pošiljati podatkovni tok multicast med dvema ali več lokacijami v svojem VPN. Na primer za potrebo videokonferenc ali za prenos podatkov pomembnih poslovnih aplikacij. Tudi večje borze opravljajo poslovanje v svojem navideznem zasebnem omrežju s pomočjo tehnologije multicast. To storitev imenujemo multicast VPN ali mVPN. Da ponudnik omogoči tak tip prenosa, mora na svojem omrežju (usmerjevalnikih) opraviti nekaj sprememb, s predpostavko, da ima na omrežju že omogočeno multicast ter VPN podporo. Storitev mVPN se izvaja na ponudnikovem omrežju, za usmerjanje in upravljanje pa skrbi ponudnik.

2 NAČINI PRENOSA PODATKOV SKOZI OMREŽJE

Poznamo tri načine prenosa podatkov skozi omrežje:

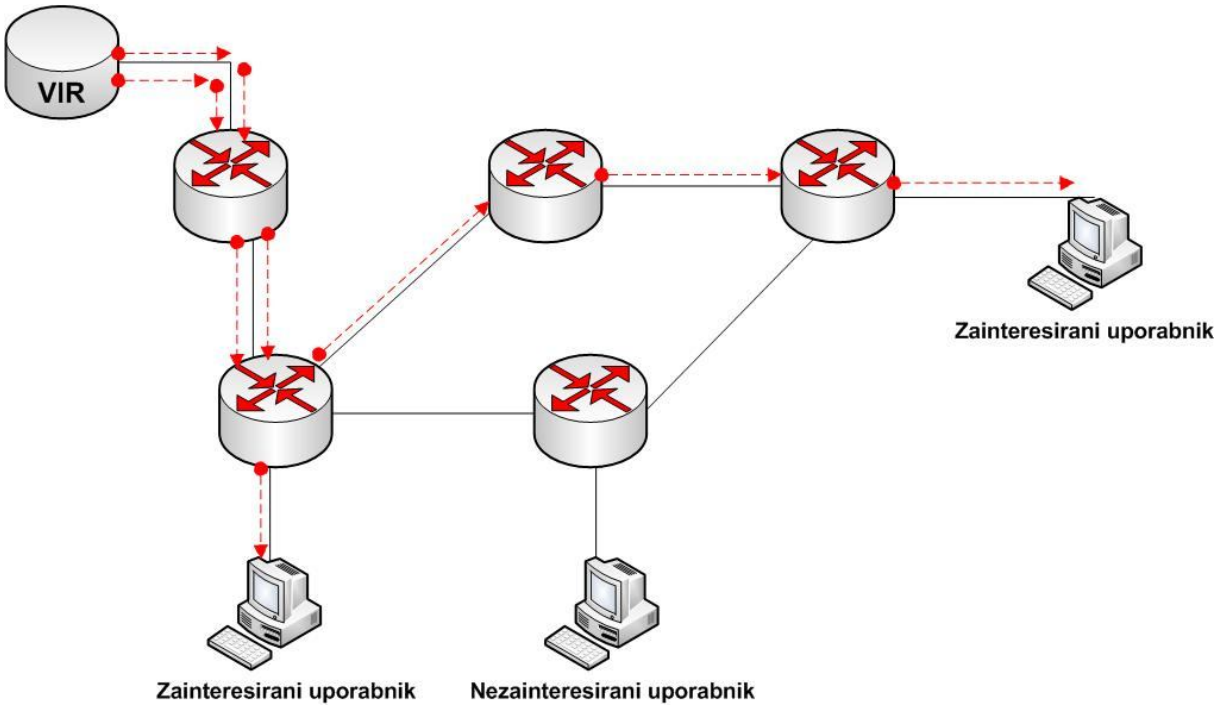
1. **Oddajanje enemu prejemniku (Unicast)** – prenos podatkov do določenega naslovnika preko dostave **»eden-do-enega«**.
2. **Razpršeno oddajanje vsem prejemnikom (Broadcast)** – prenos podatkov do vseh naslovnikov preko dostave **»eden do vseh«**.
3. **Oddajanje več prejemnikom hkrati (Multicast)** – prenos podatkov do zainteresiranih naslovnikov preko dostave **»eden-do-več«**.

Internet je bil prvotno zasnova na modelu unicast podatkovnega prenosa. Na žalost pa ta način ne omogoča nekaterih tipov prometa. Za razliko od modela unicast, ponuja multicast učinkovit način prenosa podatkov, ki ga lahko opredelimo kot **»eden-do-več«** ali **»več-do-več«**.

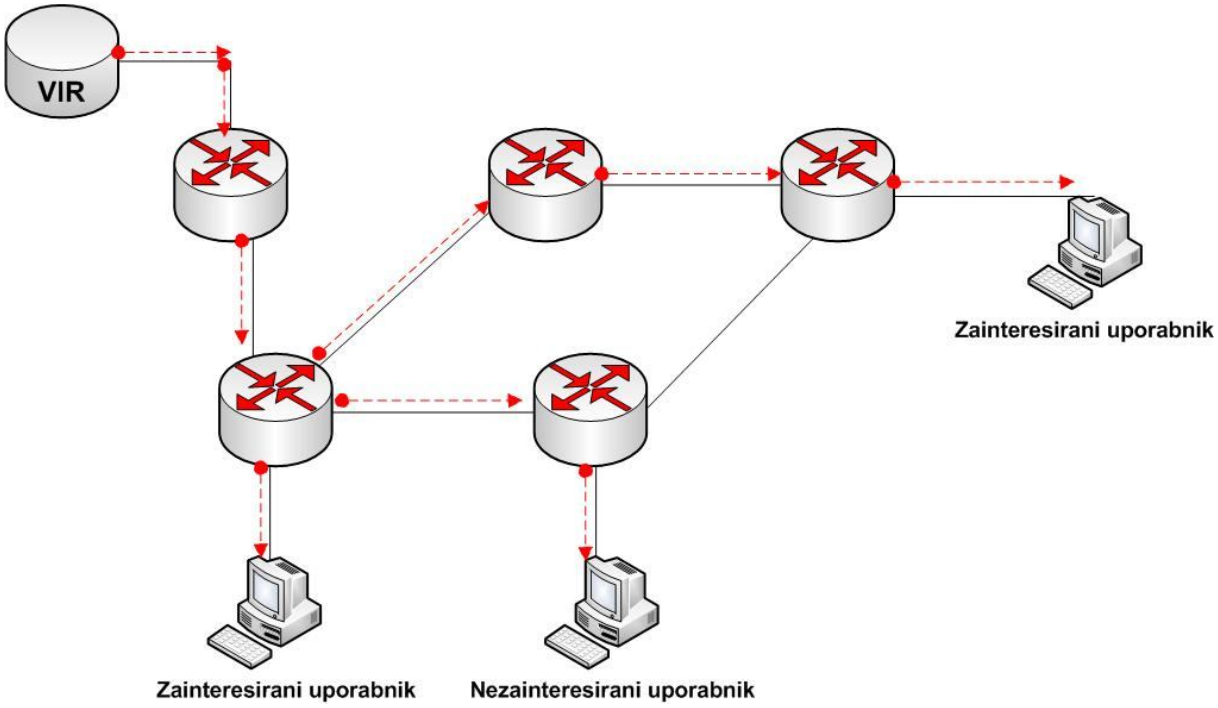
Radio in televizija sta dober primer prometa, ki ustreza »eden-do-več« načinu. Za prenos unicast bi morale radijske postaje vzpostaviti za vsakega naslovnika ločeno logično sejo, kar bi posledično pripeljalo do podvojitve ali pomnožitve oz. linearnega naraščanja prometa s strani strežnika do uporabnikov.

Pri načinu broadcast pošilja izvor tok paketov bodisi enemu ali več naslovnikom. Omrežje ta tok multiplicira in ga prenese tudi tistim naslovnikom, ki niso zainteresirani, zato je ta način dostave posledično neučinkovit na omrežjih, kjer je veliko nezainteresiranih naslovnikov. Povezava, ki povezuje nezainteresirane gostitelje, mora prenašati neželen promet, kar zasede prepotrebne omrežne vire.

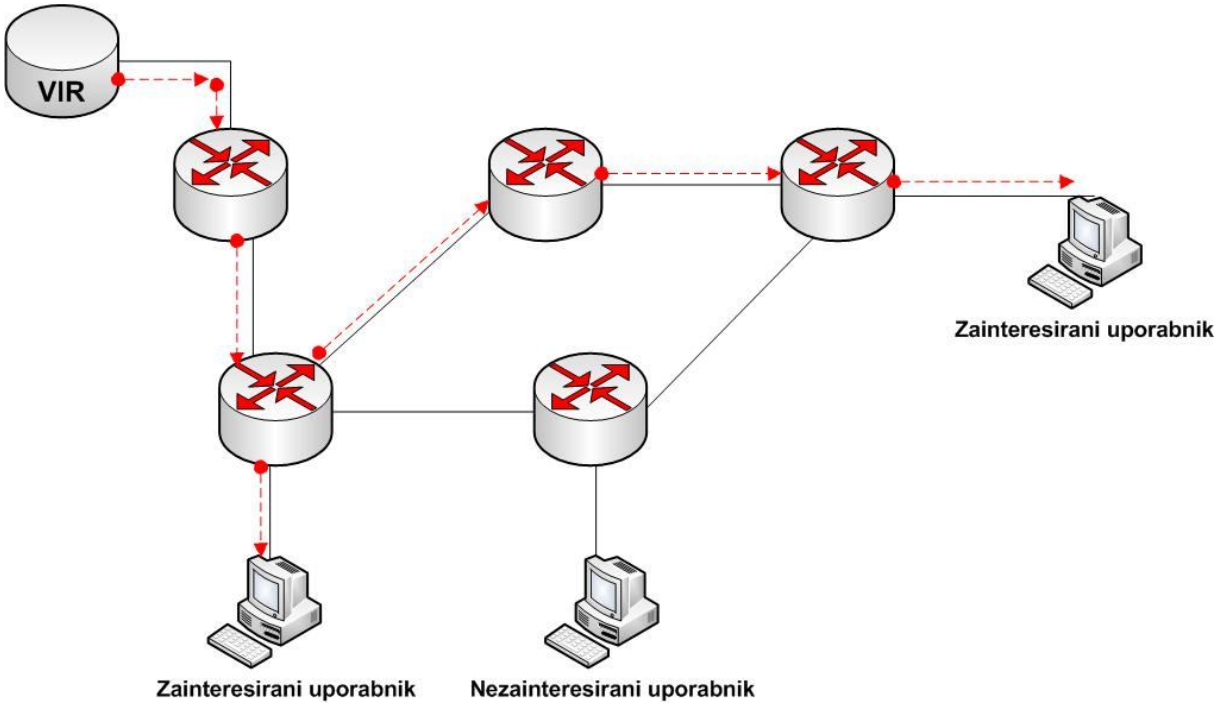
IP-multicast je tehnologija, ki ne obremenjuje pasovne širine, ker omejuje promet tako, da pošlje **en sam** tok podatkov hkrati do mnogo uporabnikov. Aplikacije uporabljajo prednosti tehnologije multicast na področju video konferenc, učenja na daljavo, borznega poslovanja, novic … Multicast omogoča prednosti unicast in broadcast protokolov brez prej omenjenih slabosti. Pri multicastu se pošlje en tok podatkov, ki najdejo pot do zainteresiranega uporabnika. Za razliko od unicasta in broadcasta omrežje prenaša konstanten tok podatkov ne glede na število poslušalcev. Omrežje je odgovorno za repliciranje in dostavo podatkov le do zainteresiranih naslovnikov oziroma slušateljev, ki so se povezali npr. na radijsko postajo. Ta metoda omogoča najbolj učinkovito uporabo virov, ker potuje tok prometa samo skozi tiste omrežne povezave, ki vodijo do zainteresiranih gostiteljev. Z uporabo multicasta ne obremenjujemo vira, ker pošiljamo v omrežje en sam tok podatkov, kakor tudi ne obremenjujemo omrežja, ker se pošilja promet samo zainteresiranim gostiteljem.[3][6]



Slika 2-1: Promet unicast



Slika: 2-2: Promet broadcast



Slika 2-3: Promet multicast

2.1 SLABOSTI PRI UPORABI MULTICAST-a

Kljub vsem že naštetim prednostim uporabe multicasta, obstajajo omejitve in določene slabosti. Te omejitve se nanašajo na **nezanesljivo dostavo paketov**, **podvajanje paketov** ter **zamašitev omrežja** (network congestion).
Kot pri unicast je tudi pri multicast **dostava paketov** dokaj **nezanesljiva**. IP- paketi multicast uporabljajo protokol UDP (User Datagram Protocol), ki je najbolj preizkušen in učinkovit pri prenosu podatkov v realnem času (pretok avdio in video vsebin). Aplikacija, ki jo uporablja IP-multicast, mora biti pripravljena na (občasno) izgubo paketov in mora to nadomestiti na aplikacijskem nivoju ali preko zanesljivega protokola multicast. Dr. Deering je v svoji tezi zapisal, da je ob topološki spremembi omrežja, ki ji sledi sprememba logične poti, verjetnost, da paketi multicast dosežejo cilj, manjša od te verjetnosti pri uporabi paketov unicast. Razpošiljanje paketov multicast temelji na IP-naslovu vira. Da preprečimo zanko v omrežju, se paket *zavrže*, če ne prispe skozi vmesnik, ki vodi nazaj do vira.

Podvojeni paketi v omrežju se pri IP-multicast pojavljajo v podobni obliki kot pri unicast. Bistvena razlika je v usmerjanju, in sicer da usmerjevalniki pošiljajo kopije paketov multicast skozi več vmesnikov. Tako se poveča verjetnost, da večje število podvojenih paketov doseže sprejemnika. Takšen primer se lahko pojavi na redundantnih omrežjih, kjer obstaja več poti do sprejemnikov. Podvojeni paketi se pojavljajo, dokler usmerjevalni protokoli multicast ne odstranijo (*obrežejo*) odvečne poti do sprejemnika.

Zamašitev omrežja (Network Congestion)

V primeru unicast prilagodijo pretok podatkov TCP-mehanizmi, to pa prestavlja zamašitev omrežja. Ker IP-multicast ne uporablja TCP-ja, ampak že prej omenjeni protokol UDP, multicast ne vsebuje mehanizma, ki bi preprečeval zamašitve. Protokol UDP se obnaša enako tudi v primeru unicast. Razlog, zakaj se uporablja UDP in ne TCP, je neprimernost TCP-ja za prenos podatkov v realnem času. Ko protokol TCP (izgubljeni ali zavrženi) paket ponovno pošlje, ta postane neuporaben za avdio in video pretok podatkov v realnem času. [2]

3 IP-NASLOVNI PROSTOR

Trenutno je v večinski uporabi ipv4 internetni naslovni prostor. IP-naslov je 32-mestno binarno število, ki označuje gostitelja/host oz. napravo znotraj internetnega naslovnega prostora. To 32-bitno število je sestavljeno iz štirih osembitnih števil, ki jih lahko zapišemo tudi v desetiški obliki.

Na primer: naslov **193.189.161.55** v desetiški obliki je v binarni obliki sestavljene iz 0 in 1. **11000001.10111101.10100001.10100001** predstavlja zgoraj naveden naslov.

Del bitov naslova lahko uporabimo za določitev podomrežja znotraj omrežja.

Kot smo že omenili, IPv4 uporablja 32-bitne naslove, kar omejuje naslovni prostor na 4.294 milijarde možnih unikatnih naslovov. Od tega je za posebne namene (privatni naslovi) rezerviranih 18 milijonov naslovov, kar pomeni, da je na internetu možnih 4.276 naslovov. Prvotno so bili IP naslovi namenjeni organizacijam skupaj s omejitvami *classful*. To pomeni, da so se dodeljevali razredi A-omrežja izključno z 8-bitno masko, razredi omrežja B s 16- in razredi omrežja C s 24-bitno masko. Se pravi, da je lahko podjetje pridobilo v uporabo razred A, čeprav še zdaleč ni potrebovalo toliko naslovov. Ta način se je izkazal za precej neučinkovit, še zlasti v zadnjem obdobju, ko primanjkuje IP naslovov. Eden izmed načinov, kako to rešiti, je brezrazredno med-domensko usmerjanje (CIDR), ki omogoča, da lahko razredom določamo masko podomrežja poljubne dolžine (VLSM). To je v praski vsaj malo upočasnilo hitro zmanjševanje in posledično pomanjkanje IP naslovov.

Pri naslavljanju poznamo tri osnovne tipe razredov ter dva dodatna razreda:

Razred A: 0.....|..... ....
V prvem zlogu imamo rezervirani prvi bit, tako da ostane za naslov omrežja sedem bitov ali drugače – možnih je 128 različnih naslovov omrežij. Ostali trije zlogi so namenjeni za naslavljanje naprav. Tako je možno v nekem omrežju nasloviti 16777214 naprav. Kako smo dobili to številko? Ker za naprave ostanejo trije osembitni zlogi, jih seštejemo in dobimo število 24, ki je potenca osnove 2. Rezultat te potence je 16777216, moramo pa mu odšteti 2, zaradi samih ničel in enic – omrežnega in broadcast naslova, ki ne moreta biti v uporabi za naprave.

Razred B: 10..... ..... | ....
V tem razredu sta za oznako velikosti omrežja rezervirana 2 bita. Ostane še 14 bitov za naslov omrežja, kar pomeni 16384 različnih naslovov omrežij. Za naprave ostaneta zadnja dva zloga oziroma 16 bitov, ki jih lahko porabimo za naslavljanje 65534 naprav.

Razred C: 110..... .... | .....
V razredu C lahko tvorimo 2097152 naslovov omrežij in v vsakem omrežju naslavljamo 254 naprav.

Poznamo še dva razreda; razred D, ki je rezerviran za naslove multicast , in razred E, ki je namenjen testiranju. Spoznajmo na hitro še razred D.

3.1 NASLOVNI PROSTOR MULTICAST

Za multicast IP naslove je rezerviran razred D: 1110.... ....
V tem razredu so za naslov omrežja rezervirani 4 biti. Za multicast uporabljamo IP-številke med 224 in 239 v prvem zlogu, torej zajema naslove od 224.0.0.0 do 239.255.255.255. [4]

Za razliko od naslovov IP-unicast, ki enolično identificirajo en IP-naslov, naslov IP-multicast označuje poljubno skupino IP-gostiteljev, ki so se pridružili skupini in želijo prejemati promet poslan v to skupino.

3.2 UPORABA NASLOVNEGA PROSTORA IP-MULTICAST

Začetni naslov	Končni naslov	Opis
224.0.0.0	224.0.0.255	Rezervirano za posebne "poznane" naslove multicast
224.0.1.0	238.255.255.255	Globalni-internetni naslovi multicast
239.0.0.0	239.255.255.255	Lokalni-administrativni naslovni prostor

3.2.1 REZERVIRANI NASLOVI IP-MULTICAST

Uporaba »poznanih« naslovov multicast:

Naslov	Opis
224.0.0.0	Osnovni naslov
224.0.0.1	Vsi gostitelji v omrežju
224.0.0.2	Vsi usmerjevalniki v omrežju
224.0.0.5	Naslov usmerjevalnega protokola OSPF
224.0.0.9	Naslov usmerjevalnega protokola RIPv2
224.0.0.10	Naslov usmerjevalnega protokola EIGRP
224.0.0.13	PIM Verzija 2
224.0.0.14	Protokol za rezervacijo virov RSVP
224.0.0.18	Virtualni redundantni usmerjevalni protokol (VRRP)
224.0.0.22	IGMP verzije 3
224.0.0.251	Naslovi multicast DNS
224.0.1.39	Cisco Avto-RP-napoved
224.0.1.40	Cisco Auto-RP-iskanje

3.2.2 NASLOVI ETHERNET MULTICAST

Nekaj poznanih naslovov ethernet multicast. To so naslovi na drugi plasti referenčnega modela ISO/OSI.

Naslov Ethernet multicast	Tip	Opis
01-00-0C-CC-CC-CC	0x0802	Iskalni protokol Cisco (CDP), Povezovalni protokol Vlan (VTP)
01-00-0C-CC-CC-CD	0x0802	Protokol vpetega drevesa (STP) IEEE 802.1D
01-00-5E-xx-xx-xx	0x0800	IPv4 IGMP multicast naslovi
33-33-00-00-00-00	0x86DD	IPv6 iskanje sosedov
33-33-xx-xx-xx-xx	0x86DD	IPv6 multicast naslovi

4 MULTICAST NA OMREŽJU

V zgodnjih osemdesetih letih je bil multicast omejen na lokalna omrežja (LAN), s podporo protokolov kakršna sta Ethernet in Token Ring, za razliko od razširjenih LAN-ov (današnjih WAN omrežij), ki niso podpirali multicast. Na tem področju ni bilo sprememb do poznih osemdesetih, ko je g. Steve Deering iz univerze Stanford predstavil razširitve unicast usmerjevalnih mehanizmov OSPF in RIP, kateri je sledila doktorska teza z naslovom [Multicast Routing in a Datagram Network]. V tezi je opisal tudi Host Membership Protocol, ki je predstavljal osnovo za današnji standardni Internet Group Membership Protocol (IGMP), ki ga gostitelji multicasta uporabljajo za signalizacijo usmerjevalnikom, da se želijo včlaniti v skupino multicast. Teza dr. Deeringa je vsebovala še vektorsko osnovan usmerjevalni protokol IP-multicast kot osnovo za Distance Vector Multicast Routing Protocol (DVMRP), ki ga je Deering razvil nekaj let kasneje. Ta dva protokola (IGMP in DVMRP) sta omogočila, da je IP- paketno omrežje podpiralo multikastno podporo na tretji oz. omrežni plasti referenčnega modela ISO/OSI. V kasnejšem obdobju se je multicast razvijal dalje in sledili so dodatni protokoli, kot je Protocol Independent Multicasting (PIM) in multiprotocol extensions to the Border Gateway Protocol (MBGP). Te protokoli so omogočili multicastu povzpeti se do velikih korporativnih mrež in nenazadnje do tej tehnologiji domačega interneta. Prelomno leto za razvoj tehnologije multicast je bilo 1992, ko je dr. Deering predstavil Multicast Backbone-MBone, ki je v začetku predstavljal navidezno omrežje, sedaj pa je v internetu praktično nepogrešljiv. MBone je bil sestavljen iz tunelov, katerih začetne točke so bile delovne postaje, ki so podpirale DVMRP in ki so bile sposobne procesirati unicast-enkapsulirane pakete multicast ter te pakete pošiljate na primerne vmesnike na usmerjevalnikih. Marca, leta 1992, so na osnovi omenjene MBone prenašali prvi zvočni zapis iz IETF-konference v San Diegu na 20 oddaljenih lokacij po svetu, to pa je bil tudi prvi takšen prenos multicasta na svetu. [1][2]

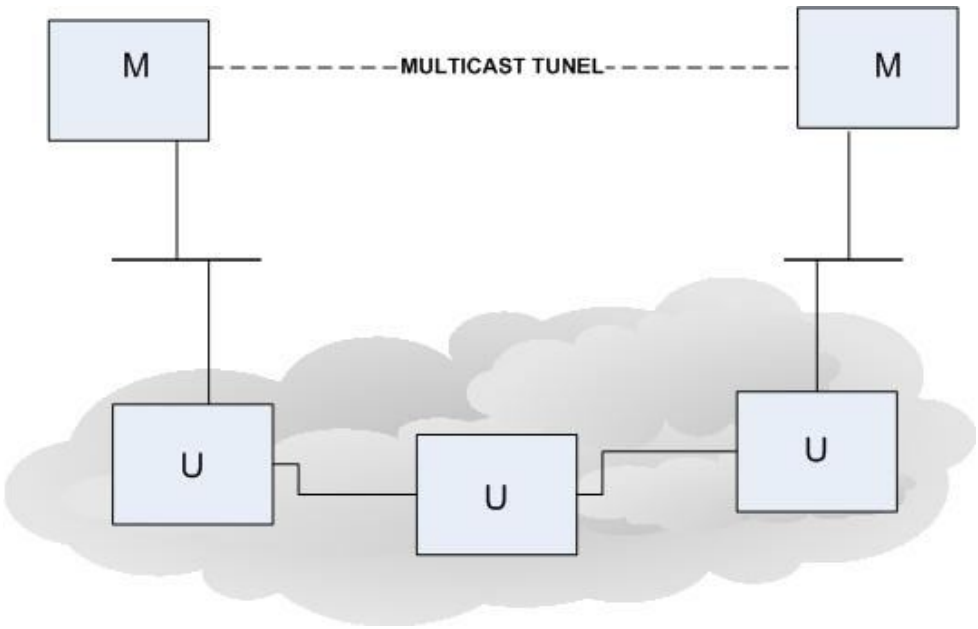
4.1 MBONE

Kot je znano, je leta 1992 Steve Deering predstavil prvo ogrodno omrežje (**MBone**), takrat pa se je znotraj IETF (*Internet Engineering Task Force*) tudi pričelo z aktivnim razvojem programske opreme, ki bi omogočila oddajanje več uporabnikom hkrati z obstoječo strojno opremo.

4.2 ZGRADBA OMREŽJA MBONE

MBone je navidezno omrežje, saj uporablja iste fizične povezave kot internet. Oddajanje več prejemnikom hkrati je omogočeno s transparentnim prehajanjem paketov multicast po omrežju IP (internetu). Jedro sistema je program »mrouted«, ki je nameščen na delovnih postajah s podporo omrežju MBone. Program sprejete pakete multicast zamaskira v obliko unicast in jih usmeri na izhodne vmesnike do omrežja internet.

Povezava med tovrstnimi delovnimi postajami (*M-usmerjevalniki*) je zagotovljena z uporabo tuneliranega protokola od točke do točke. Le-ta omogoča transparenten prenos paketov multicast med posameznimi točkami z uporabo interneta. Vsak tunel povezuje dve točki z eno logično povezavo, ki lahko poteka preko skupine IP-usmerjevalnikov.[9]



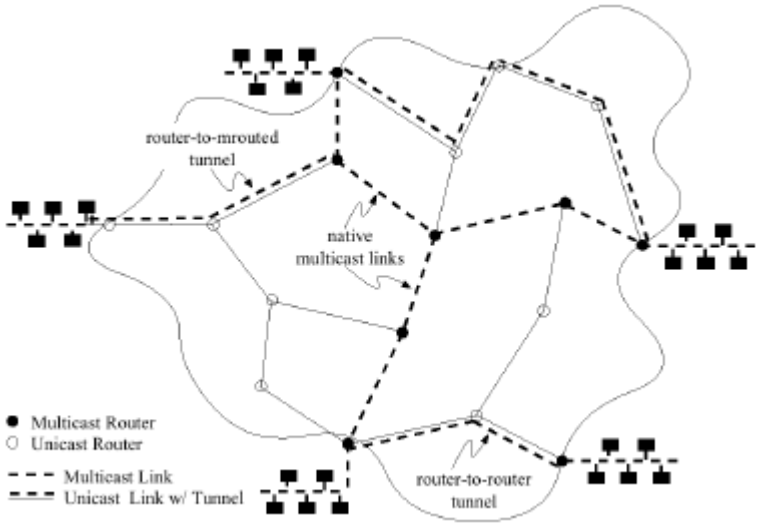
Slika 4-1: Tunel multicast [9]

M-usmerjevalnik zamaskira prejeti paket multicast v IP-paket ter ga odda v omrežje. IP-usmerjevalniki (U na sliki 4-1) vzdolž tunela ne vedo ničesar o vsebini paketa.

Ko zamaskiran paket pride do M-usmerjevalnika na ponorni strani, le-ta odvrže IP-glavo paketa ter vsebino paketa multicast usmeri do uporabnika. (Slika 4-2)

Slika 4-2: Maskiranje paketa multicast v IPv4-paket [9]

Topologijo omrežja MBone lahko ponazorimo kot kombinacijo zvezde in zanke, kjer kraki zvezde predstavljajo povezave znotraj zaključenega omrežja, med tem ko so povezave med vozlišči v zanki tunelov med m-usmerjevalniki. (Slika 4-3)[9]



Slika 4-3: Zgradba omrežja Mbone [9]

4.3 METODA POVRATNE POTI – (RPF, REVERSE PATH FORWARDING)

Usmerjanje multicast se precej razlikuje od standardnega usmerjanja unicast. Na splošno, usmerjevalniki opravljajo usmerjanja unicast, ki temeljijo na ciljnem naslovu paketa. Ko paket unicast prispe do usmerjevalnika, le-ta preveri ciljni naslov paketa v svoji usmerjevalni tabeli. Usmerjevalna tabela pove usmerjevalniku, skozi kateri vmesnik naj posreduje paket do ciljnega omrežja. Paketi unicast se nato usmerjajo od vira do naslovnika (cilja).

Pri usmerjanju multicast usmerjevalniki nastavijo posredovanje v nasprotni smeri kot pri modelu unicast, od sprejemnika do korena distribucijskega drevesa. Usmerjevalniki izvajajo RPF-preverbo, da določijo vmesnik, ki je topološko najbližje korenu drevesa (slika 4-4). RPF je ključni koncept pri usmerjanju multicast. V RPF-preverjanju, opravi usmerjevalnik vpogled v svojo usmerjevalno tabelo, da določi svoj RPF-vmesnik, ki je hkrati najbližji vmesnik korenu. Ta RPF-vmesnik je sprejemni vmesnik za skupino multicast.

RPF-preverba je nujna za implementacijo multicasta na usmerjevalnikih. Ko paket multicast prispe na usmerjevalnikov vmesnik, usmerjevalnik razlaga izvorni naslov v multicastnem IP-paketu, kot ciljni naslov paketa unicast. Izvorni naslov multicast se nahaja v usmerjevalni tabeli unicast in določenem izhodnem vmesniku. Če je odhodni vmesnik v usmerjevalni tabeli unicast enak kot vmesnik, na katerem je bil prejet paket multicast, potem paket uspešno opravi RPF-preverbo. Paketi multicast, ki ne opravijo RPF-preverbe uspešno, se zavržejo, ker sprejemni vmesnik ni na najkrajši poti nazaj do vira.

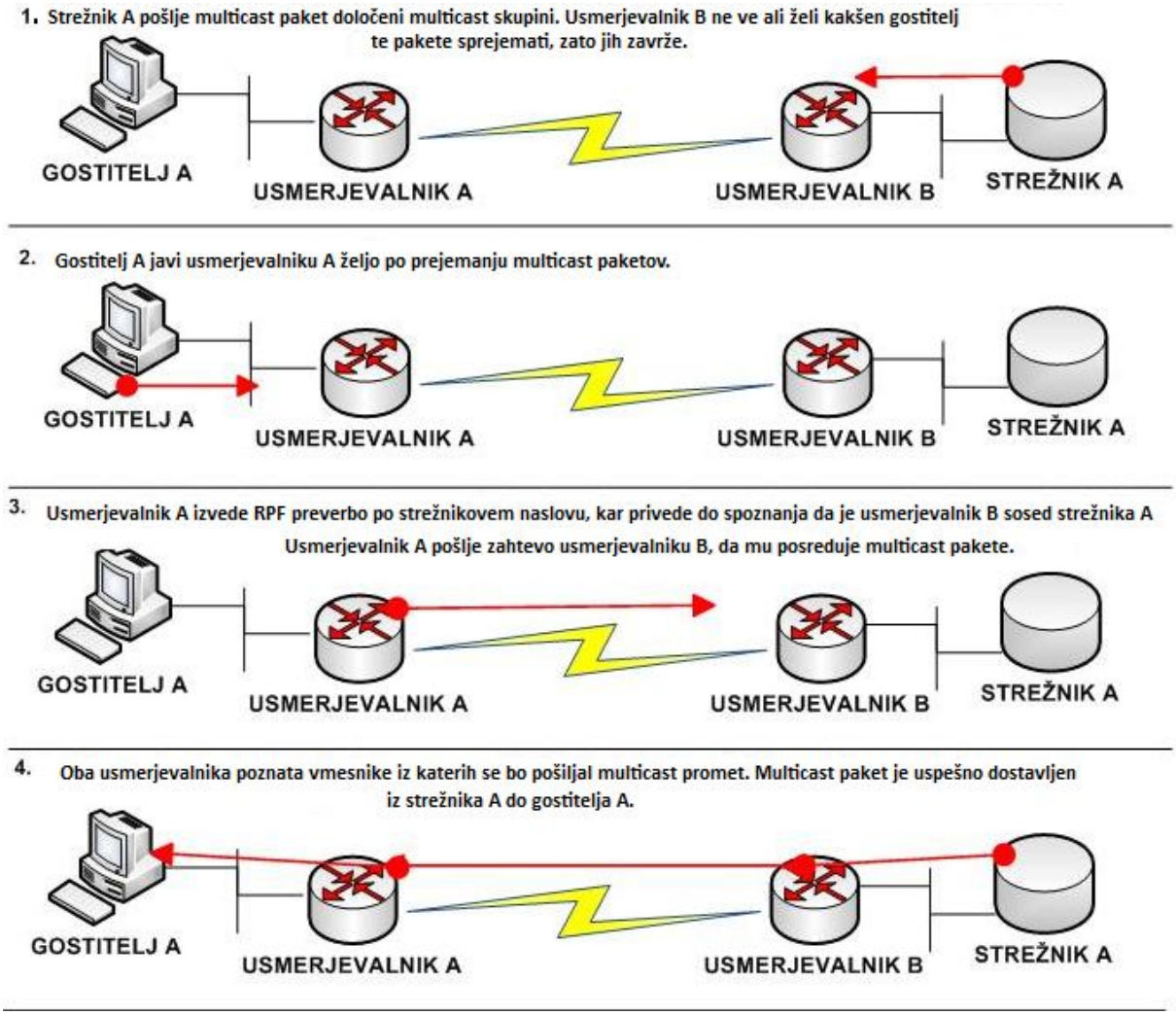
Skoraj vsi IP multicast usmerjevalni protokoli uporabljajo neke vrste PRF, oziroma preverbe dohodnih vmesnikov kot osnovni mehanizem za določitev, ali naj dohodni paket posredujejo dalje, ali pa ga zavržejo. Če je RPF- preverba uspešna, se paket posreduje dalje, sicer pa se zavrže.

Za promet, ki potuje navzdol po izvornem drevesu, se mehanizem RPF- preveritve izvaja v naslednjih korakih [2]:

1. Usmerjevalnik preuči izvorni naslov prejetega paketa multicast, da določi, ali je paket prejel preko vmesnika, ki je na povratni poti nazaj k viru.
2. Če je paket prispel preko vmesnika, ki vodi nazaj k viru, je RPF-preveritev uspešno opravljena, in paket se posreduje dalje.
3. Če je RPF-preveritev neuspešna, se paket zavrže.

Kako usmerjevalnik določi, kateri vmesnik je na povratni poti nazaj k viru, je odvisno od uporabljenega usmerjevalnega protokola. V nekaterih primerih, multicastni usmerjevalni protokol vzdržuje ločeno usmerjevalno tabelo multicast, ki jo uporablja za RPF-preveritve. Primer takšne uporabe je DVMRP.

V drugih primerih pa multicastni usmerjevalni protokol uporablja obstoječo usmerjevalno tabelo unicast, s pomočjo katere določi vmesnik, ki je na povratni poti k viru. To metodo uporablja Protocol Intependent Multicast (PIM), katerega bomo spoznali v naslednjem poglavju.[2]



Slika 4-4: Metoda povratne poti (RPF) [3]

4.4 TABELA RPF

Tabela RPF igra pomembno vlogo v usmerjanju prometa multicast. Uporablja se za vsako RPF-preverjanje, ki se izvaja na paketih multicast, ki dosežejo usmerjevalnik. RPF ne vsebujejo naslovov skupin multicast, ker se preverjanja izvajajo samo na unikatnih naslovih,

da poiščejo vrhnji vmesnik do vira ali RP. Kadar se za RPF uporablja ista tabela kot za usmerjanje paketov unicast, se uporabljajo običajni usmerjevalni protokoli (RIP, OSPF, IS-IS,BGP...). [3]

4.5 DISTRIBUCIJSKA DREVESA

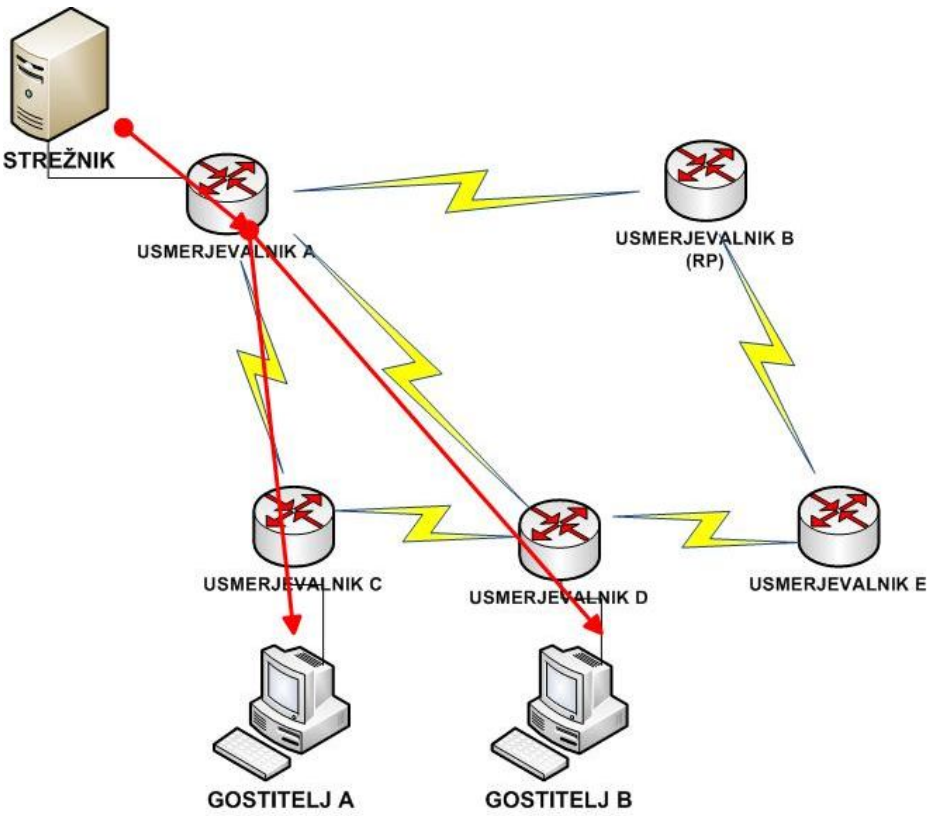
Za prenos podatkov zainteresiranim uporabnikom **usmerjevalnik** ustvari **distribucijsko drevo**. Vsako podomrežje, ki vsebuje vsaj enega zainteresiranega uporabnika, postane **list drevesa**. Koren drevesa je pri viru (izvoru podatkov), **veje drevesa** povezujejo podomrežja zainteresiranih sprejemnikov (liste drevesa). Paketi multicast se pošiljajo preko vej drevesa. Kadar se uporabnik odjavi iz skupine, se odstrani tudi veja z drevesa, da se paketi multicast ne replicirajo več po tem delu omrežja.

V primeru unicast se promet usmerja skozi omrežje preko ene same poti – od vira do ciljnega gostitelja. V modelu multicast vir pošilja promet na naslov poljubni skupini gostiteljev, ki jo imenujemo skupina za oddajanje več prejemnikom (multicast group). Da razpošljejo promet multicast do vseh sprejemnikov, se uporabljajo distribucijska drevesa, da določijo pot, ki jo promet IP- multicast opravi skozi omrežje. Dva bistvena tipa distribucijskih dreves sta **izvorna drevesa** *(source trees)*, ki jih imenujemo tudi **drevesa najkrajše poti,** ter **souporabniška drevesa** *(shared trees).*[2][5]

4.5.1 DREVO NAJKRAJŠE POTI – (SPT, SHORTEST PATH TREE)

Najpreprostejša oblika multicast-distribucijskih dreves je izvorno drevo, čigar koren je vir prometa multicast in katerega veje tvorijo skupno vpeto drevo (Spanning tree) skozi omrežje do sprejemnikov. Ker njegova drevesa uporabljajo najkrajšo pot skozi omrežje, jih imenujemo **drevesa najkrajše poti**.

V tej metodi je vir distribucijskega drevesa njegov koren. Ko usmerjevalnik izve, da je zainteresirani slušatelj eden izmed direktno povezanih vmesnikov, se skuša včlaniti v drevo te skupine. Da zgradi drevo najkrajše poti, mora izvesti RPF-preverbo, ki jo izvede z iskanjem virovega naslovnega prostora v svoji usmerjevalni tabeli. PRF preverjanje pove usmerjevalniku, kateri vmesnik je najbližji viru. Usmerjevalnik tako določi pot paketom multicast, ki od določenega vira k določeni skupini potujejo skozi ta vmesnik. [2][3]



Slika 4-5: Drevo najkrajše poti

4.5.2 SOUPORABNIŠKA DREVESA, TOČKA STIČIŠČA, DREVO TOČKE STIČIŠČA – (SHARED TREES, RENDEZVOUS POINT, RENDEZVOUS POINT TREE)

Za razliko od STP, ki imajo koren drevesa v samem viru, je koren pri souporabniških drevesih usmerjevalnik, lociran nekje v jedru omrežja. Ta koren pogosto poimenujemo *rendezvous point* (RP) ali *core* oz. točka stičišča, zato souporabniška drevesa imenujemo tudi *rendezvous point* trees (RPT) ali *core-based trees* (CBT). Ta način se uporablja v PIM-SM metodi (ki jo bom predstavil v prihodnjih poglavjih). Paketi iz vrhnjega toka in včlanitve (join) iz dostopnih usmerjevalnikov se srečajo v tej točki – točki stičišča. V RP-metodi ostali usmerjevalniki ne poznajo naslovov vseh skupin multicast. Vse kar potrebujejo, je IP-naslov RP-usmerjevalnika, le-ta namreč pozna vire vseh multikastnih skupin. [5]

Da se včlani v souporabniško drevo oz. Rendez Vous Point Tree (RPT), kot se imenuje v PIM-SM-metodi, mora usmerjevalnik C narediti naslednje korake [5]:

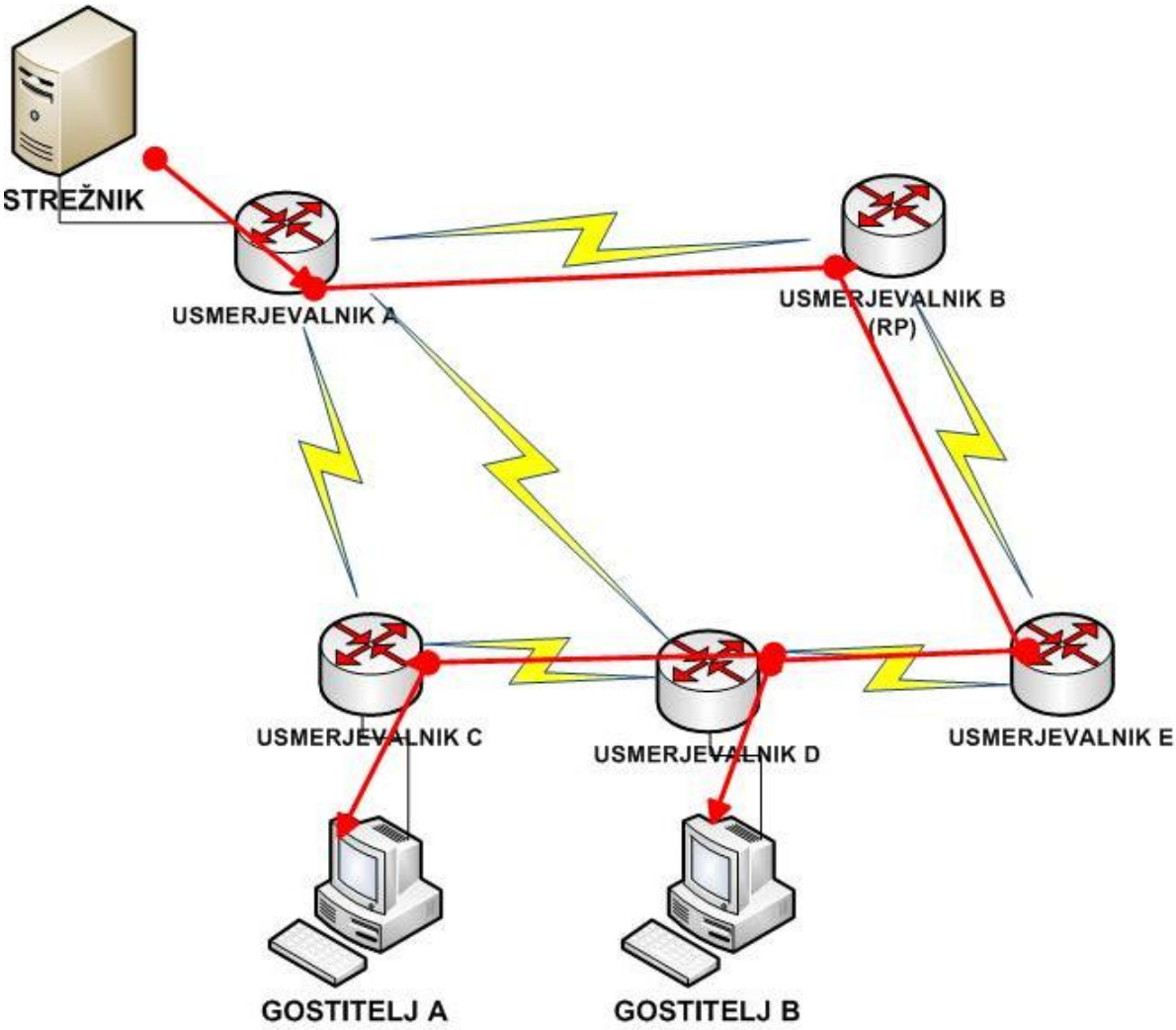
- Določiti IP-naslov RP za določeno skupino. To lahko določi statično ali s pomočjo ugnezdenih protokolov.
- Zgraditi skupno drevo za to skupino. Usmerjevalnik C izvrši RPF-preverbo do RP-naslova, ki ga dobi v svoji usmerjevalni tabeli. To dobi prek vmesnika, ki je najbližji RP-usmerjevalniku. Usmerjevalnik C sedaj ve, da bodo paketi multicast te RP določene skupine preko tega RPF- vmesnika.
- Pošlje sporočilo *join* skozi ta vmesnik z uporabo primernega protokola multicast (PIM-SM mode) in obvesti vrhnji usmerjevalnik, da se želi pridružiti skupnemu drevesu. To sporočilo označimo kot (*,G[1]), ker je S[2] v tistem trenutku še neznan, poznan je samo RP, ki pa ni vir paketov multicast. Usmerjevalnik, ki dobi (*,G) sporočilo join, doda vmesnik, na katerem je bilo prejeto sporočilo v OIL (Outgoing Interface List), in sproži RPF-preverbo na svojem PR-naslovu. Ta usmerjevalnik pošlje (*,G) sporočilo iz PRF-vmesnika proti viru, da obvesti usmerjevalnik nad njim, da se želi pridružiti skupini.

Vsak usmerjevalnik proti vrhu ta proces ponovi z oglaševanjem sporočil *join* skozi RPF-vmesnik in gradnjo skupnega drevesa, dokler je to možno. Ta proces se ustavi ko:

- dosežemo RP za to skupino, ali
- ko dosežemo usmerjevalnik, ki je že v tranzicijskem stanju multicast preko RPT.

V obeh od omenjenih primerov je povezava narejena in paketi lahko potujejo od vira do RP in kasneje od RP do sprejemnika. RPT ponavadi ni najkrajša možna pot od sprejemnika do vira, obstajajo pa načini migracije skupnega drevesa k SPT takrat, ko se začne prenos paketov. [5]

[1]G-Group ali Skupina [2]S-Source ali vir.



Slika 4-6: Drevo stične točke ali RPT

5 MULTICAST USMERJANJE

5.1 PROTOKOLNO NEODVISNO ODDAJANJE VEČ PREJEMNIKOM – (PROTOCOL INDEPENDENT MULTICAST-PIM)

PIM je družina multicast usmerjevalnih protokolov, ki omogočajo eden-do-več ali več-do-več distribucijo podatkov preko lokalnega omrežja (LAN) ter prostranega omrežja (WAN) oziroma interneta. Protokolno neodvisen se označuje zato, ker ne vključuje svojega lastnega mehanizma za odkrivanje topologije omrežja, ampak se poslužuje že obstoječih usmerjevalnih protokolov kot so BGP ali OSPF… [3]

V uporabi so trije načini usmerjanja:

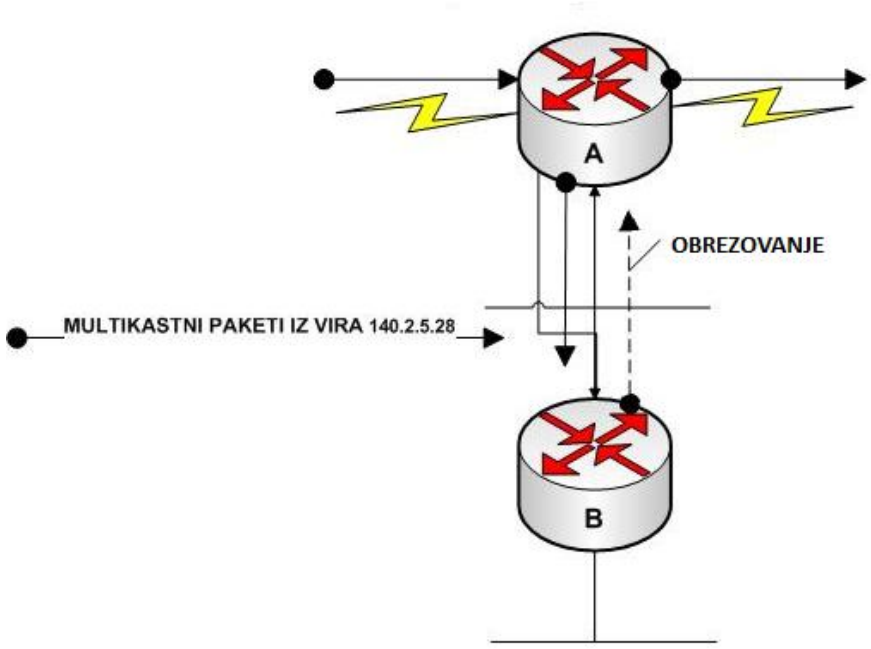
- protokol zgoščenega načina – Dense mode protokols (DVMRP in PIM-DM);
- protokol redkega načina – Sparse mode protocols (PIM-SM, PIM-SSM, BIDIR-PIM;
- protokol stanja-povezav – Link-state protocols (MOSPF).

5.2 PIM-DENSE MODE (PIM-DM)

Ta protokol uporablja drevo najkrajše poti za dostavo (S,G) multikastnega prometa po metodi *potisni (push)*. Ta metoda predvideva, da je v vsakem podomrežju vsaj eden (S,G)-sprejemnik prometa multicast, zato se promet potiska oz. poplavlja na vse točke v omrežju. Ta proces je podoben radijskemu ali televizijskemu zračnemu oddajanju.

5.2.1 POPLAVLJANJE IN OBREZOVANJE (FLOODING & PRUNING)

Omenjeno poplavljanje na omrežju prinaša s tem povezan **strošek** (***cost***), kot so obremenitve pasovne širine, centralne procesne enote itd. Da se izognemo takšni porabi omrežnih virov, morajo usmerjevalniki pošiljati **sporočila obrezovanja** (**Prune messages**) nazaj proti viru distribucijskega drevesa, da zaustavijo neželen multicast promet. To pomeni, da so veje drevesa brez sprejemnikov odstranjene z distribucijskega drevesa, na katerem ostanejo veje, ki vsebujejo sprejemnike.



Slika 5-1: Obrezovanje (pruning)

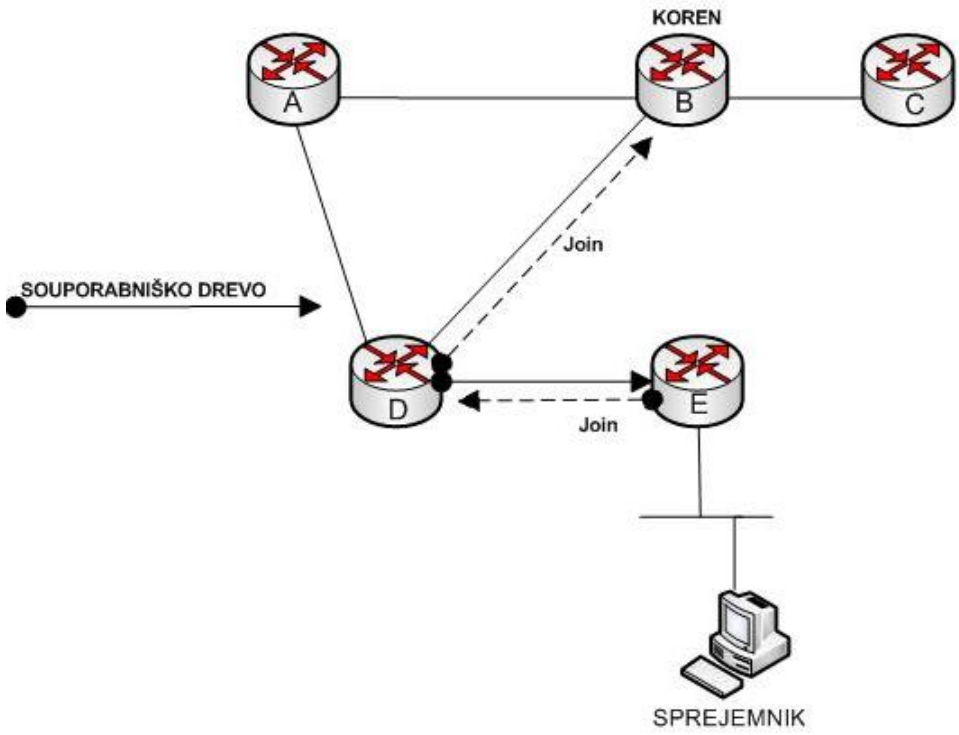
Ko usmerjevalnik A prejme sporočilo ***prune*** za promet (S,G)-multicast na odhodnem vmesniku (Eth0), se ta vmesnik nastavi v obrezano stanje in ustavi pošiljanje prometa iz vmesnika. V tem primeru je vmesnik povezan z več dostopnim omrežjem, na katerem ni nobenega sprejemnika, ki želi prejemati promet multicast. Kadar želi usmerjevalnik ponovno aktivirati vmesnik, to izvede s pomočjo časovnega izteka (timeout), v času katerega se obrezani vmesnik postavi v aktivno stanje. [2]

5.3 PIM-SPARSE MODE (PIM-SM)

Trenutno najbolj uporabljen multicastni usmerjevalni protokol PIM-SM za distribucijo prometa multicast do sprejemnikov uporablja drevo najkrajše poti (SPT). Namesto uporabe metode *potisni*, uporablja metodo *povleci* (pull), v kateri se ves promet »povleče« do sprejemnikov. V slednji metodi se predpostavlja, da je v osnovi ves multikastni model neželen, če ni za to posebne zahteve, ki se izvrši preko sporočila *join*.

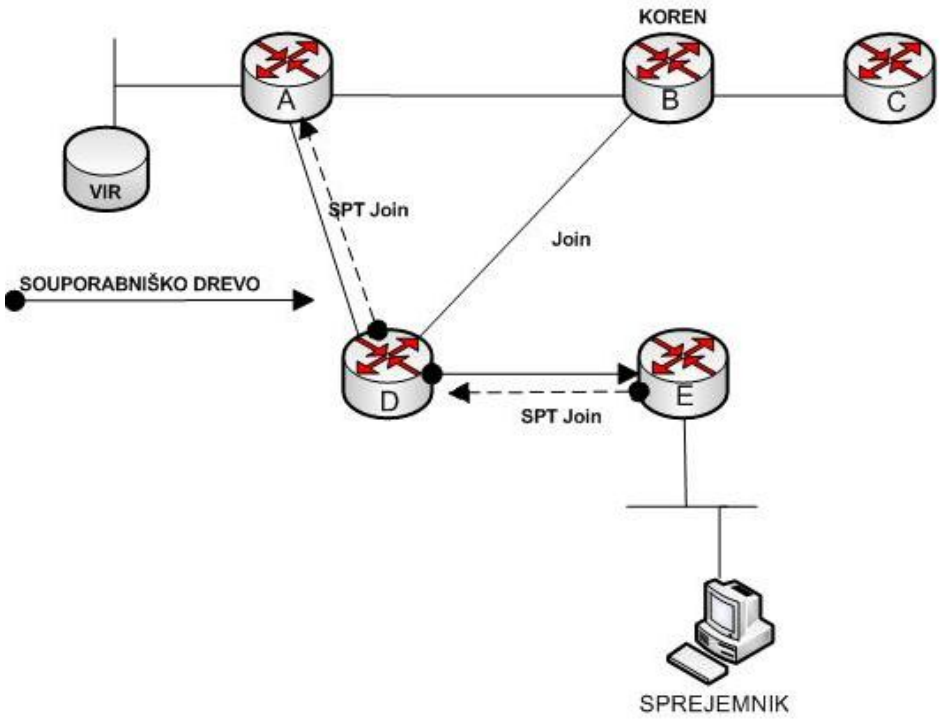
5.3.1 SPOROČILA JOIN NA SOUPORABNIŠKIH DREVESIH

Da se promet multikast v redkem načinu »povleče« do sprejemnika, se mora ustvariti veja na korenu drevesa do sprejemnika. Da ustvarimo takšno vejo, usmerjevalnik pošlje sporočilo join na souporabniško drevo proti korenu drevesa. To sporočilo join potuje preko usmerjevalnikov in gradi vejo souporabniškega drevesa. [2]



Slika 5-2: Sporočila join na souporabniških drevesih

Slika 5-2 prikazuje, kako se sporočilo *join* pomika proti korenu souporabniškega drevesa. Usmerjevalnik E ima povezan sprejemnik in pošlje sporočilo join proti usmerjevalniku B preko usmerjevalnika D. Sporočilo potuje od hop-a do hop-a ter gradi vejo drevesa, dokler ne doseže korena. Na sliki 5-3 vidimo, kako se join obnašajo na drevesu najkrajše poti. V tem primeru usmerjevalnik A pošlje SPT sporočilo *join* proti viru preko usmerjevalnika C. STP-join potuje do usmerjevalnika A, medtem gradi drevo najkrajše poti.



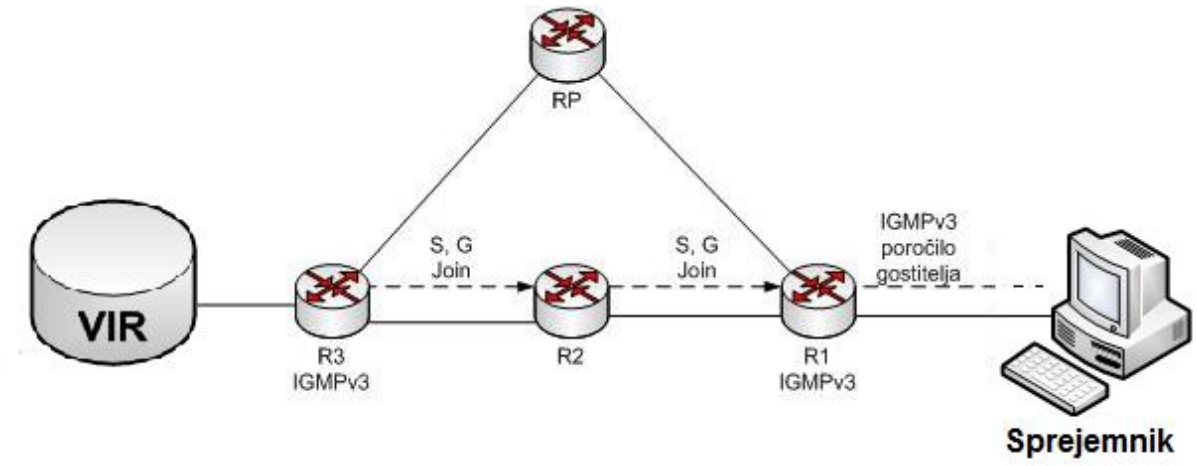
Slika 5-3: Sporočila join na drevesu najkrajše poti

5.3.2 SPOROČILA OBREZOVANJA V REDKEM NAČINU

V redkem načinu se sporočila obrezovanja pošiljajo navzgor po distribucijskem drevesu, kadar promet multicast ni več zaželen. To omogoči vejam souporabniških dreves ali dreves najkrajše poti, ki so bile ustvarjene preko sporočil join, da se te veje odstranijo, ko niso več potrebne. Za primer: če usmerjevalnikov list ugotovi, da nima več neposredno povezanih gostiteljev (ali navzdol povezanih usmerjevalnikov) za določeno skupino multicast, ta usmerjevalnik pošlje sporočilo obrezovanja proti viru distribucijskega drevesa, da ugasne tok neželenega prometa multicast te skupine. Namesto da se čaka na vejo, da se odstrani zaradi časovnega izteka, se s pošiljanjem sporočil obrezovanja bistveno izboljša zakasnitev (latency). [3]

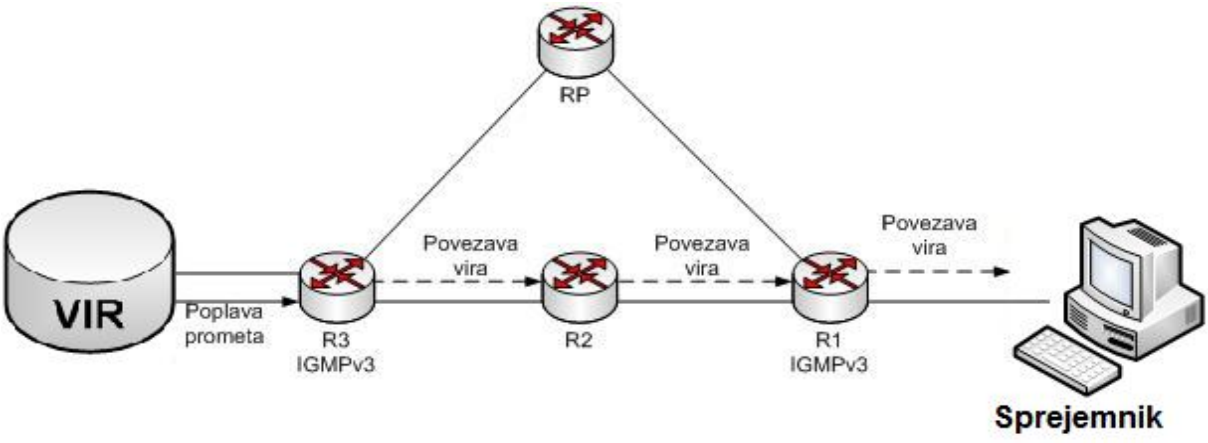
5.4 PIM-SSM

Protokol PIM-SSM je bolj preprost kot PIM-SM, ker je podprt le model eden-k-več (angl. one-to-many). Zgradi strukturo najkrajše poti po drevesu SPT, ki je usmerjena proti viru. V SSM-arhitekturi usmerjevalnik, ki je najbližje zainteresiranemu gostitelju, dobi informacijo o naslovu unicast vira prometa multicast. Tako se PIM-SSM izogne RP-povezavi in gre preko drevesne strukture direktno do vira. V PIM-SSM konfiguriranem omrežju se gostitelj vpiše v SSM- kanal in objavi željo, da bi se vpisal v skupino G in vir S. Neposredno povezan PIM-SM-usmerjevalnik, ki je prejemnikov DR-usmerjevalnik, pošlje sporočilo (S, G) join svojemu sosedu. [22][15]



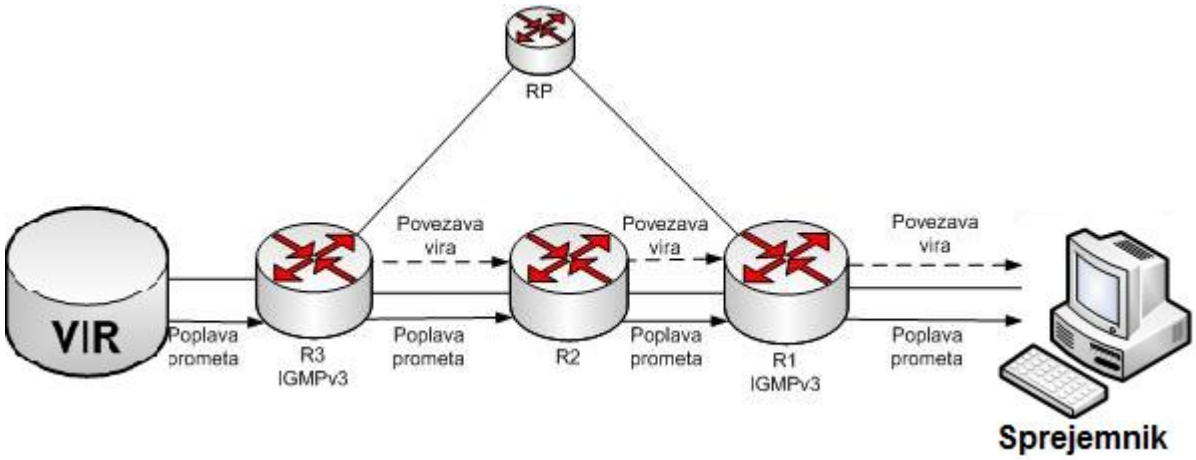
Slika 5-4: DR pošlje sporočilo join

Sporočilo S, G join začne svojo pot, ki jo zgradi s skoki, dokler ne doseže vira. Na sliki 5-5 je vidna pot po omrežju do usmerjevalnika Router3, ki je usmerjevalnik povezan na vir. [22][15]



Slika 5-5: Pot po omrežju do usmerjevalnika R3

Z uporabo zgrajene poti promet multicast tako doseže vse svoje gostitelje. [19]



Slika 5-6: Promet doseže vse gostitelje

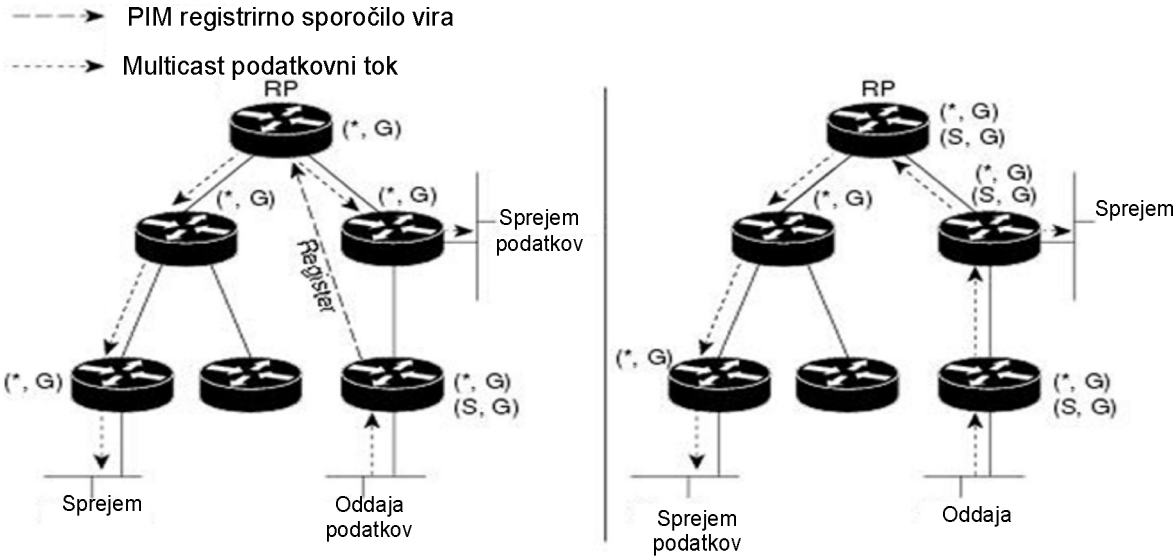
PIM-SSM-usmerjevalnik mora implementirati navzgornji in navzdolnji prenos podatkov (S, G), pozdravna sporočila *Hello*, protokol za odkrivanje sosedov source discovery ter pravila za posredovanje paketov.

5.5 BIDIR PIM

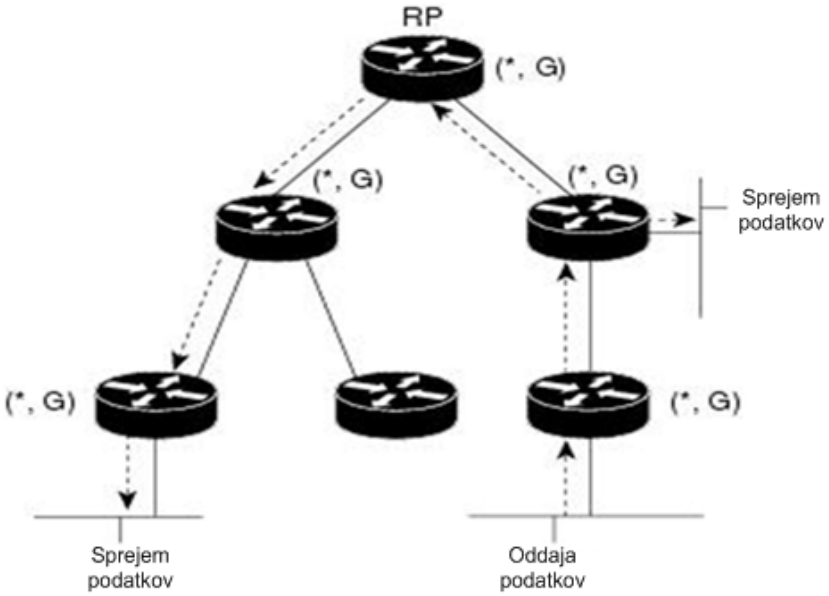
Dvosmerni protokoli Independent multicast (BIDIR-PIM) je različica PIM-SM, ki gradi dvosmerno deljena drevesa, ki povezujejo vire multicast in sprejemnike. Dvosmeren (angl. bidirectional) PIM je varianta protokola PIM, v katerem je paketni promet za skupino multicast usmerjen glede na pravila skupine multicast. V dvosmernem protokolu PIM je promet usmerjen vzdolž deljene drevesne strukture (angl. group shared tree), ki je vkoreninjena v RP-točko skupine. IPv6-naslov RP-točke igra ključno vlogo pri vzpostavitvi topologije spanning tree brez zanke. Ta naslov je lahko katerikoli prosti naslov dosegljivega omrežja v PIM-domeni. Članstvo v dvosmerni skupini se signalizira z eksplicitnimi sporočili *join*. Promet je od virov brezpogojno poslan navzgor preko drevesne strukture do RP točke in nato navzdol do prejemnikov. Dvosmeren PIM je bil načrtovan za aplikacije več-k-večim znotraj PIM-domen. Je izpeljanka protokola PIM-SSM in uporablja veliko STP-operacij.

V primerjavi s PIM-SM ne uporablja registrirnega procesa za vire, to je potrebno za posredovanje prometa po vseh usmerjevalnikih, ki so izključno osnovani na usmerjevalnih vpisih(*, G) multicast.

Na slikah spodaj je vidna razlika med primeroma, ko usmerjevalnik ustvari neusmerjeno deljeno drevesno strukturo (angl. undirectional shared tree) in strukturo vira drevesa (angl. source tree) proti dvosmerni deljeni drevesni strukturi. [23][15]



Slika 5-7: Deljena drevesna struktura [23]



Slika 5-8: Dvosmerna drevesna struktura [23]

Pri posredovanju paketov navzdol od RP-točke ni razlik med Bidir-PIM in PIM-SM. PIM-SM pa ne more posredovati prometa v smeri navzgor drevesne strukture, saj sprejme promet le od RPF-vmesnika. Ta vmesnik kaže v smeri proti RP-točki, zato dovoljuje le navzdolnji prenos podatkov. V tem primeru se navzgornji prenos enkapsulira v sporočila unicast, ki se prenašajo od DR- usmerjevalnika proti viru preko RP-točke. V drugem koraku pa RP-točka združi STP, ki je vkoreninjen proti viru. [23][15]

5.5.1 DVOSMERNO SKUPINSKO GRAJENJE DREVESNE STRUKTURE

Procedura za združitev souporabniške strukture in dvosmerne strukture poteka tako, da v omrežju z lokalnimi sprejemniki samo izvoljeni DF-usmerjevalnik poseli izhodno listo vmesnikov na osnovi prejetih sporočil IGMP join in pošlje sporočila (*, G) Join/Leave navzgor proti RP-usmerjevalniku. Ko se nižje ležeči usmerjevalnik želi pridružiti strukturi shared tree, je RPF-sosed v sporočilih PIM Join/Leave vedno izvoljen DF-usmerjevalnik za vmesnik, ki vodi k RP-točki. Ko usmerjevalnik prejme sporočilo Join/Leave, a ta usmerjevalnik ni njegov DR za ta vmesnik, sprejeto sporočilo zavrne. V omrežju, kjer vsi usmerjevalniki podpirajo dvosmerno strukturo shareed tree, so sporočila(S, G) Join/Leave ignorirala. Prav tako ni potrebe po pošiljanju (opozorilnih) sporočil PIM alert, saj DF-volitve izločijo paralelne navzdolnje poti do katerekoli RP-točke. [23][15]

5.5.2 POSREDOVANJE PAKETOV

Usmerjevalnik (*, G) vnose za dvosmerne skupine. Spisek teh vnosov vključuje vse vmesnike, za katere je bil usmerjevalnik DF izvoljen in za katere je sprejel sporočila IGMP ali PIM join. Če je usmerjevalnik lociran v delu, kjer se samo pošilja podatke, bo prav tako ustvaril vnos(*, G), v spisek pa ne bo vpisal nobenih vmesnikov. Če je paket prispel iz RPF-vmesnika proti RP-točki, se ga posreduje navzdol glede na spisek (*, G)-vnosov. V nasprotnem primeru pa DF-usmerjevalnik za sprejemni vmesnik posreduje paket navzgor v smeri RP, vsi ostali usmerjevalniki pa morajo zavreči ta paket. [23][15]

5.6 PROTOKOLI STANJA POVEZAV (LINK STATE PROTOCOLS)

Ti protokoli, kot je npr. MOSPF, se obnašajo podobno kot protokol zgoščenega načina, v tem da oboji uporabljajo SPT za razpošiljanje prometa multicast do sprejemnikov. Protokol stanja povezav pa ne uporablja poplavljanja in obrezovanja, ki je uporabljen v DVMRP in v PIM-DM. Namesto uporabe le-tega, uporabljajo za poplavljanje posebno informacijo multicast o stanju povezav, ki poišče sprejemnike na omrežju. Vsi usmerjevalniki na omrežju uporabljajo to informacijo za izgradnjo dreves najkrajše poti od vsakega vira do vseh sprejemnikov v skupini. [2]

6 PROTOKOL MULTICAST ZA UPRAVLJANJE SKUPIN

Obstajata dva protokola za upravljanje skupin:

- **INTERNETNI PROTOKOL ZA UPRAVLJANJE SKUPIN (IGMP);**
- **PROTOKOL MULTICAST ZA ODKRIVANJE POSLUŠALCEV (Multicast Listener Discovery, MLD).**

6.1 INTERNETNI PROTOKOL ZA UPRAVLJANJE SKUPIN (IGMP)

Internet group management protocol - IGMP se je razvil iz Host Membership Protocol-a, ki ga je opisal Dr. Deering v svoji doktorski tezi [Multicast Routing in a Datagram Network]. IGMP-sporočila uporabljajo gostitelji za obveščanje njihovih lokalnih usmerjevalnikov multicast, kdaj se želijo prijaviti (*join*) v želeno skupino multicast (*group*) in sprejemati promet multicast oziroma, kdaj se želijo odjaviti iz omenjene skupine. S prejeto informacijo preko IGMP-usmerjevalnikov vzdržujejo seznam članstva v skupini multicast. Članstvo v skupini je aktivno na usmerjevalnikovem vmesniku, če je vsaj en gostitelj (ali več) preko tega vmesnika podal IGMP-zahtevo za članstvo v skupini in prejemanje podatkov multicast iz te skupine. [2]

Obstajajo tri verzije protokola IGMP [8]:

- **IGMPv1** (rfc1112, 1989)
  Gostitelji se lahko povezujejo v skupine multicast, nimajo pa možnosti odjave. Za odjavo iz skupine so usmerjevalniki uporabljali mehanizme, ki so delovali na osnovi časovnega izteka za odkrivanje skupin brez zainteresiranih članov.

- **IGMPv2 (**rfc2236, 1997)
  Obstoječemu protokolu so bila dodana odjavna sporočila (leave messages), ki so omogočala hitro odjavo iz skupin.

- **IGMPv3** (rfc3376, 2002)
  Nekaj občutnih sprememb; omogočeno je bilo, da gostitelj (sprejemnik) navede seznam gostiteljev, od katerih želi prejemati promet (uporabljen v source specific multicast SSM). Promet neželenih gostiteljev se blokira znotraj omrežja. Gostiteljem je omogočeno tudi blokiranje paketov prihajajočih iz virov, ki pošiljajo neželen promet.

Trenutno sta de-facto standarda IGMPv2 in IGMPv3.

6.2 IGMPv3

Vsebuje vse atribute kot njegova predhodnika.

6.2.1 FORMAT SPOROČIL IGMPv3

IGMP-sporočila so obdana (enkapsulirana) v IPv4 z protokolom IP verzije 2. Vsako IGMP-sporočilo je poslano z IP-time-to-live vrednostjo 1, in nosi možnost IP Router Alert v glavi paketa.

Obstajata dva tipa IGMP-sporočil, ki se nanašata na protokol IGMPv3.

Šestnajstiška vrednost	Ime sporočila
0x11	Memberhip query
0x22	Version 3 Membership Report

Izvedba IGMPv3 mora podpirati tri tipe sporočil za delovanje s prejšnjimi verzijami IGMP.

0x12	Version 1 Membership report [RFC-1112]
0x16	Version 2 Membership report [RFC-2236]
0x17	Version 2 Leave Group [RFC-2236]

6.2.1.1 SPOROČILA POVPRAŠEVANJA PO SKUPINI (MEMBERSHIP QUERY MESSAGE)

Max Resp Code – to polje določa maksimalni čas, ki je dovoljen, preden se pošlje poročilo o odzivnosti (responding report).

Group Address – polje je nastavljeno na število 0, ko se pošlje General Querry, in nast.

Querier's Query Interval Code – to polje določa [Query Interval], uporabljen s strani povpraševalca.

Number of Source (N) – polje označuje, koliko izvornih naslovov je predstavljenih v povpraševanju.

Source Adress [i] polje določa vektor IP unicast naslovov, ko je vrednost n v Number of Sources (n) polju.

Obstajajo tri variante sporočil povpraševanja po skupini:

1. »**General Query**« - splošno povpraševanje;
2. »**Group-Specific Query**« - povpraševanje specifične skupine
3. »**Group-and-Source-Specific Query**«.

V IGMPv3 se splošna povpraševanja pošiljajo na IP s ciljnim naslovom 224.0.0.1. Group-Specific in Group-and-Source-Specific povpraševanje se pošiljajo z IP ciljnim naslovom, ki je enak kot multikastni naslov povpraševalca.

6.2.1.2 POROČILO STANJA O SKUPINI (MEMBERSHIP REPORT MESSAGE)

Poročila v verziji 3 se pošiljajo z IP-ciljnim naslovom 224.0.0.22, katera lahko poslušajo vsi usmerjevalniki, ki podpirajo IGMPv3. Sistemi, ki obratujejo na prvi in drugi verziji IMGP, pošiljajo poročila na skupino multicast, ki je določena v skupinskem naslovu polja sporočila.

6.2.2 IMGPv3 S STALIŠČA ČLANOV SKUPINE

Naslov multicast vseh sistemov 224.0.0.1 se upravlja kot poseben primer. Na vseh sistemih – vseh gostiteljih in usmerjevalnikih, vključno usmerjevalnikih multicast – se sprejeti paketi pošljejo na naslov vseh sistemov. Naslov je omogočen na vseh vmesnikih, na katerih je podprt multicast.

Obstajata dva tipa dogodkov, ki sprožita IGMPv3-dogodke na vmesniku:

- sprememba vmesnikovega stanja prejemanja;
- prejem poizvedbe.

Namen protokola IGMP je, da omogoči vsakemu usmerjevalniku multicast, da se nauči za vsako neposredno povezano omrežje, čigar naslovi multicast imajo interes do sistemov povezanih na teh omrežij.

IGMP verzije 3 je omogočil usmerjevalnikom multicast, da se naučijo, kateri viri imajo interes do sosednjih sistemov, za pakete poslane na katerikoli naslov multicast. Če ima usmerjevalnik multicast več kot en vmesnik na istem omrežju, je dovolj, da poganja protokol IGMP na enem izmed teh vmesnikov. Na vsakem vmesniku, ki poganja ta protokol, mora usmerjevalnik omogočiti prejemanje naslova multicast 224.0.0.22 iz vseh virov. Usmerjevalniki multicast morajo vedeti, da je vsaj en sistem na povezanem omrežju zainteresiran za prejemanje paketov iz določenega naslova multicast.

7 BGP (Border Gateway Protocol)

Usmerjanje zajema dve osnovni aktivnosti: iskanje optimalne poti in prenos informacij (označimo jih s paketi) skozi medmrežja. Prenos paketov skozi medmrežja je razmeroma enostaven. Določitev poti pa zna biti po drugi strani precej kompleksna. Protokol, ki prevzema nalogo določanja poti na medmrežju, je Border Gateway Protocol (BGP).

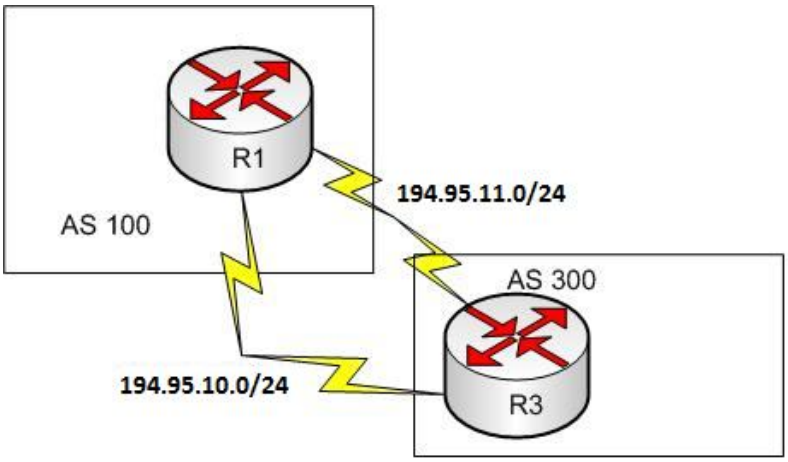
BGP je bil razvit, da nadomesti predhodnika Exterior Gateway Protocol (EGP).

7.1 DELOVANJE BGP

BGP opravlja tri naloge usmerjanja: **usmerjanje med avtonomnimi sistemi, usmerjanje znotraj avtonomnega sistema in usmerjanje skozi avtonomni sistem.** [14]

7.1.1 USMERJANJE MED AVTONOMNIMI SISTEMI

To usmerjanje nastopa med dvema ali več BGP-usmerjevalniki v različnih avtonomnih sistemih. Peer usmerjevalnik uporablja BGP za dosledno ohranjanje pregleda nad topologijo omrežja. Komunikacija BGP-sosedov (usmerjevalnikov) med avtonomnimi sistemi poteka na istem fizičnem omrežju. Internetno omrežje je primer celote, ki uporablja ta tip usmerjanja, ker je sestavljen iz avtonomnih sistemov ali administrativnih domen. Te domene predstavljajo institucije, podjetja, organizacije. BGP se uporablja za določitev poti, da omogoči optimalno usmerjanje znotraj internetnega omrežja. [14]



Slika 7-1: Usmerjanje med avtonomnimi sistemi

7.1.2 USMERJANJE V AVTONOMNEM SISTEMU

Usmerjanje v avtonomnem sistemu nastopi med dvema ali več BGP- usmerjevalniki znotraj enega samega avtonomnega sistema. V tem sistemu usmerjevalniki *peer* uporabljajo BGP za vzdrževanje pregleda topologije medmrežja. BGP se uporablja tudi, da se določi, kateri usmerjevalnik bo služil za povezovanje z eksternimi avtonomnimi sistemi. Tudi v tem primeru bo internet služil kot primer uporabe BGP usmerjanja znotraj avtonomnega sistema. Organizacija, npr. večje podjetje, lahko uporablja BGP za zagotavljanje optimalnega usmerjanja znotraj svoje lastne administrativne domene ali avtonomnega sistema. BGP lahko zagotavlja usmerjevalne storitve med avtonomnimi sistemi in znotraj avtonomnega sistema.

7.1.3 USMERJANJE SKOZI AVTONOMNI SISTEM

Tranzitno usmerjanje se izvaja med dvema ali več usmerjevalniki, ki si izmenjujejo promet skozi avtonomni sistem, na katerem ne teče protokol BGP. V teh avtonomnih sistemih BGP-promet ne izvira v samem avtonomnem sistemu. BGP mora vzpostaviti komunikacijo s tranzitnim sistemom tako, da vmesni protokol uspešno prenaša BGP-promet. [14]

7.2 USMERJANJE V PROTOKOLU BGP

Podobno kot v vsakem usmerjevalnem protokolu, tudi BGP vzdržuje usmerjevalne tabele, pošilja usmerjevalne posodobitve in se na podlagi usmerjevalne metrike odloča, kako bo usmerjal. Glavna funkcija BGP-sistema je izmenjava informacij od dosegljivosti omrežja, vključno z informacijami o seznamu poti avtonomnih sistemov drugih BGP-sistemov. Ta informacija se lahko uporabi za sestavo grafa povezljivosti avtonomnih sistemov, iz katerih se lahko odstranijo slabše smeri in politika, katerega avtonomnega sistema lahko uveljavljamo.

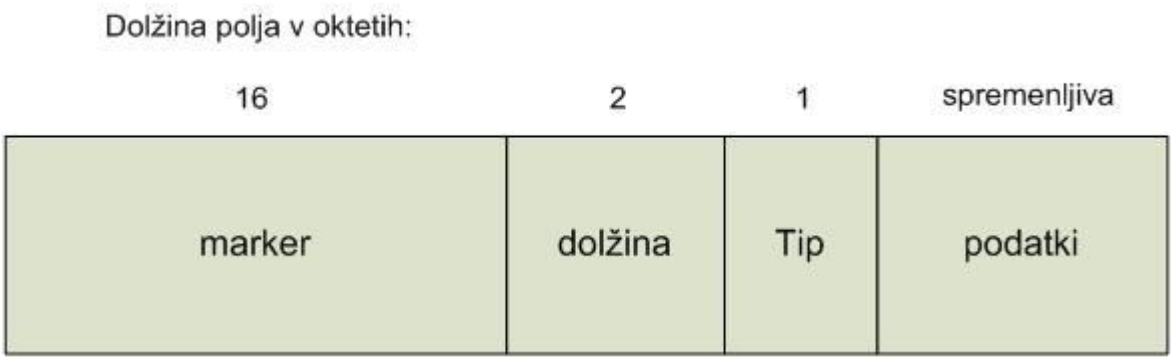
Vsak BGP-usmerjevalnik vzdržuje svojo usmerjevalno tabelo, v kateri so vse možne poti do določenega omrežja. Usmerjevalnik te tabele ne osvežuje, ampak dobiva usmerjevalne informacije preko soležnih usmerjevalnikov toliko časa, dokler se od njih dobiva posodobitve (update).

BGP-naprava izmenjuje usmerjevalne informacije na osnovi prvotne podatkovne izmenjave in po prvotni izmenjavi. Ko se usmerjevalnik prvič poveže na omrežje, BGP-usmerjevalnik z njim izmenja celotno BGP-tabelo. Podobno je, ko se usmerjevalne tabele spremenijo, usmerjevalniki pošljejo delež svojih spremenjenih usmerjevalnih tabel. BGP-usmerjevalniki ne pošiljajo redno posodobitve usmerjevalnih tabel, oglašujejo pa jih samo v smeri najboljše poti.

BGP uporablja eno samo usmerjevalno metriko za določitev najboljše poti do želene mreže. Ta metrika je sestavljena iz poljubne enotne številke, ki označuje prednostno stopnjo želene povezave. Metrika BGP je dodeljena vsaki povezavi (link), določi jo omrežni administrator. Ta vrednost, ki je dodeljena tej povezavi, je lahko osnovana na podlagi števila poti, stabilnosti, hitrosti, zakasnitev ali cene (path passes, stability, speed, delay, cost). [14]

7.3 GLAVA PAKETA BGP

Vsi tipi BGP-sporočil uporabljajo osnovno glavo, sporočila odpri, posodobi in obvesti imajo še dodatna polja, sporočilo vzdržuj pri življenju pa uporablja samo osnovno glavo. [14]



Slika 7-2: Glava paketa BGP [14]

Vsak paket BGP vsebuje glavo, ki določa funkcijo paketa. Polja v glavi paketa pomenijo naslednje:

- Marker – vsebuje vrednost prisotnosti, ki jo lahko sprejemnik sporočila napove.
- Dolžina – določa celotno dolžino sporočila v oktetih (vključno z glavo). Vrednost tega polja mora biti med 19 in 4096.
- Tip – eno-oktetno polje določa naslednji tip sporočil (odpri, posodobi, vzdržuj pri življenju, obvesti).
- Podatki – vsebuje informacije zgoraj ležečega sloja.

7.3.1 TIPI SPOROČIL BGP

V RFC 1771 so navedeni štirje tipi BGP-sporočil [14]:

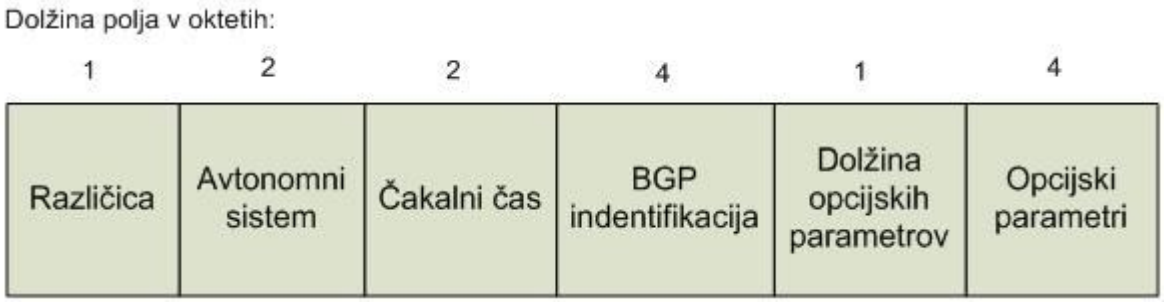
- SPOROČILO ODPRI,
- SPOROČILO POSODOBI,
- SPOROČILO VZDRŽUJ PRI ŽIVLJENJU,
- SPOROČILO OBVESTI.

7.3.2 SPOROČILO ODPRI

To sporočilo odpre BGP-komunikacijsko sejo med soležnimi usmerjevalniki in je prvo sporočilo, ki se pošlje vsaki strani, ko se vzpostavi TCP-seja preko vrat 179. Sporočila odpri se potrdijo preko uporabe sporočil vzdržuj pri življenju, ki se pošljejo s strani soležnega usmerjevalnika in morajo biti sprejeti, preden se začnejo izmenjavati sporočila posodobitev, sporočila vzdržuj pri življenju in sporočila obvesti. [14]

Format sporočila ODPRI

Ta sporočila so sestavljena iz glave in dodatnih polj:



Slika 7-3: Glava sporočila "ODPRI" [14]

Ti paketi dodatno vsebujejo naslednja polja, ki zagotavljajo pogoje zamenjave med dvema BGP-usmerjevalnikoma, da lahko vzpostavita enakovreden odnos [15]:

- Različica – vsebuje številko BGP-različice, da lahko prejemnik ugotovi, če uporablja enako različico kot pošiljatelj.
- Avtonomni sistem – indicira številko avtonomnega sistema pošiljatelja.
- Čakalni čas – določa maksimalen čas v sekundah brez potrdila o sporočilu, preden se predpostavi, da je oddajnik nefunkcionalen.
- BGP-identifikacija – priskrbi identifikacijo BGP pošiljatelja (IP-naslov), ki je določen pri zagonu in je enak za vse lokalne vmesnike ter vse enakovredne BGP.
- Dolžina opcijskih parametrov – določa dolžino neobveznega polja.
- Opcijski parametri – vsebuje seznam neobveznih polj.

7.3.3 SPOROČILA POSODOBI

Sporočila posodobi se uporabljajo za zagotavljanje usmerjevalnih posodobitev, napram ostalim BGP-sistemom, z omogočanjem usmerjevalnikom, da si izoblikujejo dosleden pogled topologije omrežja. Posodobitve se zaradi zanesljive dostave pošiljajo preko protokola TCP. Ta sporočila lahko iz usmerjevalne table odstranijo eno ali več neizvedljivih smeri in lahko hkrati oglašuje in odstranjuje poti. [14]

Slika 7-4: Glava paketa sporočila "POSODOBI" [14]

Paketi BGP, ki označujejo sporočilo Posodobi, vsebujejo naslednja polja [15]:

- dolžina neizvedljivih poti – določa celotno dolžino poti, ki se jih odstranjuje ali pa da ni prisotno;
- poti za odstranitev – vsebuje seznam predpon IP za poti, ki se jih odstranjuje;
- dolžina vseh lastnosti poti – določa celotno dolžino polj z lastnostmi poti ali pa da polje ni prisotno;
- lastnosti poti – opisuje karakteristike oglaševane poti;
- informacije o dosegljivosti na omrežnem sloju – vsebuje seznam prefiksov IP naslovov za oglaševane poti.

7.3.4 SPOROČILA VZDRŽUJ PRI ŽIVLJENJU

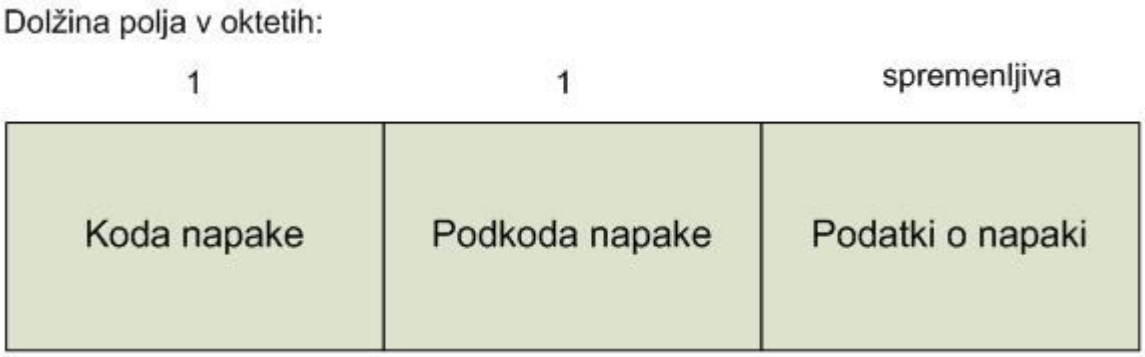
Ta sporočila obveščajo BGP-soležne usmerjevalnike, kdaj je naprava v aktivnem stanju. Ta sporočila se pošiljajo dovolj pogosto, da seja ne poteče. Ta čas je ponavadi ena tretjina Hold time intervala, sporočilo pa ne sme biti poslano hitreje kot v intervalih ene sekunde. Če je čas Hold Time enak nič, potem sporočilo Vzdržuj pri življenju ne sme biti poslano. [14]

7.3.5 SPOROČILA OBVEŠČANJA

Ta sporočila se pošljejo, kadar se zazna napaka. Sporočila obveščanja se pošljejo, da se aktivna seja zapre in da se obvesti povezane usmerjevalnike, zakaj se je ta seja zaprla. [14]

Format paketa BGP za sporočila obvesti

Ta sporočila so sestavljena iz glave in dodatnih polj [15]:



Slika 7-5: Glava sporočila "OBVESTI" [14]

Ta paket se uporablja za opozarjanje na določene napake. Izvorni BGP- usmerjevalnik tako opozori enakovredne usmerjevalnike. Paketi, ki označujejo BGP-sporočilo Obvesti, dodatno vsebujejo naslednja polja [15]:

- koda napake – določa tip napake, ki se je zgodila;
- podkoda napake – določa natančnejše informacije o napaki; vsaka koda napake ima lahko eno ali več pod-kod napake;
- podatki o napaki – vsebuje podatke o prejšnjih dveh poljih; to polje se uporablja za diagnozo vzroka nastanka napake.

8 MPLS (Multi Protocol Label Switching)

MPLS, ali po slovensko večprotokolna komutacija z zamenjavo oznak, je arhitektura, ki omogoča hitro preklapljanje in usmerjanje paketov ter imenuje, usmerja in posreduje tokove paketov skozi omrežje. Bolj specifično, MPLS ima mehanizme, ki omogočajo označevanje IP naslovov v preprostejše fiksno dolge etikete z uporabo paketno posredovalnih ter paketno preklopnih tehnologij. MPLS združuje delovanje in zmogljivosti druge in tretje (povezovalne - preklopi in omrežne - usmerjanje) plasti referenčnega modela ISO/OSI. MPLS leži med podatkovnim (druga plast) in mrežnim (tretja plast) nivojem in je tako pogosto označen kot "2.5 nivojski" protokol. Načrtovan je bil z namenom zagotavljanja storitve prenosa podatkov za tok-krožno in paketno bazirana omrežja, ki imajo isti paketni model. [14]

Glavne lastnosti protokola MPLS [15]:

- **Hitrost in zakasnitve** – preklapljanje na podlagi oznak za razliko od tradicionalnega posredovanja IP-paketov zagotavlja učinkovito rešitev problema zakasnitve in slabe kvalitete IP-omrežij.

- **Razširljivost** – zagotavlja nebolečo razširljivost sistema v primeru povečanja uporabnikov omrežja, saj znakovno preklapljanje večjemu številu IP-naslovov dodeli eno ali več oznak. To zmanjša velikost tabel, ki shranjujejo informacije o naslovih oz. oznakah in dovoljujejo usmerjevalnikom podporo večjega števila uporabnikov.

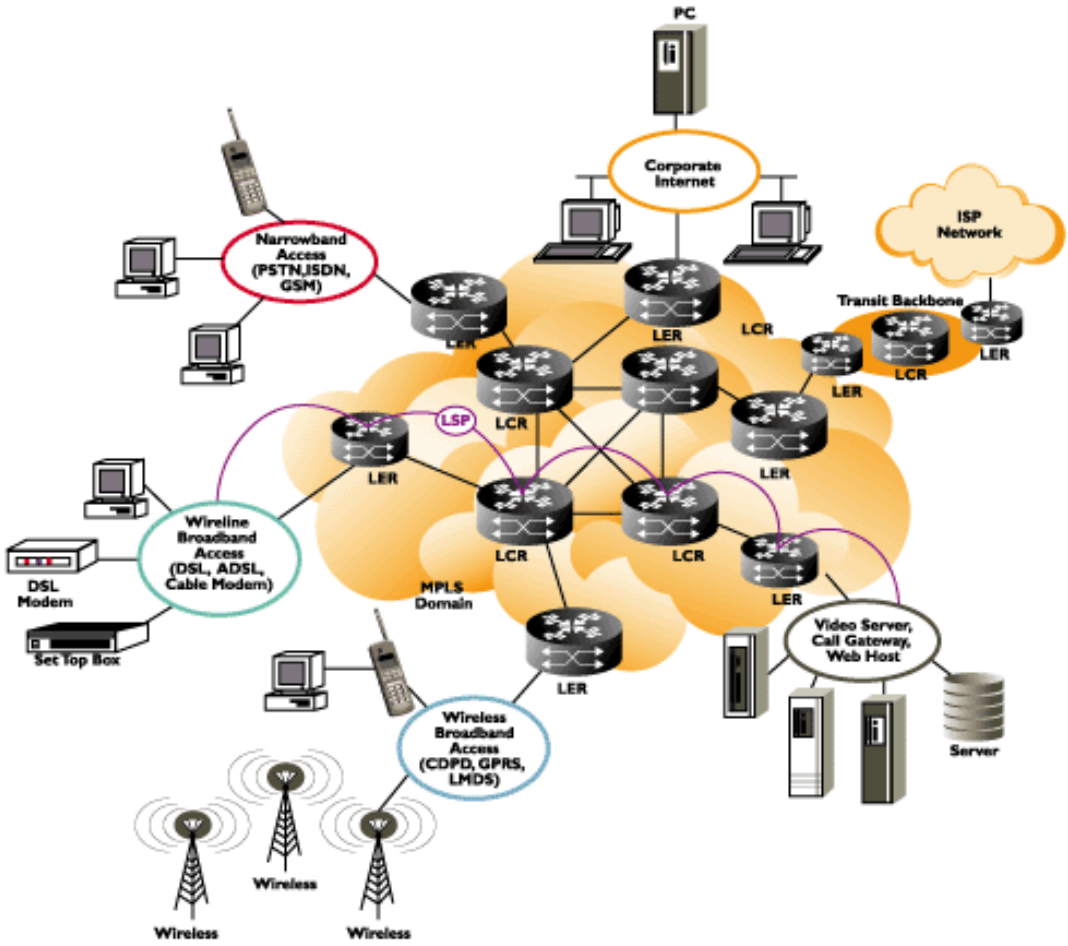
- **Enostavnost** – MPLS je v bistvu posredovalni protokol (oz. skupek protokolov, če upoštevamo še protokole, ki mu pri delovanju pomagajo, npr. BGP, OSPF itd.). Deluje po preprostem principu posredovanja paketov na osnovi oznak.

- **Prilagodljivost** – protokol je pri transportu izredno prilagodljiv in neodvisen od tipa medija, preko katerega se podatki prenašajo. Ponudnikom MPLS-storitev se pri implementaciji storitve ponuja širok spekter različnih tehnologij transporta podatkov, kot so: ATM, Frame Relay (FR), Gigabitni Ethernet itd.

- **Zagotavljanje kakovosti (QoS)** – pri ločevanju vrste prometa in njihovega obravnavanja je MPLS dragoceno orodje za reševanje problemov z zakasnitvami in ostalimi kriteriji za zagotavljanje kvalitete storitev.

8.1 ZGRADBA OMREŽJA MPLS

Usmerjevalnike v MPLS-omrežju v splošnem delimo na vhodne in izhodne robne usmerjevalnike ter hrbtenične usmerjevalnike. Usmerjevalniki, ki imajo vse vmesnike omogočene za MPLS, se imenujejo usmerjevalniki LSR (angl. Label Switch Router). Ti usmerjevalniki analizirajo glavo paketa in na osnovi usmerjevalne topologije na omrežnem nivoju določijo pot L (angl. Label Switch Path), po kateri bo paket potoval, vsakemu paketu pa se na podlagi razvrstitve v različne razrede prometa FEC (angl. Forward Error Correction) doda MPLS-oznaka. Paket se nato posreduje naprej vzdolž LSP-poti preko LSR-usmerjevalnikov, katerih osnovni princip je posredovanje prometa na podlagi zamenjave oznak v glavi paketa. Ko paket prepotuje omrežje, izhodni LSR- usmerjevalnik odigra še zadnjo vlogo in odstrani oznako ter posreduje naprej paket v tradicionalno IP-omrežje.



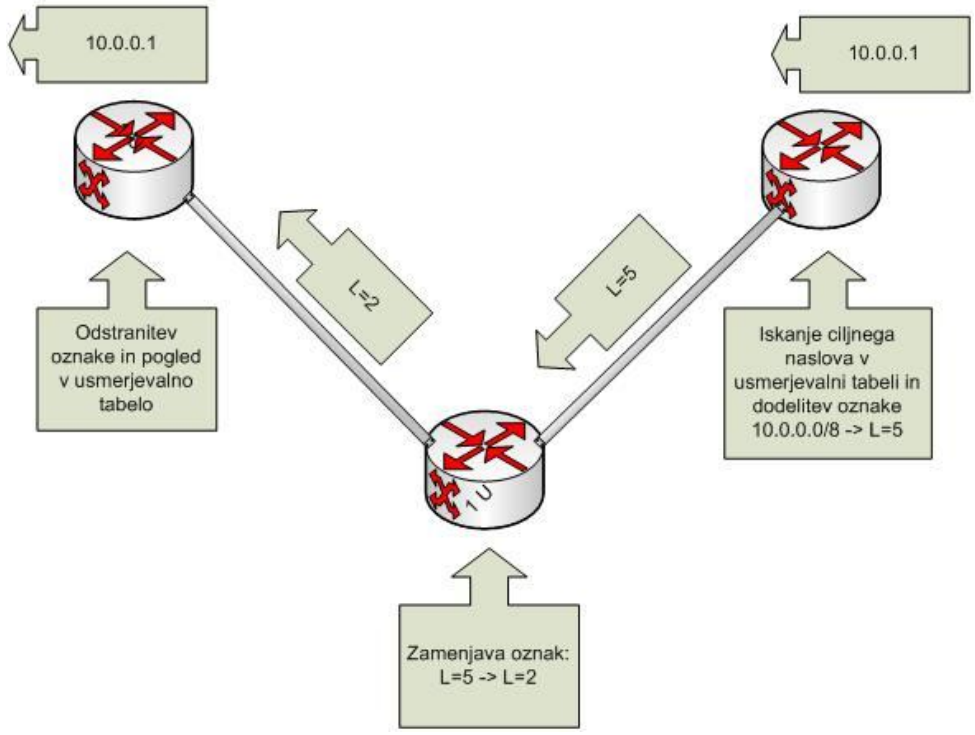
Slika 8-1: Zgradba omrežja MPLS

8.1.1 OZNAKE MPLS

V konvencionalnem posredovanju na tretji plasti, ko paket potuje preko omrežja, vsak usmerjevalnik izvleče vse potrebne informacije iz glave paketa tretje plasti. Ta informacija se naknadno uporablja kot indeks v usmerjevalni tabeli, za določitev naslednjega skoka paketa v omrežju. V večini primerov je naslovni prostor naslovnika edino relevantno polje v glavi paketa, vendar so včasih ustrezna tudi druga polja v paketu. Kot rezultat mora biti analiza glave opravljena neodvisno v vsakem usmerjevalniku, skozi katere paket potuje, kakor tudi vpogled v usmerjevalno tabelo.

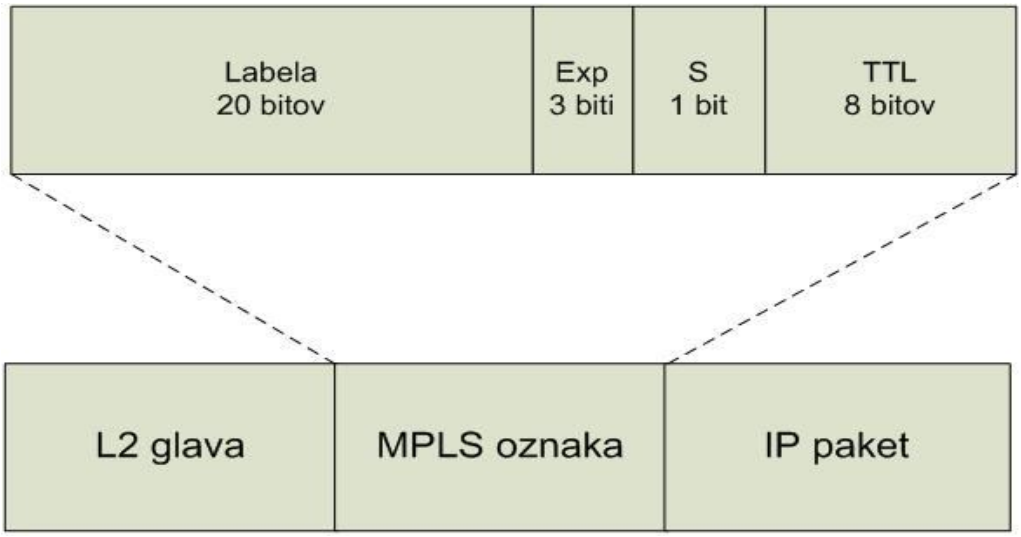
Pri protokolu MPLS je analiza glave na tretji plasti opravljena samo enkrat. Ta glava se preslika v fiksno dolžino nestrukturirane vrednosti, ki jo imenujemo *oznaka.*

Veliko različnih glav se lahko preslika v samo oznako, dokler so te glave rezultat iste izbire naslednjega skoka v omrežju. V veljavi predstavlja oznaka *ekvivalentni posredovalni razred (forwarding equivalence class)* – ki so paketni niz na poti, ki se začne na določenem usmerjevalniku. Začetni izbor oznake ni nujno, da je osnovan samo na podlagi glave na tretji plasti, lahko se tudi osnuje na podlagi politike (*policy*). Ko je oznaka izbrana, se kratka glava oznake postavi na začetek paketa tretje plasti, tako da se vrednost oznake lahko prenaša preko omrežja v paketu. Pred vsakim naknadnim skokom se odločitev o posredovanju izvede z vpogledom v oznako. Ni potrebe po ponovni analizi glave. Ker je oznaka fiksne dolžine in nestrukturirane vrednosti, je vpogled vanjo hiter in preprost. [14]



Slika 8-2: Koncept delovanja protokola MPLS [15]

8.1.1.1 STRUKTURA OZNAKE MPLS



Slika 8-3: Struktura oznake MPLS [15]

- **Oznaka** – vrednost etikete prenaša trenutno vrednost oznake (20 bitov). Ko je etiketiran paket prejet, vrednost etikete na vrhu sklada preveri:

  1. naslednji hop na katerega se usmeri paket;

  2. operacijo, ki se izvede na vrhu sklada pred usmeritvijo; ta operacija lahko zamenja vrhnjo oznako sklada z drugo, ali povleče vrednost iz sklada, ali zamenja vrhnjo vrednost sklada ter potisne eno ali več dodatnih vnosov na to mesto.

- **Exp** – za eksperimentalno uporabo, uporablja se za definicijo razreda Class of Service.

- **S** – dno sklada: ta bit je nastavljen na 1 za zadnji vnos na skladu ter na 0 pri vseh ostalih oznakah vnosov sklada. Če ima vrednost 1, je to zadnja oznaka v paketu.

- **TTL** – Time To Live – življenjska doba polja se uporablja za kodiranje TTL- vrednosti.

8.1.2 DISTRIBUCIJA ETIKET

Vsak usmerjevalnik z označenim stikalom (label switching router, LSR) izvaja neodvisne, lokalne odločitve, katera vrednost oznake bo predstavljala določen ekvivalentni posredovalni razred. Ta oznaka se drugače imenuje *zavezovanje oznak (label binding)*. Vsak LSR obvešča svoje sosede, kadar izvede zavezovanje oznak. To se opravi s pomočjo protokola za izmenjavanje oznak (Label Distribution Protocol, LDP). Ko se označen paket pošlje iz LSR A sosednjemu LSR B, je vrednost oznake v paketu vrednost, ki ji jo dodeli LSR B in predstavlja ekvivalentni posredovalni razred tega paketa. Tako se vrednost oznake spreminja z vsakim skokom paketa skozi omrežje.

8.1.3 MPLS IN USMERJANJE

Oznaka predstavlja ekvivalentni posredovalni razred, ampak ne predstavlja določene poti skozi omrežje. Na splošno je pot skozi omrežje izbrana s strani obstoječih tretje-plastnih usmerjevalnih algoritmov, kot so OSPF, EIGRP in BGP. To pomeni, da na vsakem skoku, ko se izvrši vpogled v oznako, naslednji skok določi dinamični usmerjevalni algoritem. [14]

8.1.4 PROMETNI INŽENIRING MPLS

MPLS je integracija tehnologij druge in tretje plasti. Da se izvedejo tradicionalne lastnosti druge plasti tudi na tretji plasti, MPLS omogoča prometni inženiring. Torej se lahko omogoči enotirno omrežje, ki je lahko doseženo samo s prekrivanjem omrežja na drugi in tretji plasti.

Prometni inženiring MPLS avtomatično vzpostavi in vzdržuje tunel skozi hrbtenično omrežje z uporabo protokola rezervacije virov (resource reservation protocol, RSVP). Pot, ki jo uporabi dani tunel kadarkoli v času, se določi na osnovi tunelove potrebe virov in omrežnih virov, kot je npr. pasovna širina.

Poti tunelov so izračunane v glavi tunela, osnovane na primerni uporabi med potrebnimi in razpoložljivimi viri. IGP avtomatično usmerja promet skozi te tunele. Navadno paket, ki potuje skozi prometno inženiring-MPLS-hrbtenično omrežje, potuje skozi en sam tunel, ki povezuje izvorno točko z ponorno točko. Eden od pristopov za izgradnjo hrbteničnega omrežja je, da definiramo zvezdo tunelov od vsake ponorne naprave do vsake ponorne naprave. IGP, ki upravlja na izvorni napravi, določi, kateri promet naj gre skozi katero ponorno napravo in usmerja ta promet skozi tunel od izvora do ponora. Pri prometnem inženiringu MPLS izračuni poti in signalizacijski moduli določijo pot, ki je sprejeta od tunela LSP ob upoštevanju virov razpoložljivosti in dinamičnem stanju omrežja. Pri vsakem tunelu, se obdrži določeno število poslanih paketov in bajtov.

Občasno je podatkovni tok tako velik, da ne more potekati skozi eno samo povezavo, torej se ne more prenašati preko enega samega tunela. V takih primerih se nastavi več tunelov med enim izvorom in ponorom, podatkovni tok pa se deli med njimi. [14]

Družina protokola MPLS vsebuje [17]:

- MPLS: MPLS-arhitektura;
- MPLS povezanih usmerjevalnih signalizacijskih protokolov kot so BGP, ATM , OSPF itd.;
- LDP: protokol za distribucijo oznak;
- CR-LDP: protokol za izmenjevanje oznak z omejitvami;
- RSVP-TE: protokol rezervacije virov - prometni inženiring.

8.2 SIGNALIZACIJSKI PROTOKOLI MPLS

Danes se uporabljajo trije različni signalizacijski protokoli za upravljanje MPLS- poti: LDP (Label Distribution Protocol), RSVP (Resource Reservation Protocol) in CR-LDP (ang. Constraint Based - LDP). LDP se izvaja po skokih in izbere isto fizično pot, kakor bi jo IGP (Interior Gateway Protocol) protokol ter podpira manjšo kompleksnost LSP-poti. RSVP je že znan protokol, ki omogoča razširljivost na eksplicitno določene smeri in distribucije oznak. Uporablja se s strani internetnih operaterjev v produkcijskih omrežjih. CR-LDP razširja protokol LDP s podporo eksplicitno določenih smeri z enako funkcionalnostjo kot RSVP. IETF je podprl vse tri standarde za signalizacijo v protokolu MPLS.

8.2.1 LDP

V MPLS-omrežju se morata dva označeno komutirana usmerjevalnika uskladiti o pomenu oznak, ki se uporabljajo za razpošiljanje prometa med in skozi njiju. Protokol za distribucijo oznak (*Label Distribution Protocol, LDP*) je protokol, ki opredeljuje sklop postopkov in sporočil, s katerim eden LSR obvesti drugega, kakšne vezave oznak je opravil.

LSR uporablja omenjeni protokol za vzpostavitev označeno komutirane poti skozi omrežje, tako da pripne informacijo usmerjanja na omrežni plasti neposredno v označeno komutirane poti (LSP) povezovalne plasti. Te LSP imajo lahko ponorno točko na svojem sosedu ali pa na izhodnem vozlišču nekje v omrežju. Na vsak ustvarjen LSP je povezan s svojim ekvivalentnim posredovalnim razredom. Ta razred določa, kateri paket se pripne na kateri LSP. Dva LSP-usmerjevalnika, ki uporabljata LDP za izmenjavo informacij o pripetih oznakah, sta imenovana kot LDP-soležna usmerjevalnika, ki imata med seboj vzpostavljeno LDP-sejo. Pri eni sami seji mora vsak soležni usmerjevalnik znati sam poiskati informacije o pripetih oznakah, ali drugače povedano, je dvosmerni protokol. [18]

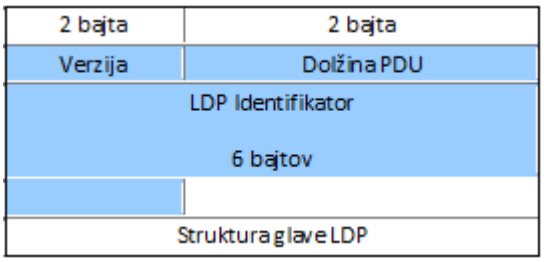
OBSTAJAJO ŠTIRI VRSTE SPOROČIL LDP:

- sporočila odkritja (*Discovery messages*),
- sejna sporočila (*Session messages*),
- oglaševalna sporočila (*Advertisement messages*),
- sporočila obveščanja (*Notification messages*).

Vse sporočila LDP imajo skupno strukturo, ki uporablja shemo kodiranja Tip-Dolžina-Vrednost (TLV). To TLV-kodiranje se uporablja za kodiranje večine informacij prenesenih preko LDP-sporočil. Vrednosti del TVL-kodiranega objekta lahko vsebuje eno ali več TVL-zapisov.

Sporočila se pošiljajo kot LDP PDU. Vsak PDU lahko vsebuje eno ali več LDP- sporočil. Vsaj LDP PDU predstavlja LPD-glavo, ki ji sledi eno ali več LDP-sporočil.

Slika 8-4 prikazuje strukturo LDP-glave [18]:



Slika 8-4: Struktura glave LDP

Verzija
Številka verzije protokola.

Dolžina PDU
Celotna dolžina PDU brez polja dolžine verzije ter polja dolžine PDU.

LDP-identifikator
To polje enolično označeni prostor pošiljanja LSR, za katerega zaprosi PDU. Prve štiri oktete kodirajo IP-naslovni prostor, ki je dodeljen LSR, zadnja dva pa nakazujeta prostor oznake znotraj LSR.

8.2.2 RSVP-TE

Protokol z rezervacijo virov s prometno razširitvijo (ang. RSVP traffic extension - RSVP-TE) je nadgradnja protokola RSVP.

Protokol RSVP vzpostavi sejo, kot je podatkovni tok s specifično destinacijo in protokolom TCP. V kombinaciji RSVP z MPLS lahko tok podatkov ali sejo določimo bolj prožno. Vstopni usmerjevalnik LSP poti uporablja številne metode, da ugotovi, h kateri oznaki spadajo določeni paketi. Ko je oznaka dodeljena množici paketov, ta oznaka definira paketni tok skozi LSP. Pri tem označujemo LSP kot LSP-tunel, ker je promet nejasen vsem vmesnim vozliščem skozi označeno komutirano pot.

RSVP dovoljuje uporabo *izvornega usmerjanja*[1], kjer vstopni usmerjevalnik določi celotno pot skozi omrežje. Vstopni usmerjevalnik lahko uporablja *izračun omejene prve najkrajše poti* (Constrained Shortest Path First) za določitev ciljne poti. Izračunana pot se nato uporablja za vzpostavitev označeno komutirane poti. [18]

9 NAVIDEZNA ZASEBNA OMREŽJA (VIRTUAL PRIVATE NETWORKS - VPN)

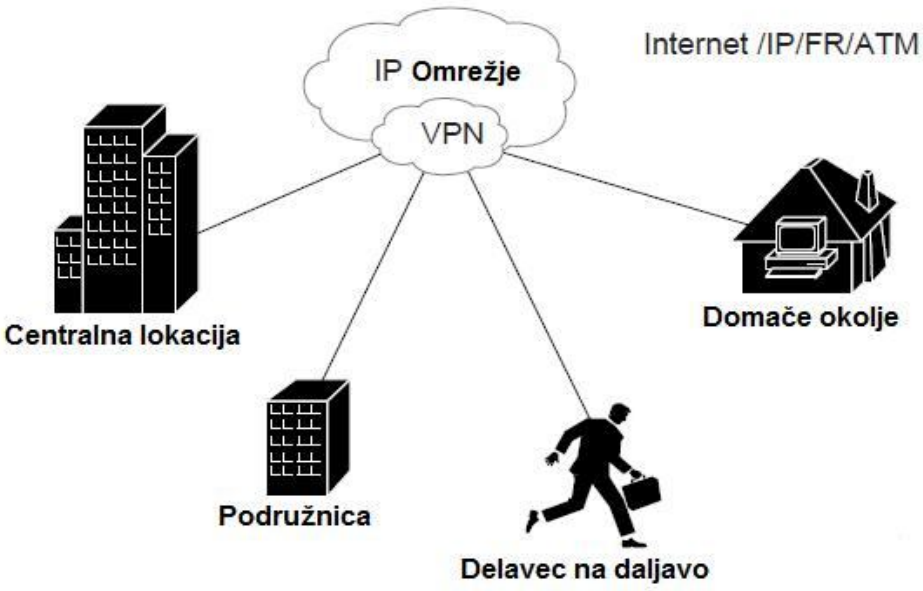
Navidezna zasebna omrežja (v nadaljevanju VPN) so opredeljena kot omrežja podjetja ali organizacije, ki so razporejena na deljeni oziroma skupni infrastrukturi internetnega ponudnika in delujejo z enakimi lastnostmi kot privatno omrežje. VPN je varno, IP-osnovano omrežje, ki uporablja vire na enem ali več fizičnih omrežjih. VPN vsebuje geografsko razpršene lokacije, ki komunicirajo med seboj preko skupnega hrbteničnega omrežja.

Ostajajo trije tipi VPN, ki usklajujejo, kako jih podjetja in organizacije uporabljajo:

- **Dostopovna VPN (Access VPN)** – omogočajo oddaljeni dostop do podjetjevega intranet ali ekstranet omrežja preko deljene infrastrukture. Dostopovna VPN omogočajo uporabnikov da dostopajo do podjetjevih virov kadarkoli in kjerkoli. Dostopovna VPN zajemajo analogne, klicne, DSL, mobilne, kabelske in optične tehnologije za varno povezljivost mobilnih uporabnikov ter delavcev na daljavo in podružnic.

- **Intranet VPN** – povezuje centralno lokacijo organizacije, podružnice in oddaljene pisarne preko deljene infrastrukture z uporabo dodeljenih povezav (dedicated connections). Poslovanje uživa enake privilegije ter omejitve kot privatno omrežje, vključujoč varnostni vidik, zagotavljanje storitev (QoS), upravljanje ter zanesljivost.

- **Ekstranet VPN** – povezuje stranke, dobavitelje, partnerje ali interesne skupine v korporativni intanet preko deljene infrastrukture z uporabo dodeljenih povezav. Tudi pri tem tipu VPN uživa poslovanje enake privilegije in omejitve kot Intranet VPN.



Slika 9-1: Logično topološki pogled VPN

9.1 IP VPN

V privatnih lokalnih omrežjih (LAN) so IP-osnovana intranet omrežja drastično spremenila način poslovanja in delovanja podjetij ter organizacij. Združbe selijo svoje poslovne aplikacije na intranetna omrežja in jih preko prostranega omrežja (WAN) razširijo še na svoje oddaljene lokacije. Združbe z uporabo ekstraneta (intranet, ki obkroža več podjetij) zajemajo tudi potrebe svojih strank, dobaviteljev in poslovnih partnerjev. Ekstranet omogoča podjetjem, da zmanjšajo stroške poslovnih procesov z avtomatizirano dobavno verigo, elektronsko izmenjavo podatkov (EDI) ter drugimi oblikami omrežnega poslovanja. Da bi izkoristili to poslovno priložnost, morajo imeti ponudniki internetnih storitev infrastrukturo IP VPN, ki omogoča zasebne omrežne storitve preko javne infrastrukture oziroma preko hrbteničnega omrežja internetnega ponudnika.

Za učinkovito izvajanje IP VPN v ISP-omrežju je potrebno zagotoviti naslednjim kriterijem:

Zasebnost (Privacy) – vsa IP VPN ponujajo zasebnost preko deljene (javne) omrežne infrastrukture. Večina združb uporablja šifriran tunel. Ta je samo eden izmed mnogih načinov zagotavljanja omrežne in podatkovne zasebnosti.

Razširljivost (Scalability) – za pravilno zagotavljanje storitev morajo VPN služiti do več sto tisoč spletiščem in uporabnikom. VPN je tudi orodje za upravljanje storitev pri internetnih ponudnikih za nadzor dostopa do storitev. Na primer zaprta skupina uporabnikov podatkovnih in glasovnih storitev.

Prilagodljivost (Fleksibilnost) – IP VPN morajo znati ravnati v kakršnihkoli vzorcih podatkovnega prometa v združbinem intranetu in ekstranetu, v katerih promet ne teče več samo proti/in s centralne lokacije. VPN morajo tudi imeti zmožnost prilagajanja, da lahko hitro dodajo nova mesta, povežejo uporabnike preko različnih medijev in izpolnjujejo vse bolj napredne tipe prometa ter zagotavljajo pasovna širino novim intranetnim aplikacijam.

Predvidljivo delovanje (Predictable Performance) – delovanje se lahko razlikuje glede na zahteve različnim vrstam storitev, vendar s skupno zahtevo, da je delovanje predvidljivo. Primeri stopenj performančnih zahtev zajemajo:

- oddaljeni dostop za mobilne uporabnike – zahteva razširjeno povezljivost;
- poslovalnice – zahteva trajnostno raven zmogljivosti zaradi interaktivne narave intranetnih aplikacij v podružnici;
- video konference – zahtevajo posebne parametre.

IP VPN *označujemo tudi z imenom* ***LAYER3 VPN*** *oziroma VPN na tretji plasti.*

9.2 MPLS VPN

MPLS VPN omogoča ponudnikom internetnih storitev, da razporedijo razširljive VPN in gradijo temelje za zagotovitev storitev z dodano vrednostjo vključujoč v nadaljevanju opisane storitve.[20]

Nepovezana storitev (Connectionless Service)

Nepovezana storitev je storitev, v kateri se prenašajo podatki, ne da bi se pred tem vzpostavljala zveza med udeleženci v komunikaciji. Da lahko v takšnem IP okolju vzpostavimo zasebnost, trenutne VPN-rešitve naložijo usmerjene, točka-točka, prekrivne povezave. Vendar tudi ko se izvaja preko nepovezanega omrežja, VPN ne zna izkoristiti prednosti lahke povezljivosti in možnosti več storitev na takšnem omrežju. Ko vzpostavimo VPN preko nepovezanega omrežja, še vedno potrebujemo tunele in šifriranje za omrežno zasebnost/varnost, s tem pa tudi odpravimo bistveno kompleksnost.

Centralizirana storitev (Centralized Service)

Gradnja VPN v tretji plasti omrežja dopušča dostavo ciljno usmerjene storitve na skupino uporabnikov, ki jih zastopa VPN. VPN internetnim ponudnikom zagotavlja več kot le mehanizem za zasebno povezavo uporabnikov do intranet storitev. Zagotavlja tudi prožen način dostave storitev z dodano vrednostjo ciljnim kupcem. Razširljivost je ključnega pomena, ker želijo stranke uporabljati storitve zasebno v njihovih intranet in ekstranet aplikacijah. Ker so MPLS VPN vidni kot privatna intranet omrežja, lahko uporabljamo IP-storitve, kot so:

- multicast,
- zagotavljanje kakovosti storitev (QoS),
- IP-telefonija,
- centralizirane storitve, vključno z vsebino.

Lahko se prilagodi več kombinacij specializiranih storitev za posamezne kupce. Na primer: specializirana storitev, ki združuje IP multicast z nizko zakasnitvijo storitev, omogoča videokonference v intranetu.

Razširljivost (Scalability)

Če ustvarimo VPN na osnovi usmerjene, točka-točka, prekrivne povezave, Frame Relay, ATM, ali navidezne povezave (VC), je ključna pomanjkljivost VPN njegova nezmožnost razširitve. Točneje, povezavna VPN brez povezave full mesh med strankinimi lokacijami niso optimalna. Namesto tega uporabljajo model MPLS VPN peer in brezpovezavno arhitekturo tretje plasti za spodbujanje visoko razširljive VPN-rešitve. Model peer zahteva, da se stranka povezuje s samo enim ponudnikovim PE-robnim (Provider Edge) usmerjevalnikom, v nasprotju z vsemi ostalimi strankinimi lokacijami ali strankinimi CE- robnimi (Customer Edge) usmerjevalniki, ki so člani VPN. Brezpovezavna arhitektura omogoča kreiranje VPN v tretji plasti, s čimer je odpravljena potreba za tunele ali VC. Druga vprašanja glede razširljivosti MPLS VPN so posledica delitve VPN poti med PE-usmerjevalniki in nadalje delitev VPN- in IGP-poti med PE-usmerjevalniki in ponudnikovimi P- usmerjevalniki v jedru omrežja.

- PE-usmerjevalnik mora vzdrževati VPN-poti za tiste VPN, ki so člani.
- P-usmerjevalniki ne vzdržujejo nobene VPN-poti.

To povečuje razširljivost ponudnikovega jedra omrežja in zagotavlja, da nobena naprava ne predstavlja ozkega grla.

Varnost – (Security)

MPLS VPN ponuja isti tip varnosti kot povezavna VPN. Paketi iz enega VPN ne gredo nenamerno k drugemu VPN. Varnost se zagotavlja:

1. na robu ponudnikovega omrežja, z zagotavljanjem, da se prejeti paketi od stranke usmeri v pravi VPN;
2. na hrbteničnem omrežju se VPN-promet hrani ločeno. Zlonamerno sleparjenje (poskus, da pridobijo dostop do PE-usmerjevalnika) je skoraj nemogoče, ker so paketi prejeti od strank v IP-obliki.

Lahko kreiranje – (Easy to Create)

Da v celoti izkoristimo vse prednosti VPN, mora biti enostavno za stranke, da ustvarijo nove VPN ter uporabniške skupine. Ker so MPLS VPN brezpovezavne, ne potrebujemo posebnih map povezav ter topologij. Intranetu ali ekstranetu se lahko dodaja lokacije in formira zaprte uporabniške skupine. Ko se ureja VPN-lokacije na tak način, se omogoči članstvo v kateremkoli mestu v več VPN, poveča se tudi fleksibilnost v gradnji intranet in ekstranet lokacij.

Prilagodljivo naslavljanje (Flexible addressing)

Da zagotovimo VPN-storitvam večjo dostopnost, lahko stranke same zasnujejo svoj naslovni prostor, ločen od naslovnega prostora drugih strank. Večina strank uporablja privatni naslovni prostor, obrazložen v RFC 1918. MPLS VPN dopušča uporabnikom uporabo njihovega naslovnega prostora brez prevajanja omrežnih naslovov (NAT), ki omogoča javni in privatni pogled določenega naslova. NAT je potreben samo v primeru, kadar se želita povezovati dve VPN-lokaciji, katerih naslovni prostor se prekriva. Strankam to omogoča, da uporabljajo svoje neregistrirane zasebne naslove in komunicirajo preko javnega IP-omrežja.

Podpora integriranemu razredu storitev (CoS)

CoS je pomembna zahteva mnogih uporabnikov IP VPN. Zagotavlja sposobnost obravnave dveh temeljnih VPN-zahtev:

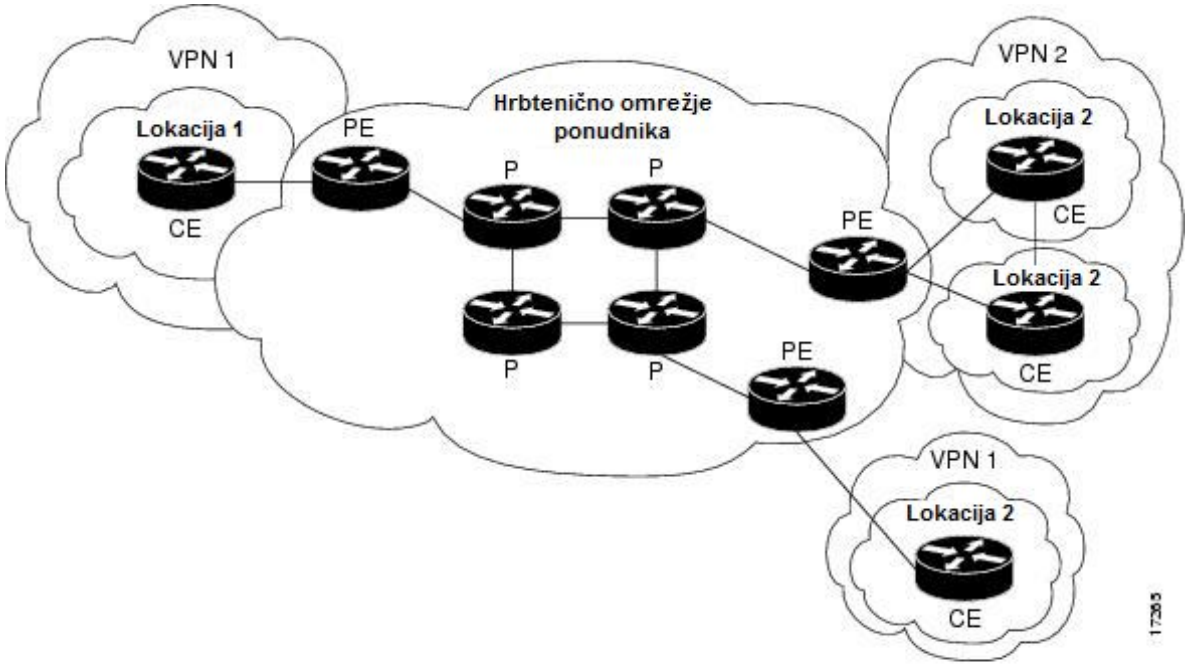
1. predvidljivo delovanje in izvajanje politike,
2. podpora za več ravni storitev v MPLS VPN.

Omrežni promet je razvrščen in označen na robu omrežja, pred samo agregacijo prometa, ki se izvršuje v jedru omrežja. Promet na robu in jedru omrežja se potem loči v različne razrede, ki delujejo na podlagi politike zakasnitve ali opuščanja paketov.

Enostavna migracija (Straightforward Migration)

Za hitri vnos VPN-storitev uporabljajo ponudniki enostavno migracijsko pot (straightforward migration path). MPLS VPN so edinstveni, ker jih lahko gradimo preko več različnih omrežnih arhitektur, kot so IP, ATM, Frame Relay in hibridna omrežja. Migracija je olajšana za končne stranke, ker ni zahteve po MPLS-podpori na strankinem robnem usmerjevalniku (CE) in tudi ni potrebe po spremembi na strankinem intranetu.

VPN na ponudnikovem hrbteničnem omrežju.

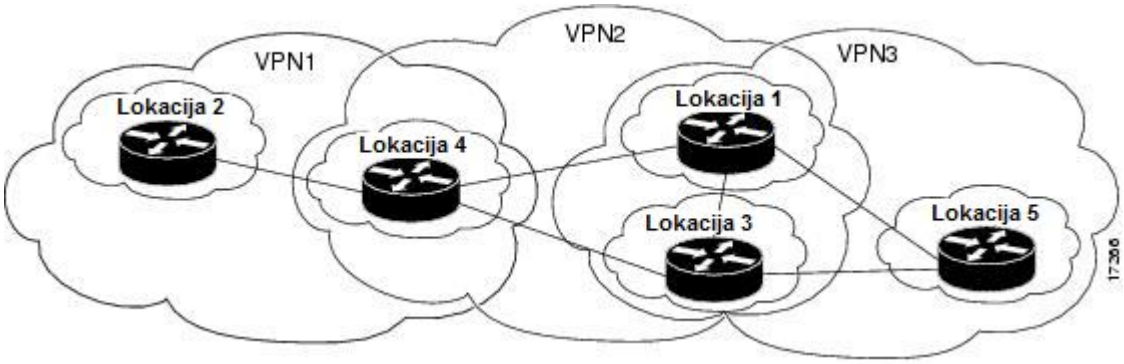


Slika 9-2: Prikaz MPLS VPN na ponudnikovem omrežju [20]

VPN je sestavljen iz strankinih naprav, povezanih na CE-usmerjevalnike. Te strankine naprave uporabljajo VPN za izmenjavo podatkov med seboj. Samo PE-usmerjevalniki so seznanjeni z VPN.

Slika 9-3 prikazuje pet strankinih lokacij, ki komunicirajo preko treh VPN- povezav. Te VPN lahko komunicirajo preko naslednjih lokacij:

- VPN1 – lokaciji 2 in 4,
- VPN2 – lokacije 1,3 in 4,
- VPN3 – lokacije 1,3 in 5.



Slika 9-3: Lokacije uporabnika znotraj VPN [20]

9.3 DELOVANJE VPN

9.3.1 VRF

Vsako VPN je povezano z eno ali več VPN-usmerjevalnih/posredovalnih instanc (VRF). VRF opredeljuje VPN-članstvo uporabnika, vezanega na PE-usmerjevalnik. VRF je sestavljen iz IP-usmerjevalne tabele (pridobljene iz Cisco Express Forwarding – CEF), množice vmesnikov, ki uporabljajo omenjeno usmerjevalno tabelo, in množice pravil ter parametrov usmerjevalnih protokolov, ki nadzirajo informacije vključene v usmerjevalno tabelo.

VPN Skupnosti ciljne poti - VPN (VPN Route Target Communities)

Distribucija VPN-usmerjevalnih informacij je nadzorovana skozi uporabo VPN- skupnosti ciljne poti, ki jih izvaja protokol BGP. Distribucija VPN-usmerjevalnih informacij deluje:

- ko se pridobljena/naučena VPN iz CE-usmerjevalnika inicira v BGP- tabelo, se nanjo navezuje seznam skupnosti ciljne poti (RT). Običajno je seznam RT izvozna množica ciljnih poti, povezanih z VRF, iz katerih je bila pot naučena.
- Uvozni seznam RT-skupnosti se navezuje na vsak VRF. Uvozni seznam označuje RT-atribute, ki jih mora imeti pot, da se uvozi v VRF. Na primer, če uvozni seznam za določeni VRF vsebuje RT-skupnosti A, B in C, potem je katerakoli VPN-pot, ki nosi katerokoli od omenjenih RT-skupnosti – A, B in C uvozi v VRF.

9.3.2 DISTRIBUCIJA BGP USMERJEVALNIH INFORMACIJ VPN

Omrežja BGP/MPLS VPN na tretji plasti predstavljajo navidezna zasebna omrežja, katera so primerna za tiste uporabnike, ki imajo več lokalnih omrežij na več različnih lokacijah in želijo za povezavo teh omrežij koristiti skupno infrastrukturo ponudnika storitev oziroma je to mehanizem, ki ponudniku storitve omogoča, da preko svojega IP hrbteničnega omrežja ponuja storitev IP VPN svojim naročnikom. BGP/MPLS VPN je pogosto imenovan tudi *Layer 3 VPN*, temelji pa na MPLS-posredovanju in protokolu BGP za izmenjavo VPN- informacij

Robni usmerjevalnik ISP (PE) se lahko nauči IP-predpono od robnega strankinega (CE) usmerjevalnika preko statične konfiguracije, skozi BGP-sejo ali preko dinamičnih usmerjevalnih mehanizmov (OSPF, EIGRP) s strani CE- usmerjevalnika. Ta IP-predpona je član IPv4-družine naslovov. Ko se PE- usmerjevalnik nauči omenjeno IP-predpono, jo pretvori v VPN-IPv4-predpono, ki jo združuje z 8-bitnim razločevalnikom usmerjevalnih smeri (RD). Generirana predpona je član VPN-IPv4-družine naslovov. Služi za enkratno identifikacijo strankinega naslova, tudi če strankina stran uporablja globalno neunikatne (neregistrirane zasebne) IP-naslove.

Usmerjevalnik smeri (RD), ki se uporablja za pridobitev VPN-IPv4-predpone, je določen s komandami, povezanimi z VRF na PE-usmerjevalniku.

BGP distribuira dostopne informacije VPN-IPv4-predpone za vsak VPN. BGP-komunikacija poteka na dveh nivojih: znotraj domene, ki jo imenujemo avtonomni sistem (notranji BGP ali IBGP), in med avtonomnimi sistemi (zunanji BGP ali EBGP). Seje med PE-PE ali PE-RR (route reflector) so IBGP-seje, PE-CE- seje pa imenujemo EBGP-seje.

BGP propagira dostopne informacije za VPN-IPv4-predpone med PE- usmerjevalniki z uporabo večprotokolnih BGP-razširitev (RFC 2283), ki označujejo podporo za naslovne družine, ki niso IPv4. To počne tako, da so bile poti določenega VPN naučene preko ostalih članov VPN.

Operater preko zasebnih omrežij MPLS/BGP VPN ponudi storitve, kot so multicast, zagotavljanje kvalitete storitve (QoS), podpora telefoniji znotraj VPN, centralizirana storitev vsebinskega in spletnega gostovanja znotraj VPN. VPN omogoča tudi združevanje specializiranih storitev za posamezne naročnike. Npr. storitev, ki združuje IP-multicast z razredom storitev, ki imajo nizko zakasnitev, omogoča videokonference v zasebnem omrežju. Varnost MPLS VPN je na enakem nivoju kot povezavno orientirani IP VPN in je zagotovljena tako, da paketi iz nekega VPN-omrežja ne morejo prestopiti v napačnega, ampak priletijo v pravilen VPN zaradi varnostne politike na robu operaterjevega omrežja. Lahko pa se izvaja tudi na hrbtenici omrežja, kjer se ločuje VPN-promet.

9.3.3 POSREDOVANJE MPLS

Glede na usmerjevalne informacije, shranjene v usmerjevalni tabeli VRF IP in tabeli VRF CEF, se paketi posredujejo do cilja z uporabo MPLS. PE-usmerjevalnik pripne oznako na predpono vsake stranke, ki se je nauči iz CE-usmerjevalnika. Predpona vključuje oznako o dostopnosti omrežja za omenjeno predpono, ki jo PE-usmerjevalnik oglašuje na ostale PE-usmerjevalnike. Ko PE-usmerjevalnik posreduje paket, ki ga dobi od CE- usmerjevalnika preko ponudnikovega omrežja, in ko ciljni PE-usmerjevalnik sprejme označen paket, označeno oznako uporabi za usmerjanje paketa proti pravemu CE-usmerjevalniku. Označeno pošiljanje preko ponudnikove hrbtenice temelji na dinamični označeni komutaciji ali prometnem inženiringu. Uporabnikovi podatkovni paketi nosijo dva nivoja oznak, ko prečkajo hrbtenično omrežje:

1 vrhnja oznaka usmeri paket proti pravemu CE-usmerjevalniku;

2 druga oznaka navaja kako naj PE-usmerjevalnik pošilja paket proti CE-usmerjevalniku.

9.4 KORISTI UPORABE IP VPN

IP VPN so privlačna, ker:

1 zmanjšujejo stroške povezovanj med poslovalnicami, delavci na daljavo oz. mobilnimi uporabniki do družbinega intraneta, ki deluje preko javnega interneta.

2 so stroškovno bolj učinkoviti kot zasebna WAN izdelana preko zakupljenih vodov.

Vendar pa standardni VPN ne eskalirajo dobro. Ti temeljijo na ustvarjanju in ohranjanju polne mreže predorov ali stalna virtualna vezja vseh straneh, ki pripadajo določenemu VPN z uporabo:

- IPSec,
- protokola za tuneliranje v drugem sloju (L2TP),
- posredovanja na drugem sloju (L2F),
- generičnega ovijanja pri usmerjanju (GRE),
- Frame Relay,
- protokola ATM.

Režija potrebna za določitev in vzdrževanje teh povezavnih shem ne more biti omogočena v ponudnikovem omrežju, ki vzdržuje na stotine ali tisoče VPN, od katerih ima vsako na desetine ali stotine lokacij in poti.

MPLS VPN se ustvarjajo na tretji plasti, so brezpovezavna, in zato tudi bistveno bolj razširljiva in enostavnejša za gradnjo in vzdrževanje kot običajna VPN. Poleg tega lahko dodamo storitve z dodano vrednostjo, kot so aplikacije in gostovanje podatkov, omrežne poslovne aplikacije in telefonske storitve. Ponudnikovo hrbtenično omrežje obravnava vsak MPLS VPN kot ločeno, brezpovezavno IP-omrežje.

MPLS VPN ponujajo:

- platformo za hitro uvajanje IP-storitev z dodano vrednostjo, kot so intranet, ekstranet, VoIP, večpredstavnost in omrežno poslovanje …;
- zasebnost in varnost je enaka kot VPN-omrežja na drugi plasti, tako da se omejuje distribucijo VPN-poti samo na tiste usmerjevalnike, ki so v določenem VPN;
- nemoteno integracijo strankinega intraneta;
- večjo razširljivost v trenutni VPN-implementaciji, z več tisoč lokacijami v VPN in na sto tisoče VPN na ponudnika storitev;
- IP Class of Service (COS) s podporo za več razredov storitev in prednostne naloge znotraj VPN, kot tudi med VPN;
- upravljanje VPN-članstva in rezervacij za nove VPN.

10 MULTICAST VPN

Ker narašča globalno povpraševanje in potreba po VPN-storitvah, narašča tudi potreba po servisih multicast VPN (mVPN). V zadnjih desetih, petnajstih letih se je multicast najbolj razširil na področju finančnih aplikacih (borza), prenosu softvera ter multimedijskih vsebin. Pred tehnologijo mVPN je bil edini način za podporo multicasta preko MPLS-omrežja, da ponudnik storitev zgradi ročne, generične, usmerjevalne (GRE) tunele med vsakim virom ter sprejemnikom. Zaradi visokih administrativnih stroškov takšna konfiguracija predstavlja (pre)velik izziv tudi za podjetja z majhnim številom lokacij in strank.

REŠITEV MULTICAST VPN CISCO

Leta 2002 je Cisco Systems® za potrebe trga predstavil praktično rešitev imenovano Multicast VPN (mVPN). Je lahko vzpostavljiva, visoko razširljiva in ima minimalne stroške realizacije ter upravljanja. S tehnologijo Cisco mVPN je ponudniku omogočeno dinamično zagotavljanje podpore multicast preko MPLS-omrežij. Arhitektura mVPN uvaja dodatni niz protokolov in postopkov, ki ponudniku storitev pomagajo omogočiti promet multicast v VPN. Tehnologija dopušča pregledni transport uporabnikovega prometa IP-multicast preko ponudnikovega hrbteničnega omrežja in je integrirana v storitev Cisco IOS unicast MPLS VPN. To omogoča ponudnikom, da svojim VPN-strankam ponuja storitve multicast kot dodatek trenutnim storitvam unicast VPN. [25]

10.1 DELOVANJE MVPN

Rešitev Cisco MVPN temelji na IETF Rosen draft (trenutna verzija je draft-rosen-vpn-mcast-11.txt). Podpira pravo dinamično naravo multicast aplikacij, ki so sprožene na strani sprejemnika, in zagotavljajo vse ponudnikove in uporabnikove potrebe. MVPN-rešitev uporablja GRE v povezavi z multicast- distribucijskim drevesnim (MDT) usmerjanjem, da omogoči razširljivost obstoječe tehnologije IP-multicast jedru omrežja. Cisco mVPN temelji na rešitvi Multicast Domain z najvišjo stopnjo optimizacije vgrajene v rešitev Cisco s pomočjo privzetega MDT in podatkovnimi MDT skalabilnimi razširitvami.

V omrežju MPLS VPN ima jedrni usmerjevalnik P-funkcijo ohranjanja usmerjevalnih informacij in oznak samo za globalno usmerjevalno tabelo. To pomeni, da ne drži usmerjevalnih in ostalih informacij o strankinem VPN. Strankin robni usmerjevalnik - CE vzdržuje sosedstvo samo z ponudnikovim robnim usmerjevalnikom – PE. CE-usmerjevalniki

ne vzpostavljajo povezave z drugimi CE-usmerjevalniki, imajo pa sposobnost dostopanja do njih preko VPN skozi najbolj optimalno pot na ponudnikovem omrežju. [25]

V ponudnikovem omrežju, ki ima omogočen multicast VPN, P-usmerjevalnik vzdržuje multicast samo v globalni tabeli in ne vsebuje informacij o uporabnikovih VPN-povezavah. Uporabnikov CE-usmerjevalnik vzdržuje sosedstvo multicast PIM samo z svojim sosedom. CE-usmerjevalniki nimajo vzpostavljenih povezav multicast z drugimi CE-usmerjevalniki, lahko pa si izmenjujejo informacije multicast preko istega VPN. [24]

10.2 ARHITEKTURA MVPN

10.2.1 DOMENE MULTICAST

Domena multicast je množica VRF-instanc, ki so si sposobni med seboj pošiljati promet multicast. Te multicast VRF poimenujemo mVRF. Domene multicast mapirajo vse strankine skupine multicast, obstoječe v določenem VPN v enotno, enkratno, globalno skupino multicast v ponudnikovem omrežju (P-omrežju). To se doseže tako, da enkapsuliramo strankine izvirne pakete multicast z uporabo GRE. Izvirni naslov GRE-paketov je BGP-povezovalni naslov originiranega PE-usmerjevalnika. Vsaka domena multicast uporablja drug naslov globalne skupine multicast.

Vsak PE-usmerjevalnik, ki podpira mVPN-stranko, je del domene multicast za to stranko. Večje število strank se lahko poveže na določen PE-usmerjevalnik, kar pomeni, da je lahko ta PE-usmerjevalnik član toliko domen multicast, s kolikor VPN strankami je povezan.

Ena izmed prednosti domen multicast je ta, da na jedrnem P-usmerjevalniku ne potrebujemo podpore za mVPN. Za podporo domen multicast je dovolj izvirni (native) multicast. P-omrežje izgradi privzeto distribucijsko drevo multicast (default-MDT) med PE-usmerjevalniki za vsako domeno multicast. To naredi z uporabo unikatnega multicast-skupinskega naslova, ki ga dodeli ponudnik. Te naslove imenujemo MDT-Skupine. Vsak mVRF pripada privzetemu MDT. Zato število informacij stanja, ki jih nosi jedrni P-usmerjevalnik ni število skupin multicast vseh strank, ampak število VPN. To znatno zmanjša količino potrebnih informacij o stanju na P-usmerjevalniku.

P-usmerjevalnik pozna samo izvorni naslov PE-usmerjevalnika in naslov MDT-skupine, ki formirajo MDT. Promet iz CE-usmerjevalnika, ki poteka po MDT, se pošilja v GRE-enkapsuliranem paketu (P-paketu) z uporabo naslova MDT-skupine kot cilja. GRE P-paket uporablja samo IP-, ne pa tudi MPLS-oznak. [24]

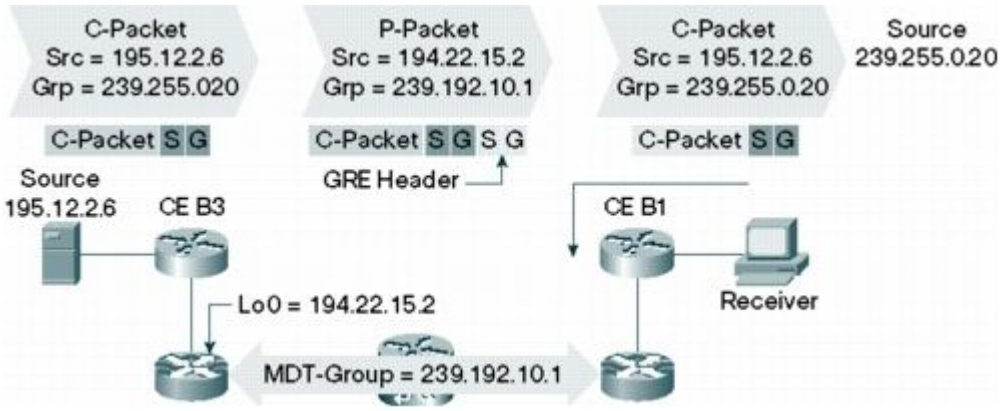
Cilji uporabe domen multicast so:

- Zagotavljanje dostave poslovnega-multicast (enterprise) prometa strankam, ki želijo uporabljati storitev mVPN;
- zmanjšanje količine informacij o stanju na P-omrežju (jedrno omrežje ponudnika) med zagotavljanjem optimalnega usmerjanja;
- omogočati strankam svobodo pri izbiri svojih skupin multicast, načinu izvedbe multicast, RP-umestitve;
- zagotoviti, da je multicast na P-omrežju popolnoma ločen od delovanja multicast na strankinem omrežju.

10.2.2 MULTICAST VRF - mVRF

Na PE-usmerjevalniku ima vsak VRF lahko nastavljeno usmerjevalno in posredovalno tabelo multicast, imenovano multicast VRF (mVRF). mVRF je vpogled PE-usmerjevalnika v uporabnikovo omrežje VPN-multicast. mVRF vsebuje vse usmerjevalne informacije multicast za ta VPN. Te informacije zajemajo vpise stanja za distribucijska drevesa ali RP-mapiranja (v primeru uporabe PIM SM). Ko PE-usmerjevalnik prejme promet multicast ali kontrolne pakete iz vmesnika v VRF na CE-usmerjevalniku, se izvede RPF-preverba in posredovanje na povezan mVRF.

Nastale mVPN-storitve omogočajo gradnjo PIM-domen, ki imajo vire in sprejemnike locirane na različnih straneh. Pomembno je omeniti, da uporaba mVPN ne spremeni načina upravljanja omrežja podjeta v smislu naslavljanja, usmerjevalne politike, ali topologije, niti ne spreminja povezljivosti z zunanjim svetom. Pomembno je še omeniti, da družbino omrežje IP-multicast nima nikakršnih povezav s ponudnikovim omrežjem multicast. Z vidika ponudnika so uporabnikovi IP-multicast-paketi zgolj podatki napram ponudnikovem popolnoma ločenem IP-multicast-omrežju. [24]



Slika 10-1: mVPN-enkapsulacija paketa [25]

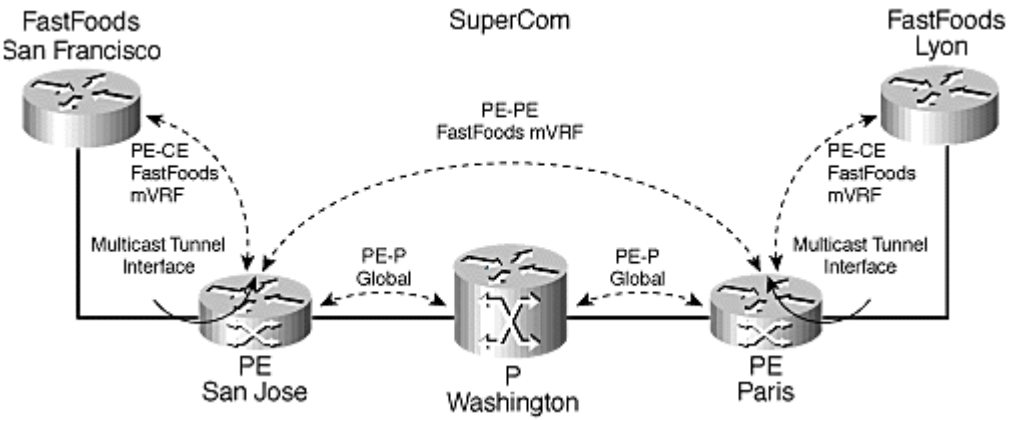
10.2.3 SOSEDSTVO mVRF PIM

Vsak VRF, ki ima omogočeno usmerjanje multicast, ima eno PIM-instanco ustvarjeno na PE-usmerjevalniku. Ta specifična instanca VRF PIM ustvari PIM-sosedstvo z vsakim PIM omogočenem CE-usmerjevalnikom v tem mVRF. Usmerjevalni multicast vnosi, ki jih vsaka PIM-instanca ustvari, so specifični glede na ustrezni mVRF.

Poleg PIM-sosedstva z CE-usmerjevalnikom, PE-usmerjevalnik ustvari dva tipa PIM-sosedstva z drugimi PE-usmerjevalniki, ki imajo mVRF v isti domeni multicast. To PE-usmerjevalnikovo PIM-sosedstvo je dosegljivo skozi *multicast tunnel interface* (MTI) in se uporablja za prenos informacij multicast med mVRF (skozi MDT) preko hrbtenice omrežja. PIM-sosedstvo PE-usmerjevalnika se ohranja z uporabo iste PIM-instance, ki se uporablja med PE- in CE-usmerjevalnikom glede na povezan mVRF.

Drugi tip PIM-sosedstva ustvari globalna PIM-instanca. PE-usmerjevalnik vzdržuje globalno PIM-sosedstvo preko svojih IGP-sosedov, ki je P-usmerjevalnik in/ali neposredno povezani PE-usmerjevalniki. Globalna PIM- instanca se uporablja za ustvarjanje multicastnih distribucijskih dreves (MDT), ki povezujejo mVRF.

CE-usmerjevalniki z uporabo globalne PIM instance ne formirajo PIM-sosedstva med seboj, niti s PE- usmerjevalnikom.



Slika 10-2: Sosedstvo mVRF PIM [24]

10.2.4 MDT

MDT so tuneli multicast, ki potekajo skozi ponudnikovo omrežje. MDT prenašajo uporabnikov promet multicast, enkapsuliran v GRE-tunele.

Obstajata dva tipa MDT [24]:

- Privzeti MDT (Default MDT) – mVRF uporablja ta MDT za pošiljanje prometa multicast nizke pasovne širine oz. prometa, ki je usmerjen proti veliki množici sprejemnikom. Privzeti MDT se vedno uporablja za pošiljanje kontrolnega prometa multicast med PE-usmerjevalniki v domeni multicast.
- Podatkovni MDT (Data MDT) – ta MDT-tip se uporablja kot tunel s širokopasovnim virom prometa skozi ponudnikovo omrežje proti zainteresiranim PE-usmerjevalnikom. Podatkovni MDT se izogiba nepotrebnemu poplavljanju uporabnikovega prometa v smeri proti vsem PE-usmerjevalnikom v domeni multicast.

10.2.4.1 PRIVZETI MDT

Ko je VRF omogočen za multicast, se mora povezati z *Default-MDT*. PE- usmerjevalnik vedno zgradi privzeti MDT za povezovanje z drugimi PE- usmejevalniki, ki imajo mVRF z isto nastavljenim naslovom MDT-skupine. Vsak mVRF je povezan z privzetim MDT. MDT se ustvari in vzdržuje v ponudnikovem omrežju s standardnimi PIM-mehanizmi. Na primer, če bomo v ponudnikovem omrežju uporabljali PIM-SM, morajo PE-usmerjevalniki v določeni

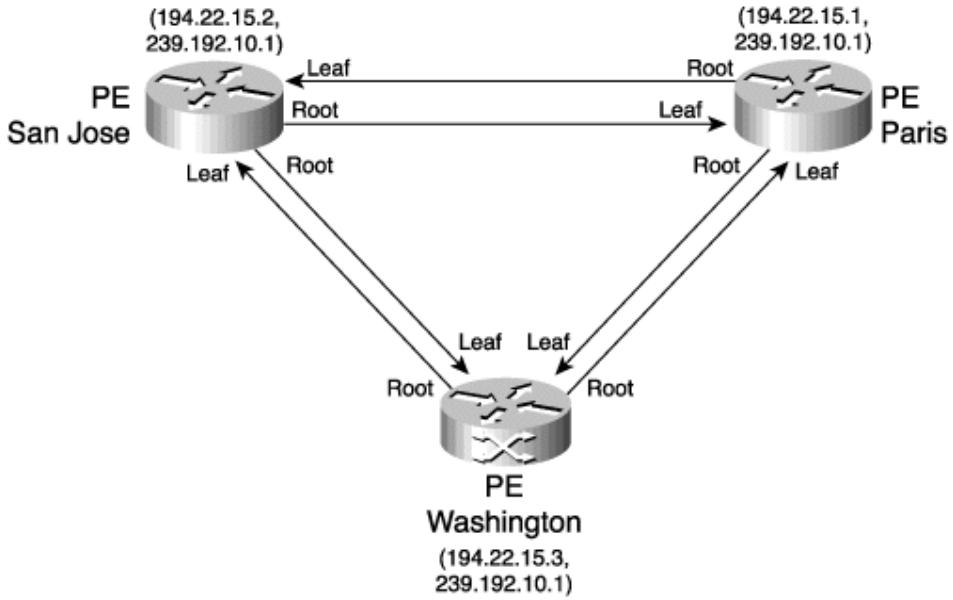
domeni multicast odkrivati drug drugega z pridruževanjem souporabniškega drevesa določene MDT-skupine, ki se usmerja na ponudnikovem RP-usmerjevalniku. [24]

Primer konfiguracije privzete MDT za VRF »blue« je pokazan spodaj:

```
ip vrf blue
 rd 100:1111
 route-target export 100:1111
 route-target import 10:1111
 mdt default 239.192.10.1
```

Primer prikazuje, da je potreben samo en dodaten ukaz v obstoječi VRF-nastavitvi. Po izvedbi ukaza *mdt default* se ustvari tunel vmesnik znotraj blue mVRF, ki omogoča dostop do skupine 239.192.10.1 znotraj ponudnikovega omrežja. Če so ostali PE-usmerjevalniki na omrežju nastavljeni v isto skupino, potem je deljeno drevo zgrajeno med temi PE-usmerjevalniki.

Ko se PE-usmerjevalnik včlani v MDT, postane koren tega drevesa, oddaljeni PE-usmerjevalniki postanejo listi tega MDT-drevesa. Nasprotno, lokalni PE-usmerjevalnik postane list MDT-drevesa, ki korenini na oddaljenih PE-usmerjevalnikih. Ker je PE-usmerjevalnik hkrati koren in list istega drevesa, je omogočeno usmerjevalniku sodelovati v domeni multicast v obliki vira sprejemnika.

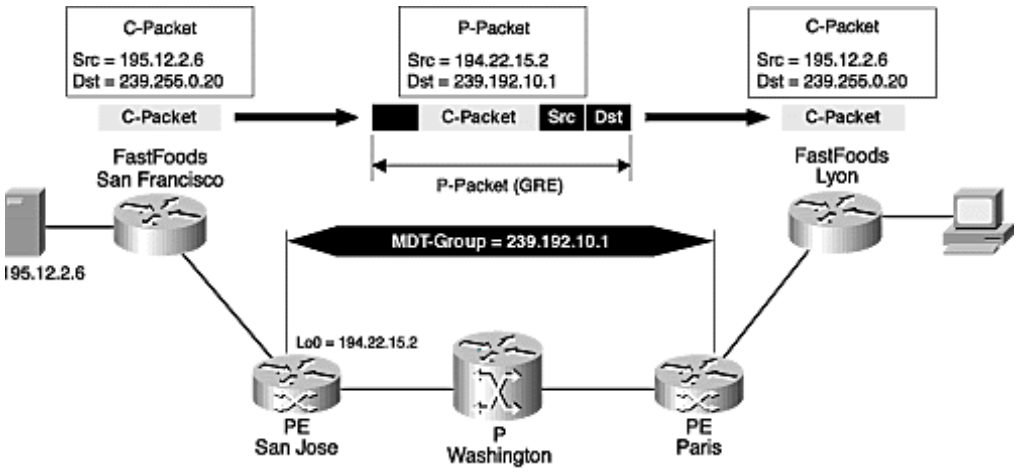


Slika 10-3: Koren MDT in listi [24]

Kot smo že omenili, ko PE-usmerjevalnik posreduje strankin paket multicast v MDT, se enapsulira v GRE. To je zato, da se lahko skupina multicast določenega VPN mapira v eno MDT-skupino v P-omrežju. Izvorni naslov zunanje IP-glave je lokalni povezovalni BGP naslov PE usmerjevalnika, ciljni naslov pa je naslov MDT-skupine dodeljen domeni multicast.

Zato zadevajo P-omrežje le IP-naslovi v GRE-glavi (dodeljeni s strani ponudnika), ne pa tudi strankino naslavljanje.

Paket se nato posreduje v P-omrežje z uporabo naslova multicast MDT-skupine, ravno tako kot vsak drug multicastni paket z normalno RPF-preverbo na izvornem naslovu (ki je v tem primeru originirani PE). Ko paket prispe na ciljni PE- usmerjevalnik iz MDT, se enkapsulacija odstrani in originalni strankin paket multicast se posreduje dodeljenemu mVRF-u. Ciljni mVRF se pridobi iz naslova MDT-skupine v ciljnem delu enkapsuliranega paketa. Zato se z uporabo tega procesa strankini paketi multicast tunelirajo skozi P-omrežje do primernih MDT-listov.



Slika 10-4: MDT-enkapsulacija paketov [24]

10.2.4.2 PODATKOVNI MDT (DATA MDT)

Ves promet ponujen Privzetem-MDT (skozi tuneliran vmesnik multicast) se distribuira na vse PE-usmerjevalnike, ki so del te domene multicast, ne glede, ali so aktivni sprejemniki v mVRF na PE-usmerjevalniku. Za širokopasovne aplikacije, ki imajo redko porazdeljene sprejemnike, lahko to predstavlja nepotrebno poplavljanje mirujočih PE-usmerjevalnikov. Da to prebrodimo, ustvarimo posebno MDT-skupino – Podatkovno-MDT, s katero zmanjšamo poplavljanje, tako da pošiljamo podatke samo PE-usmerjevalnikom z aktivnimi VPN-sprejemniki. Podatkovna MDT se ustvari dinamično, če določen tok multicast prekorači pasovni prag. Vsak VRF ima lahko bazen (pool) Podatkovnih-MDT naslovov skupin.

Podatkovni-MDT je ustvarjen samo za podatkovni promet. Ves kontrolni promet multicast potuje preko Privzete-MDT za zagotavljanje, da vsi PE- usmerjevalniki dobijo kontrolne informacije. [24]

Primer konfiguracije Podatkovnega-MDT za VRF »blue«:

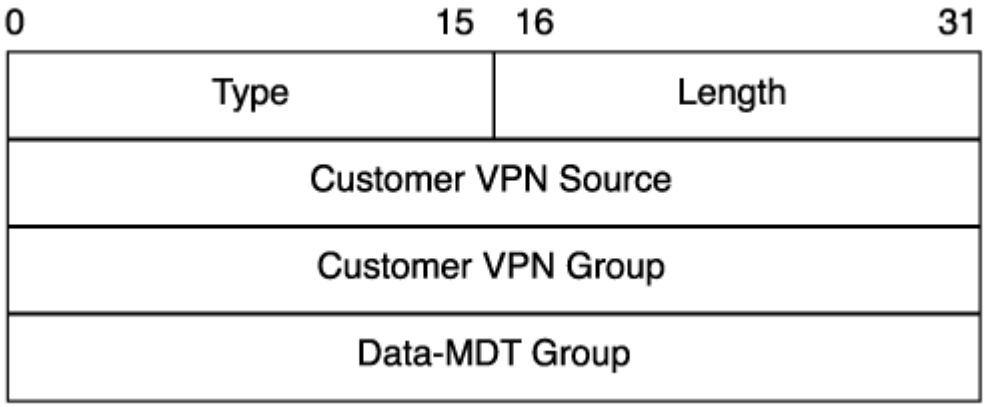
```
ip vrf blue
 rd 100:1111
 route-target export 100:1111
 route-target import 10:1111
 mdt default 239.192.10.1
mdt data 239.192.20.32 0.0.0.15 treshold 1
```

Mdt data označuje rang naslovov, ki se uporabijo v Podatkovnem-MDT bazenu. Z masko 0.0.0.15 dovoljuje uporabo naslovov od 239.192.20.32 do 239.192.20.47.

Ko PE-usmerjevalnik ustvari Podatkovni-MDT, se izvirni promet multicast enkapsulira na isti način kot pri Privzetem-MDT, z razliko ciljne skupine, ki je vzeta s Podatkovnega-MDT bazena. Vsak PE-usmerjevalnik, ki ima zainteresirane sprejemnike, mora izdati *P-join* za Podatkovni-MDT, sicer sprejemniki ne morejo videti C-paketov.

Za to mora izvorni PE-usmerjevalnik obvestiti vse PE-usmerjevalnike v domeni multicast o obstoju novo ustanovljenega Podatkovnega-MDT. To se doseže s pošiljanjem posebnih PIM-oblik kontrolnih sporočil na Privzeti-MDT, vsebujoč strankin (S,G) za Podatkovno-MDT skupino. To sporočilo se imenuje *Data-MDT join*.

Podatkovni-MDT *join* je povabilo povezanim PE-usmerjevalnikom, da se pridružijo novim Podatkovnim-MDT, če vsebujejo zainteresirane sprejemnike v ustreznem mVRF. Sporočilo se prenaša v paketu UDP, naslovljenem na *ALL-PIM-ROUTERS* skupini (224.0.0.13). Podatkovno-MDT mapiranje se oglašuje z formatom dolžine, tipa, vrednosti. [24]



Slika 10-5: Podatkovni format MDT join TVL [24]

10.2.5 MTI (Multicast Tunnel Interface)

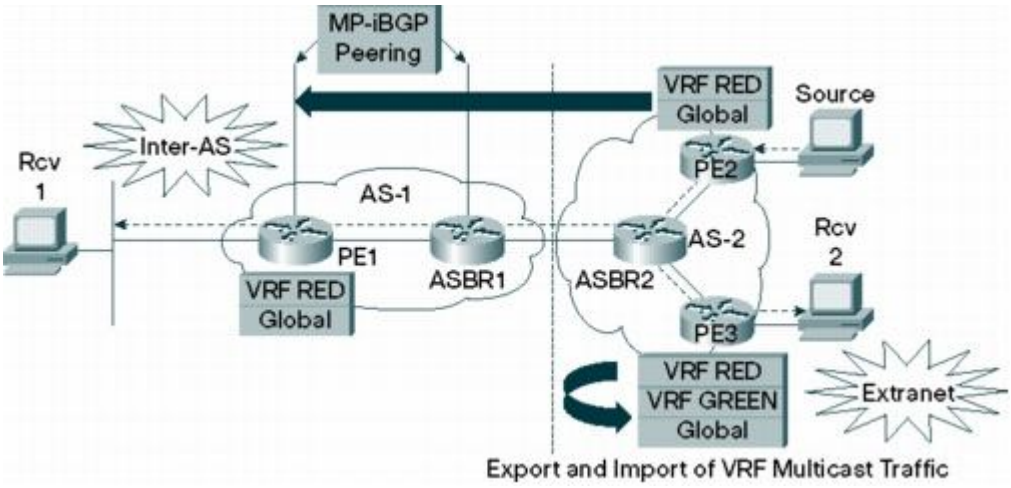
MTI predstavljajo dostop do domen multicast v Cisco IOS. Mti se pojavlja v mVRF kot vmesnik z imenom Tunnelx, kadar je x številka tunela. Za vsako domeno multicast, v kateri participira mVRF, obstaja ustrezen MTI. MTI je v bistvu prehod, ki povezuje strankino okolje s ponudnikovim okoljem (MDT). Vsak C-paket (strankin paket) poslan proti MTI se enkapsulira v P-paket (ponudnikov paket) in pošlje po MDT. Ko robni PE-usmerjevalnik pošilja promet proti MTI, prevzame vlogo korena MDT. Obratno, kadar PE-usmerjevalnik prejema promet iz smeri MTI, prevzame vlogo lista tega drevesa. PIM-sosedstva se ustvarijo z vsemi PE-usmerjevalniki v domeni multicast preko MTI. Zato so za določene mVRF, PE-usmerjevalnikovi PIM-sosedi vidni preko istega MTI. MTI je obravnavan s strani mVRF PIM-instance, kot da je LAN vmesnik. Vsi PIM LAN-postopki veljajo tudi v MTI. PE-usmerjevalnik pošilja PIM-kontrolna sporočila preko MTI, tako da se lahko multicastna posredovalna drevesa vzpostavijo med strankinimi lokacijami, ki so ločena preko ponudnikovega omrežja. Posredovalna drevesa so vidna samo v strankinem omrežju, ne pa tudi v ponudnikovem omrežju. Da se omogoči posredovanje multicast med strankinimi lokacijami, je MTI del seznama izhodnih vmesnikov (olist) za (S,G) ali (*,G) stanj, ki originirajo iz mVRF.

MTI je ustvarjen dinamično, po konfiguraciji Privzetega-MDT, in ga ni mogoče izrecno nastavljati. Način PIM Sparse-Dense (PIM SD) je omogočen samodejno, tako da lahko podira različne načine skupin. Na primer, če stranka uporablja samo PIM DM, potem bi bil PIM dodan v olist z vnosom *Forward/Dense*, da omogoči distribucijo prometa preko strankinih lokacij. Če sosedje PE-usmerjevalnika pošljejo nazaj sporočilo obrezovanja in ne prejmemo razveljavitve obrezovanja, potem bi bil MTI v vnosu *olist* nastavljen na *Prune/Dense*, kot da bi bil LAN-vmesnik.

MTI ni dostopen ali viden preko IGP (kot sta OSPF ali RIP), ki deluje v strankinem omrežju. Z drugimi besedami, nobeno usmerjanje unicast ni posredovano preko MTI, ker se vmesnik ne pojavlja v usmerjevalni tabeli unicast izbranega VRF-a. Ker se RPF-preverba izvaja na usmerjevalni tabeli unicast za PIM, ima promet prejet preko MTI neposredne posledice na trenutnih RPF-procedurah.[24]

10.3 MEDAVTONOMNI SISTEMI MVPN

Podpora več avtonomnim sistemom v Multicast VPN se lahko nastavi v VRF na usmerjevalniku, da omogočimo posredovanje mVPN-prometa iz ene lokacije VPN RED v avtonomnem sistemu 1 (AS1) na drugo lokacijo VPN RED v AS2. Ta lastnost dopušča, da se vzpostavijo MDT-tuneli med dvema PE- usmerjevalnikoma v različnih avtonomnih sistemih brez potrebe po izmenjavi usmerjevalnih informacij med dvema avtonomnima sistemoma.



Slika 10-6: Uvoz in izvoz prometa VRF multicast [25]

Da dopustimo dvema PE-usmerjevalnikoma vzpostavitev MDT-tunela preko avtonomnih sistemov, mora biti MDT-naslovna družina omogočena znotraj BGP-konfiguracije. Z uporabo MDT-avtonomnega sistema so PE-usmerjevalniki v različnih avtonomnih sistemih sposobni učenja o medsebojnem obstoju in znajo vzpostavljati povezavo med seboj. Da nastavimo MED-AS-podporo za mVPN, sta potrebna dva koncepta, o čemer pa več v nadaljevanju. [25]

10.3.1 METODA POVRATNE POTI NA RAZLOČEVALNIKU USMERJEVALNIH SMERI

Ko zagotavljamo VPN v različnih avtonomnih sistemih, usmerjevalne informacije na ponudnikovih usmerjevalnikih včasih niso dovolj za vzpostavitev MDT-tunela, ki se razteza med več avtonomnimi sistemi iz enega do drugega PE-usmerjevalnika. Ko dodamo dodatne informacije v paket *PIM join*, vmesni usmerjevalniki lahko izberejo RPF-vmesnik z neposrednim vpogledom v posebno tabelo BGP MDT. Le-ta se uporablja samo za vzpostavitev MDT- tunela, ne pa tudi za VPN-promet znotraj MDT-tunela. Za vmesne usmerjevalnike, ki ne vzpostavljajo BGP za določitev RPF-vmesnika uporablja RPF-vektor.[25]

10.3.2 SPREMENJEN FORMAT PIM JOIN

Ta metoda je potrebna, ker so poti do vira znotraj VRF poznane preko Multiprotokol BGP naslednjega skoka. Te poti niso prisotne v protokolu notranjih usmerjevalnikov (IGP) v ponudnikovem jedru. Ciljni naslov v naslednjem skoku se vnese v PIM sporočilo in je poznan kot RPF-vektor.

Nova možnost *PIM hello* je bila uvedena, da določi, kdaj je vrhnji usmerjevalnik sposoben razčlenjevati novo kodiranje. Ostali usmerjevalniki na LAN lahko prekoračijo sporočila *prune* ali prekličejo pošiljanje sporočila *join*, s tem da ustvarijo potrebo po razčlenitvi sporočila *PIM join*. Te metode so edini način, da se omogoči popolno med-AS-podporo, opisano v RFC 2547bis.[25]

10.3.3 EKSTRANET mVPN

Ekstranet lahko opišemo kot del družbinega intraneta, ki ima dostop do uporabnikov zunaj družbe. Ekstranet je VPN, ki povezuje družbine lokacije z zunanjimi poslovnimi partnerji ali dobavitelji in omogoča varno izmenjavo poslovnih informacij.

MPLS VPNs omogoča varnost z zagotavljanjem uporabniškega dostopa do dovoljenih informacij. Storitev MPLS VPN ekstranet ponuja uporabnikom ekstraneta tip unicastne povezljivosti brez zajema celovitosti poslovnih podatkov.

Funkcija Multicast VPN Ekstranet omogoča ponudnikom storitev, da spremenijo vir vsebine multicast iz VPN-RED v VPN-GREEN, kot je prikazano na zgornji sliki. To omogoča ponudnikom, da nudijo naslednje generacije prilagodljivih ekstranet storitev, ki pomagajo, da se omogoči poslovno sodelovanje med različnimi podjetji. [25]

Ekstranet mVPN se lahko uporablja za rešitve različnih problemov pri poslovanju, kot so:

• učinkovita distribucija vsebin med podjetji;

• učinkovita distribucija vsebin od ponudnika storitev ali ponudnika vsebin do različnih VPN-strank.

10.3.4 MVPN MIB/UPRAVLJANJE

Ponudnik storitev, ki omogoča storitve multicast VPN, mora upravljati z multicast VRF (mVRF) na svojih robnih usmerjevalnikih. Upravljanje zagotavlja sistem za upravljanje omrežja (NMS), ki se nahaja v VRF 0. Na splošno, NMS v enem mVRF mora omogočati upravljanje drugega mVRF. Takšen primer je že poznan za upravljanje unicast MPLS VPN z implementacijo koncepta »meta NMS« SNMP agenta. Programska oprema Cisco IOS že podpira to lastnost. Za ponudnike storitev je lahko meta NMS podobno nastavljena v globalnem VRF-u, SNMPv3 pa se priporoča za varnostne in avtentikacijske mehanizme.

Za podporo upravljanja MVPN-tehnologije potrebujemo nov MIB. Ta MIB je dostopen iz VRF 0, ali iz meta VRF, ali iz meta VRF, upravljan s strani ponudnika. Podmnožico ustreznih informacij se lahko omogoči dostopno za uporabnika v njegovem VRF. Cisco je ustvaril poseben MIB za upravljanje multicast VPN. CISCO-MVPN-MIB je zasnovan na modelu MPLS-VPN-MIB in vsebuje [25]:

- število mVRF-instanc,
- število vmesnikov na mVRF,
- informacijo o privzetih MDT-skupinah,
- informacijo o podatkovnih MDT-skupinah,
- preslikavo mVRF v MVPN-tunel-vmesnik.

11 PRAKTIČNI PREIZKUS – IMPLEMENTACIJA MULTICAST VPN

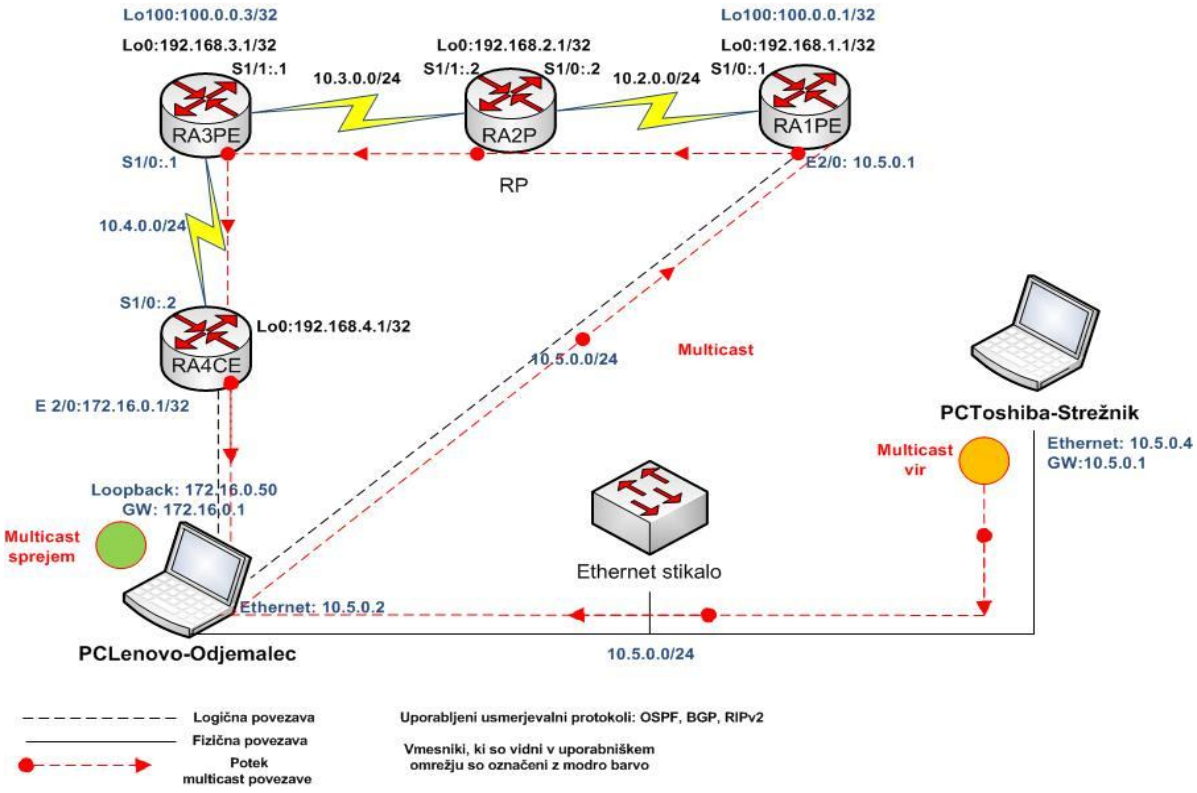
V praktičnem delu sem implementiral multicast VPN na testnem hrbteničnem omrežju hipotetičnega internetnega ponudnika. Omrežje je sestavljeno iz štirih usmerjevalnikov **Cisco** - dveh robnih in enega jedrnega usmerjevalnika pri ponudniku, enega robnega usmerjevalnika pri ponudnikovem klientu ter dveh osebnih PC-računalnikov, ki sta del klientovega omrežja. Prvi PC je služil kot strežnik, ki je povezan neposredno na ponudnikov robni usmerjevalnik, drugi PC-odjemalec pa je povezan na robni klientov usmerjevalnik. Odjemalec je tudi služil poganjanju testnih usmerjevalnikov. PC-ja sta fizično povezana preko omrežnega stikala.

Namen praktičnega preizkusa je dokazati, da je izvedba multicast VPN potrebna, če želimo stranki omogočiti pošiljanje podatkovnega toka multicast med njihovimi lokacijami v VPN.

Praktični poizkus je potekal v naslednjih korakih:

- postavitev omrežja in implementacija protokolov ter multicast VPN;
- nastavitev povezljivosti med usmerjevalniki ter strežnikom in odjemalcem;
- nastavitev strežnika in odjemalca;
- preizkus delovanja;
- primerjava konfiguracije in delovanja podatkovnega toka multicast z in brez implementacije multicast VPN.

11.1 TESTNO OMREŽNO OKOLJE



Slika 11-1: Prikaz testnega okolja

Testno okolje je sestavljeno iz že prej dveh omenjenih osebnih računalnikov – prenosnikov (v nadaljevanju PCToshiba-strežnik ter PCLenovo-odjemalec). Ker za testiranje nisem uporabljal pravih usmerjevalnikov Cisco, je na prenosniku PCLenovo za emulacijo poskrbel emulator **Dynamips**, zasnova omrežja in povezljivost s PC-jema pa je bila izvedena v grafičnem okolju **GNS3**.

11.2 TESTNA OPREMA

Osebni računalnik	Performanse	OS	Vmesnik
Toshiba satelite pro	2,2 GHz, 2GB RAM	Windows Vista Business Edition	Realtek RTL8101
Lenovo T 61	2,5 GHz, 4GB RAM	Windows Vista Enterprise	Intel 82566MM Microsoft Loobpack vmesnik

Mrežna oprema
Level one, FSW-0508TX 10/100 Ethernet stikalo

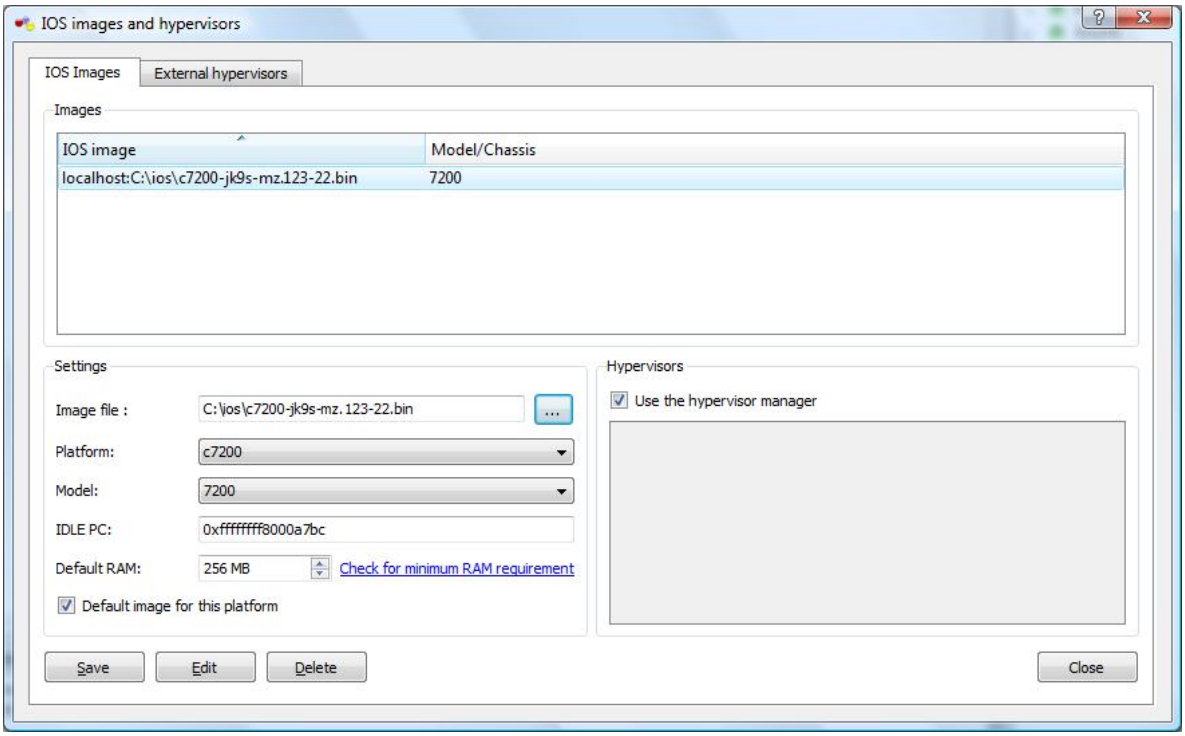
Programska oprema
GNS3 0.6.1
Dynamips-0.2.8
VLC Media Player 1.0.1

11.2.1 EMULATOR DYNAMIPS

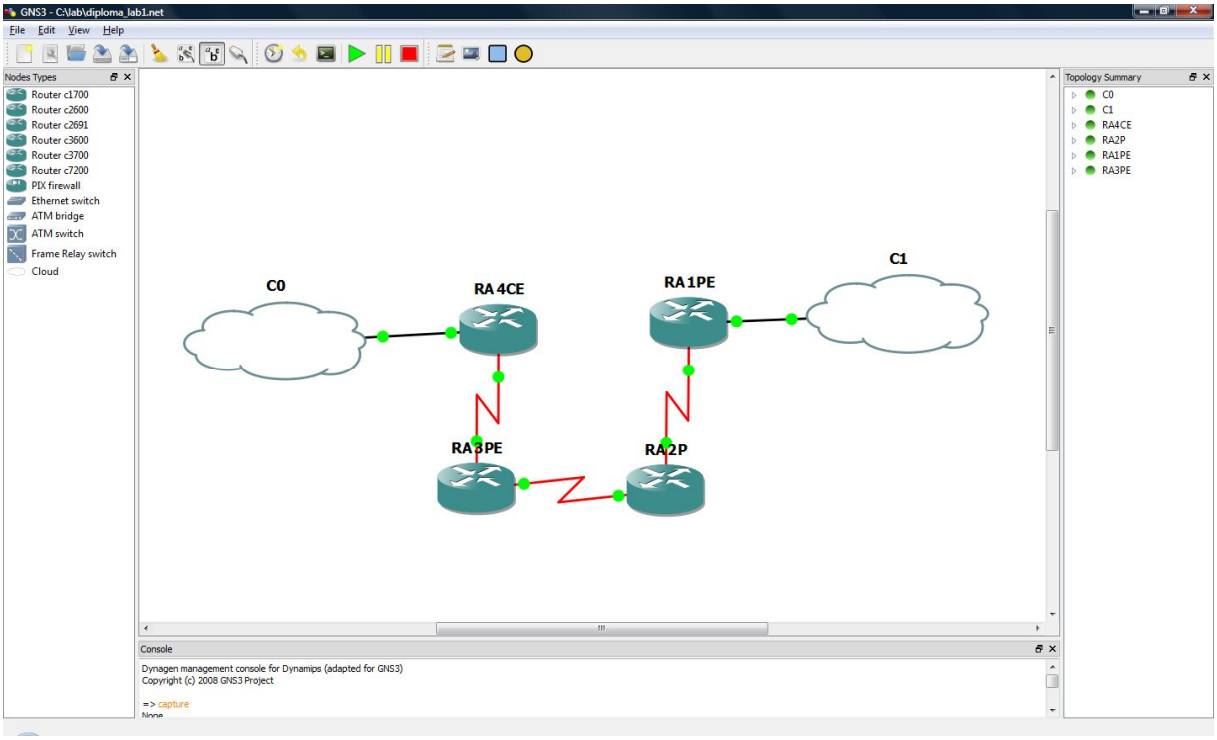
Kot sem omenil, je za emulacijo usmerjevalnikov skrbel emulator Dynamips. Dynamips je emulator, namenjen poganjanjem usmerjevalnikov Cisco, njegova prednost pa je ta, da poganja prave datoteke IOS. IOS je operacijski sistem, ki se izvaja na stikalih Cisco in usmerjevalnikih in skrbi za njihovo upravljanje. Vsi testni usmerjevalniki so serije 7200, za lažje in bolj pregledno delovanje sem uporabil eno datoteko IOS, in sicer **c7200-jk9s-mz.123-22.bin**, ki predstavlja 12.3(22) verzijo Cisco IOS operacijskega sistema (BOOTLDR: 7200 Software (C7200-JK9S-M), Version 12.3(22)). Emulator Dynamips je lahko nameščen kot samostojni program, v mojem primeru pa je bil vključen v grafično okolje programskega paketa GNS3.

11.2.2 OKOLJE GNS3

GNS3 je grafični simulator omrežja, ki omogoča izgradnjo komplesnih omrežij. Da omogoča popolne emulacije, je močno povezan z Dynamips emulatorjem. Dynamips se namesti že ob instalaciji GNS3, kjer nastavimo tudi povezavo do datoteke IOS.



Slika 11-2: Nastavitev poti do datoteke IOS v okolju GNS3



Slika 11-3: Prikaz topologije testnega omrežja v okolju GNS3

11.3 NASTAVITVE PARAMETROV OMREŽJA

Ko v grafičnem okolju postavimo omrežje, se vsi parametri (povezava do IOS datoteke, fizična povezava med usmerjevalniki in PC-jema …) shranijo v datoteko s končnico .NET.

11.3.1 GLOBALNI PARAMETRI

Globalni parametri predstavljajo nastavitve delovnega okolja, povezave do datoteke IOS ter nastavitev vrat in parametra idlepc. Slednji je parameter, ki omogoča boljši izkoristek CPU-ja, ker emulacija večjega števila usmerjevalnikov precej upočasni delovanje PC-ja.

autostart = False
[localhost:7200]
workingdir = c:\lab\diploma_peppe_working
udp = 10000
[[7200]]
image = C:\ios\c7200-jk9s-mz.123-22.b in
idlepc = 0x60c371c0

11.3.2 NASTAVITVE PONUDNIKOVIH USMERJEVALNIKOV

11.3.2.1 PARAMETRI ROBNEGA USMERJEVALNIKA RA1PE

[[ROUTER RA1PE]]

console = 2015
cnfg = C:\lab\diploma_lab_configs\RA1PE.cfg
slot1 = PA-8T
s1/0 = RA2P s1/0
slot2 = PA-8E
e2/0 = nio_gen_eth:\device\npf_{4ad39ef1-d07e-4054-a3a6-6277d5970cb4}

11.3.2.2 PARAMETRI JEDRNEGA USMERJEVALNIKA RA2P

[[ROUTER RA2P]]

console = 2014
cnfg = C:\lab\diploma_lab_configs\RA2P.cfg
slot1 = PA-8T
s1/0 = RA1PE s1/0
s1/1 = RA3PE s1/1

11.3.2.3 PARAMETRI ROBNEGA USMERJEVALNIKA RA3PE

[[ROUTER RA3PE]]

console = 2016
cnfg = C:\lab\diploma_lab_configs\RA3PE.cfg
slot1 = PA-8T
s1/0 = RA4CE s1/0
s1/1 = RA2P s1/1

11.3.3 NASTAVITVE ODJEMALČEVEGA USMERJEVALNIKA

11.3.3.1 PARAMETRI USMERJEVALNIKA RA4CE

[[ROUTER RA4CE]]

console = 2005
cnfg = C:\lab\diploma_lab_configs\RA4CE.cfg
slot1 = PA-8T
s1/0 = RA3PE s1/0
slot2 = PA-8E
e2/0 = nio_gen_eth:\device\npf_{f6054464-d234-4287-a72d-aca5c9dddf83}

Parametri **cnfg** predstavljajo povezavo do imenika, v katerega shranimo konfiguracijo usmerjevalnikov. Parameter **slot1=PA8T**, ki je enak na vseh usmerjevalnikih, predstavlja navidezno režo z fizičnimi vmesniki. PA8T je kratica za osem serijskih vmesnikov. Parameter **s1/x** predstavlja fizično povezavo med usmerjevalniki s serijskimi vmesniki. Usmerjevalnika RA1PE in RA4CE vsebujeta še parametra **slot2=PA-8E** in **e2/0.** V drugi navidezni reži je osem ethernet vmesnikov-PA8E.

Parameter e2/0 = nio_gen_eth:\device\npf_{f6054464-d234-4287-a72d-aca5c9dddf83} na usmerjevalniku RA1PE predstavlja fizično povezavo do odjemalčevega ethernet vmesnika PCLenovo.

Parameter e2/0 = nio_gen_eth:\device\npf_{f6054464-d234-4287-a72d-aca5c9dddf83} na usmerjevalniku RA4CE pa predstavlja fizično povezavo do odjemalčevega loopback vmesnika PCLenovo.

Da povezljivost med PCLenovo in virtualnim GNS3/Dynamips okoljem deluje, sta potrebna še dva navidezna oblaka z naslednjimi parametri:

[GNS3-DATA]

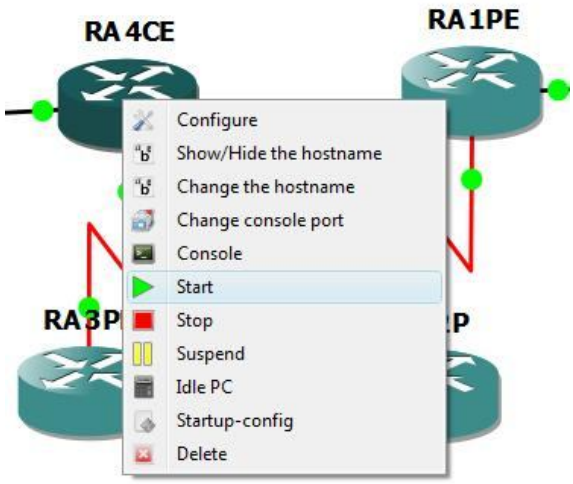
configs = diploma_lab_configs
workdir = diploma_lab_working

[[Cloud C0]]
connections = RA4CE:e2/0:nio_gen_eth:\device\npf_{f6054464-d234-4287-a72d-aca5c9dddf83}
[[Cloud C1]]
connections = RA1PE:e2/0:nio_gen_eth:\device\npf_{4ad39ef1-d07e-4054-a3a6-6277d5970cb4}

11.4 DOSTOP DO USMERJEVALNIKOV

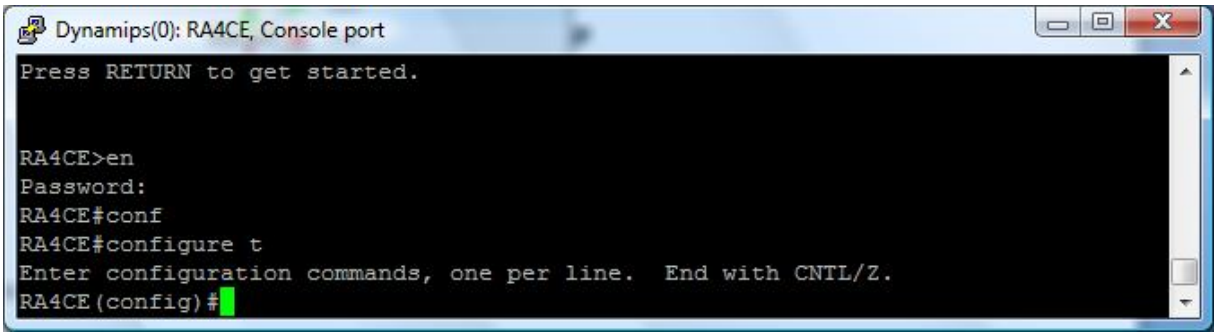
Za dostop do usmerjevalnikov sem uporabil terminalni program putty, parametre pa sem nastavil v GNS3 okolju z ukazom: *C:\putty.exe -telnet %h %p*

Usmerjevalnike v GNS3 zaženemo z ukazom start, dostopamo pa z ukazom terminal, kot je prikazano na spodni sliki:



Slika 11-4: Zagon usmerjevalnika v grafičnem okolju GNS3

Ko zaženemo »Console«, se nam odpre novo terminalsko okno z emulacijo usmerjevalnika c7200, kot je prikazano na spodnji sliki:



Slika 11-5 Dostop do naprednega načina in konfiguracije usmerjevalnika

Z ukazom »***enable***« dostopamo do naprednega načina delovanja, ukaz »configure terminal« pa nam omogoča dostop do konfiguracije usmerjevalnika.

11.5 KONFIGURACIJA USMERJEVALNIKOV

Na vseh usmerjevalnikih prvo nastavimo ime, geslo za dostop do naprednega načina delovanja ter geslo za oddaljeni dostop:

enable
configure terminal
hostname RAXXX
enable password cisco

11.5.1 KONFIGURACIJA ROBNIH USMERJEVALNIKOV

Predstavil bom konfiguracijo robnega usmerjevalnika RA1PE.

11.5.1.1 KONFIGURACIJA USMERJEVALNIKA RA1PE

Po osnovnih nastavitvah prvo omogočimo usmerjanje multicast, multicastno distribucijsko drevo – MDT, mpls ter routing instanco – VRF, nato nastavimo vmesnike.

ip vrf blue
rd 100:1111
route-target export 100:1111
route-target import 100:1111
mdt default 239.1.1.1
mdt data 239.2.2.0 0.0.0.255 threshold 1
!
ip multicast-routing
ip multicast-routing vrf blue
ip cef
mpls label protocol ldp
tag-switching tdp router-id Loopback0

Nastavitev vmesnikov:

interface Loopback0
ip address 192.168.1.1 255.255.255.255
ip pim sparse-dense-mode
!

```
interface Loopback100
 ip vrf forwarding blue
 ip address 100.0.0.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface Serial1/0
 description LINK-DO-RA2P
 ip address 10.2.0.1 255.255.255.0
 ip pim sparse-dense-mode
 tag-switching ip
 serial restart-delay 0
 clock rate 64000

!
interface Ethernet2/0
 description POVEZAVA DO VIRA
 ip vrf forwarding blue
 ip address 10.5.0.1 255.255.255.0
 ip pim sparse-dense-mode
 duplex half
```

Nastavitev usmerjanja:

```
!
router ospf 1
 router-id 192.168.1.1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.1.1 0.0.0.0 area 0
!
router rip
 version 2
 no auto-summary
 !
 address-family ipv4 vrf blue
 redistribute bgp 1
 network 10.0.0.0
 network 100.0.0.0
 default-metric 5
 no auto-summary
 version 2
 exit-address-family
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 192.168.3.1 remote-as 1
```

```
 neighbor 192.168.3.1 update-source Loopback0
neighbor 192.168.2.1 remote-as 1
 neighbor 192.168.2.1 update-source Loopback0
 !
 address-family ipv4
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 192.168.3.1 activate
 neighbor 192.168.3.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf blue
 redistribute connected
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
no ip http server
no ip http secure-server
!
ip pim bidir-enable
ip pim vrf blue send-rp-announce Loopback100 scope 100
ip pim vrf blue send-rp-discovery Loopback100 scope 100
```

11.5.2 KONFIGURACIJA JEDRNEGA USMERJEVALNIKA

Tudi na jedrnem usmerjevalniku omogočimo usmerjanje multicast ter mpls.

```
ip multicast-routing
ip cef
mpls label protocol ldp
tag-switching tdp router-id Loopback0
```

Nastavitev vmesnikov:

```
interface Loopback0

 ip address 192.168.2.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 description LINK-DO-RA1PE
 ip address 10.2.0.2 255.255.255.0
 ip pim sparse-dense-mode
 tag-switching ip
 serial restart-delay 0
!
interface Serial1/1
 description LINK-DO-RA3PE
 ip address 10.3.0.2 255.255.255.0
 ip pim sparse-dense-mode
 tag-switching ip
 serial restart-delay 0
```

Nastavitev usmerjanja:

```
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.2.1 0.0.0.0 area 0
!
ip classless
no ip http server
no ip http secure-server
!
ip pim bidir-enable
ip pim send-rp-announce Loopback0 scope 100
ip pim send-rp-discovery Loopback0 scope 100
```

11.5.3 KONFIGURACIJA KLIENTOVEGA USMERJEVALNIKA RA4CE

Tudi na uporabniškem računalniku omogočimo usmerjanje multicast

```
ip multicast-routing
ip cef
```

Nastavitev vmesnikov:

```
interface Loopback0
 ip address 192.168.4.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half


!
interface Serial1/0
 description LINK-DO-RA3PE
 ip address 10.4.0.2 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp join-group 224.2.2.2
 serial restart-delay 0
!
interface Ethernet2/0
 ip address 172.16.0.1 255.255.255.0
 ip pim sparse-dense-mode
 duplex half
!
```

Nastavitev usmerjanja:

```
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.0.0
 no auto-summary
!
```

11.6 KOMENTAR KONFIGURACIJE

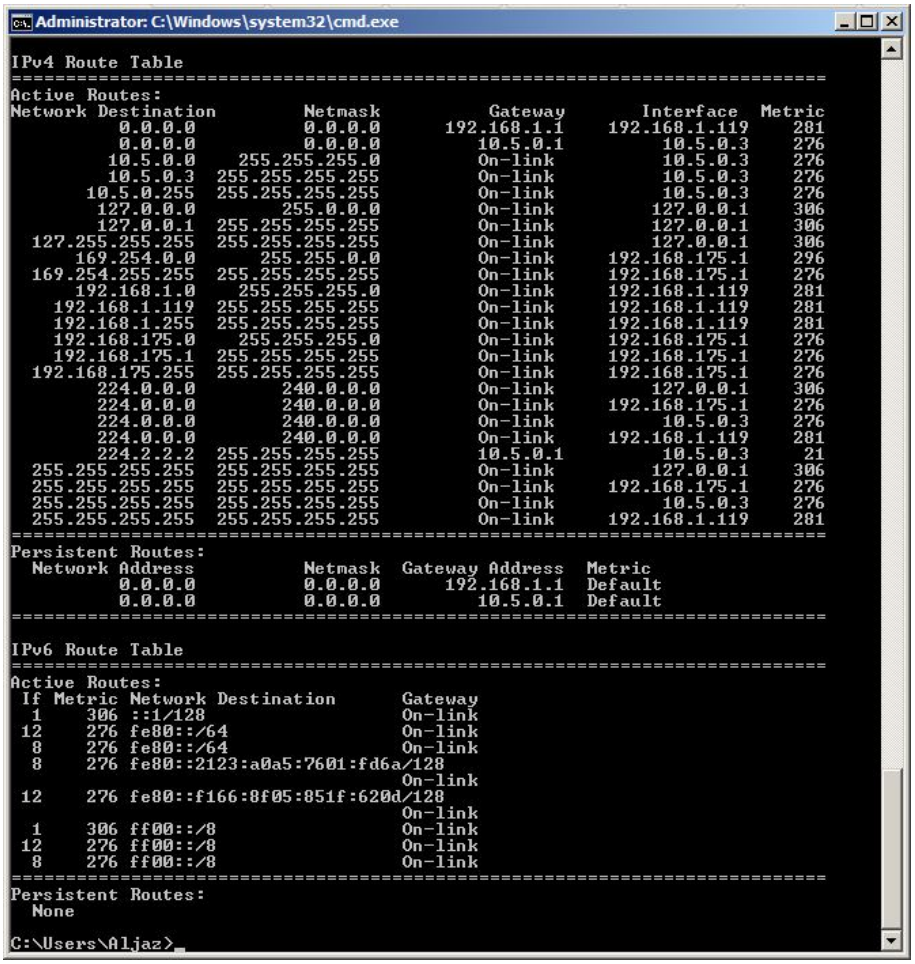
Konfiguracijo sem dobil na uradni spletni strani Cisco in je bila spremenjena za potrebe testnega omrežja. Z rdečo barvo je označen del konfiguracije, ki je potreben za implementacijo multicast VPN. Večji del konfiguracije (del, ki ni v rdeči barvi) je dovolj za pošiljanje toka multicast. Za izvedbo mVPN ter pošiljanje podatkovnega toka multicast med dvema VPN-lokacijama, je potrebna konfiguracija samo na robnih PE-usmerjevalnikih. Na jedrnem P-usmerjevalniku se ne izvaja mVPN. Tudi na uporabniškem CE-usmerjevalniku ni potrebna dodatna konfiguracija.

Po izvedbi in testiranju mVPN sem implementiral še multicast brez mVPN- konfiguracije. Na naslednjih straneh bom prikazal nastavitve strežnika in odjemalca. Primerjal in prikazal bom še delovanje obeh načinov (z implementacijo mVPN in brez nje), v zaključku pa bom obrazložil, zakaj je implementacija mVPN potrebna, če želimo zagotoviti multicast med dvema ali več lokacijami znotraj VPN.

Na vseh vmesnikih multicast je omogočen način »pim sparse-dense-mode«. Za usmerjanje protokola IPv4 skrbi usmerjevalni protokol OSPF, za usmerjanje prokotola VPNv4 pa usmerjevalna protokola BGP in RIPv2.

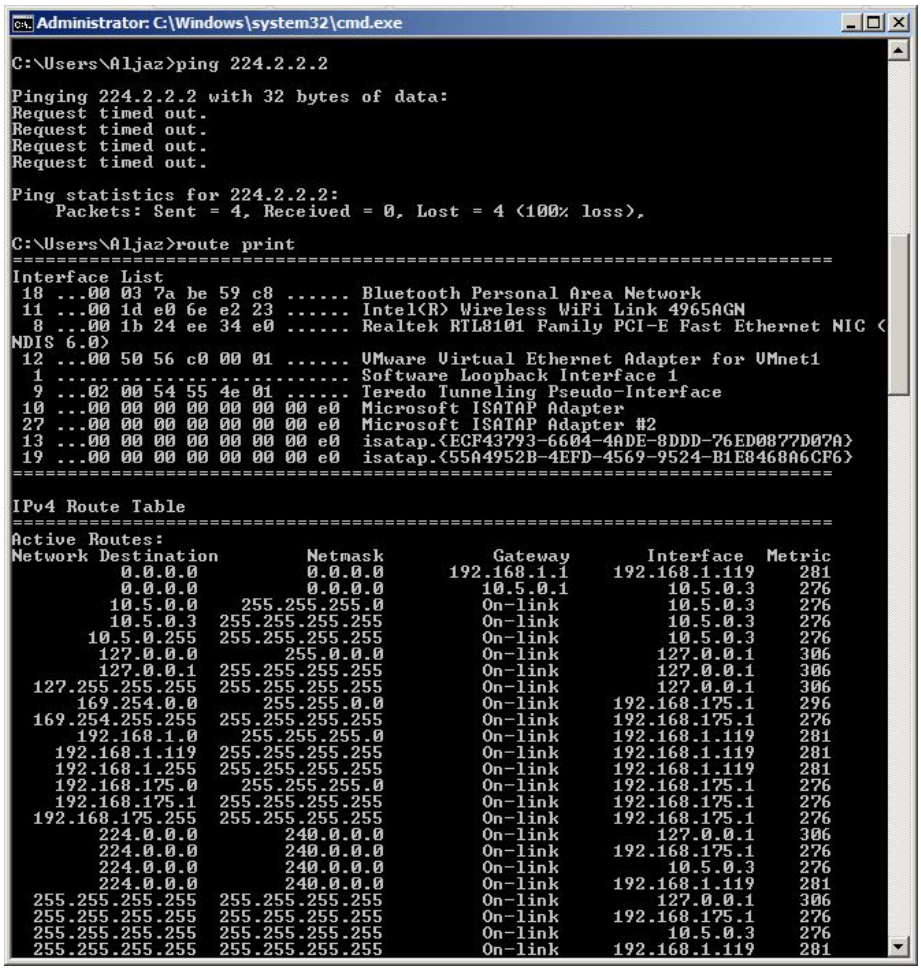
11.7 NASTAVITEV STREŽNIKA TER POŠILJANJA STREAMA

Strežnik je računalnik PCToshiba, ki je vezan na stikalo ethernet. IP-naslov računalnika je 10.5.0.4, privzeti prehod pa je 10.5.0.1, to je IP-naslov vmesnika ethernet robnega usmerjevalnika RA1PE.



Slika 11-6: Izpis poti na strežniku PCToshiba

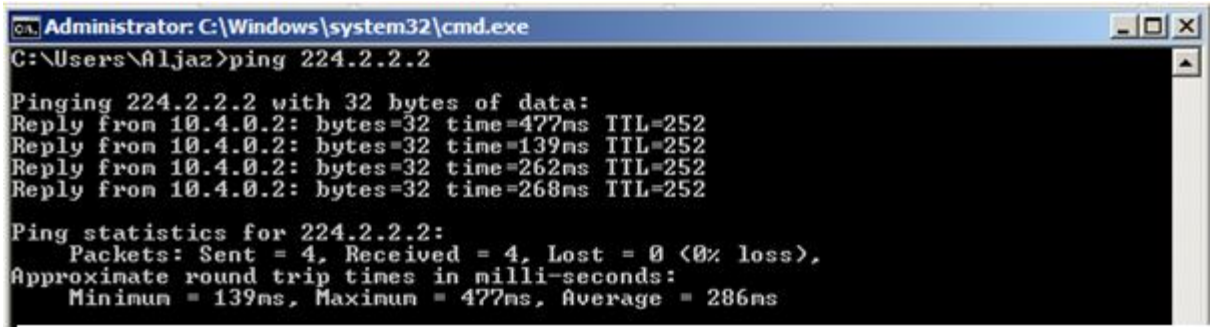
Izpis poti usmerjevalne tabele na strežniku. Na tej strani ni bilo potrebno veliko sprememb, razen vnos ene statične poti do 224.2.2.2 (multicast skupine).



Slika 11-7: Preverjanje dosegljivosti skupine multicast

Poskusimo preverjati dosegljivost cilja preko protokola ICMP (*ping 224.2.2.2*). Cilj 224.2.2.2 ni dosegljiv, kar je razvidno iz slike. Pod tem je še rezultat izpisa usmerjevalne tabele pred vnosom statične poti. Potrebno je vpisati statično host routo, ki kaže na vmesnik 10.5.0.1.

Ukaz za vnos poti je sledeč: ***route add 224.2.2.2 mask 255.255.255.255 10.5.0.1*** (gateway – eth 2/0 na dynamips oz. RA1PE).



Slika 11-8: Cilj 224.2.2.2 je dosegljiv

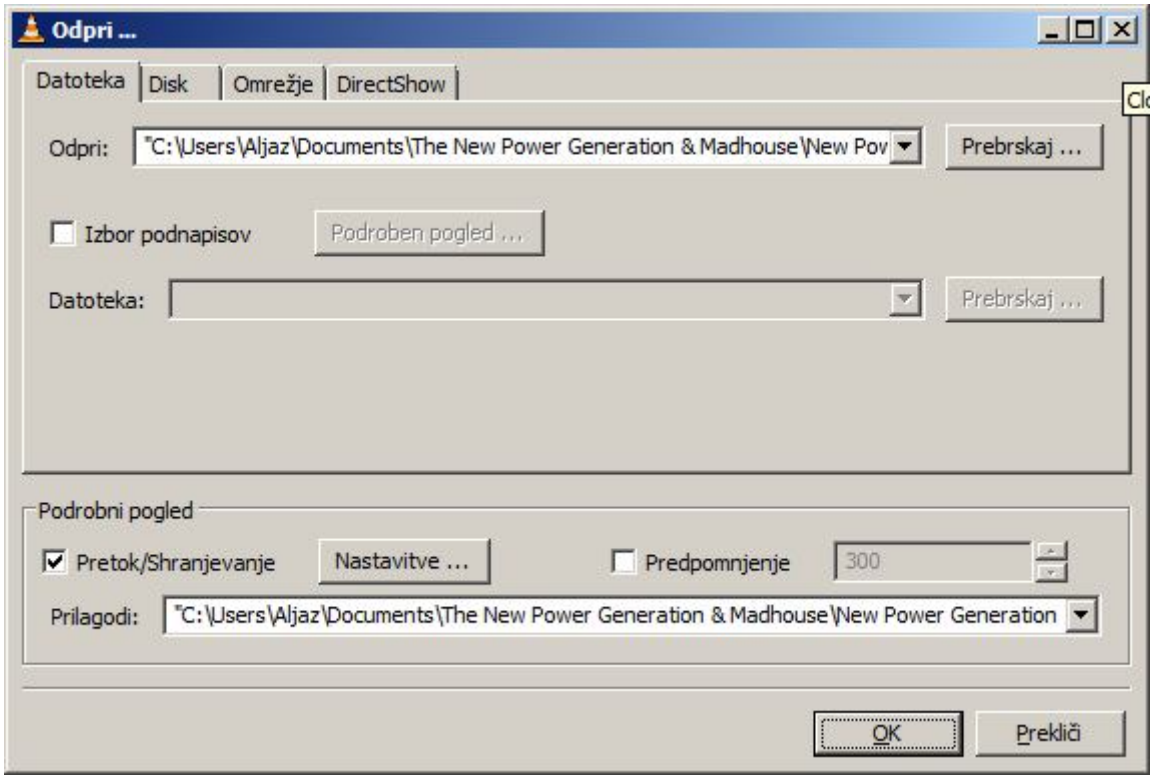
Rezultat dosegljivosti gostitelja po vnosu statične poti. Tokrat uspešno. Ko je cilj postal dosegljiv, tudi ni bilo več problemov s pošiljanjem podatkovnega toka na naslov multicastne skupine 224.2.2.2.

11.7.1 POŠILJANJE PODATKOVNEGA TOKA MULTICAST:

Za oddajanje streama na strežniku PC-Toshiba sem uporabil široko uporabljeni predvajalnik **VLC media player.**

Slika 11-9: Predvajalnik VLC

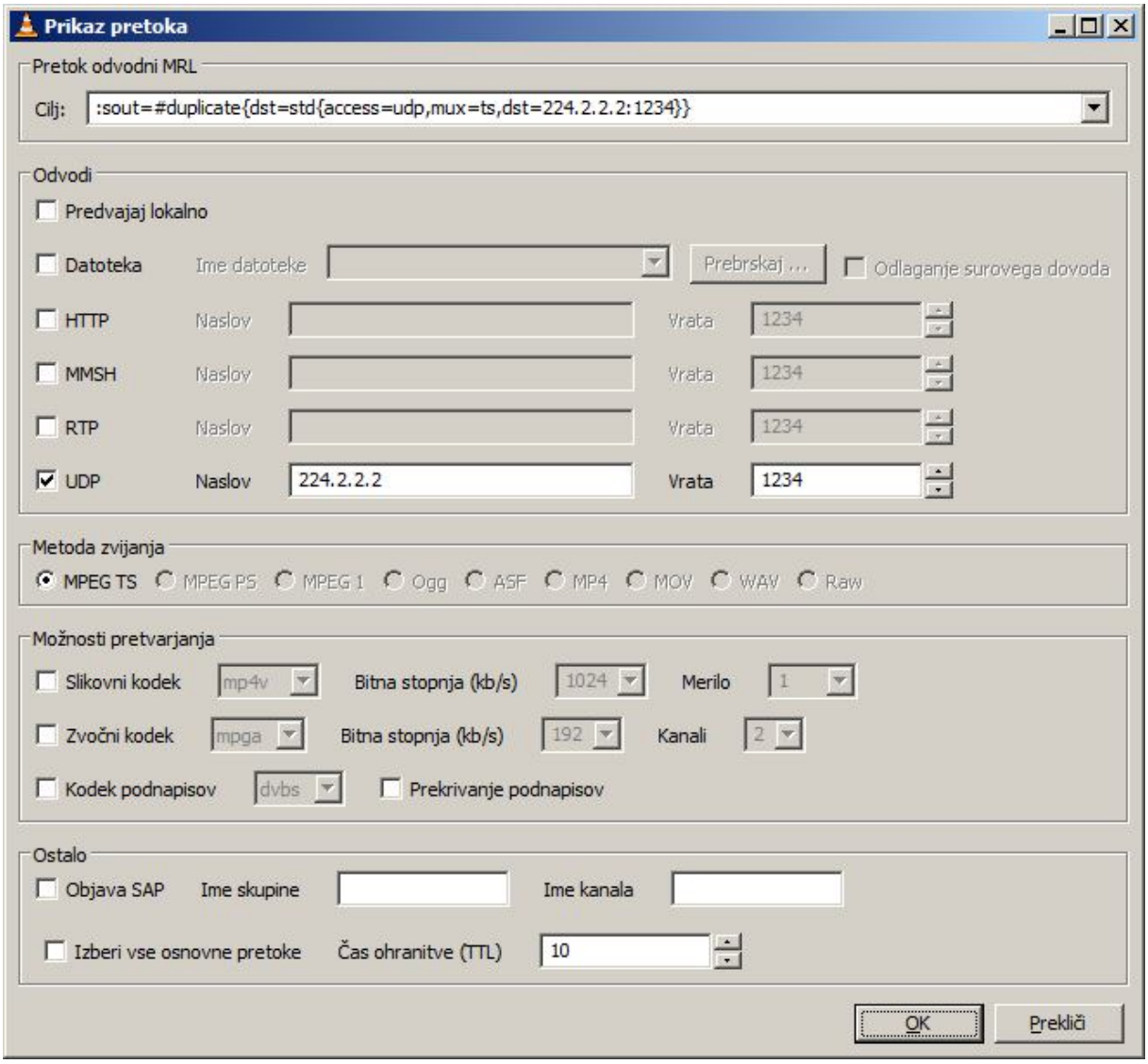
V zavihku »datoteka« izberemo parameter »odpri«, kjer se nam odpre sledeče okno:



Slika 11-10: Nastavitev predvajalnika VLC

V zavihku » prebrskaj« izberemo želeno datoteko. Sam sem opravil testiranje streama z mp3- in divx-datotekami.

Odpremo zavihek »nastavitve«, kjer nastavimo še ostale potrebne parametre:

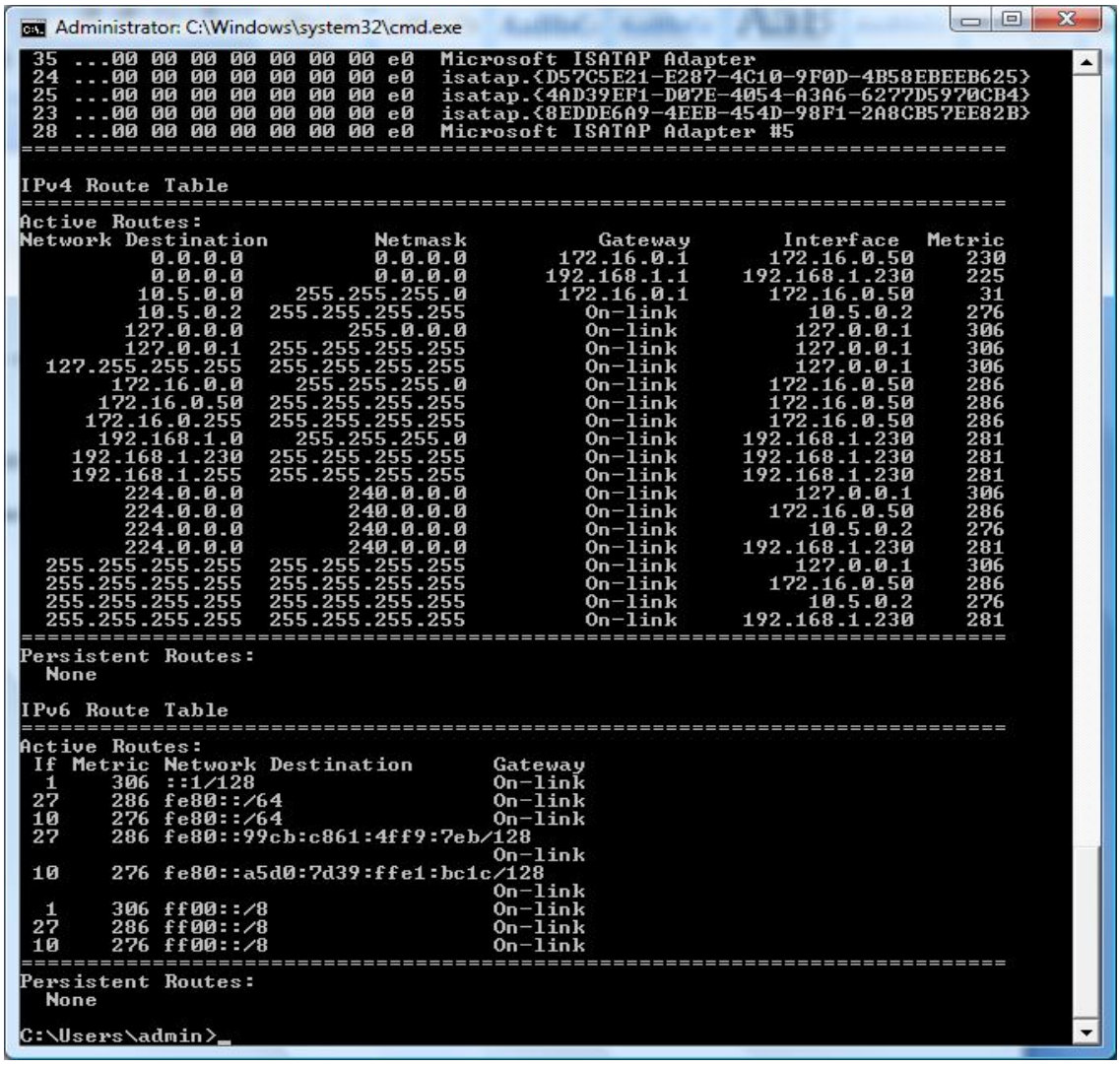


Slika 11-11: Konfiguracija predvajanja datoteke na predvajalniku VLC

Označimo zavihek UDP ter vnesemo naslov naše ciljne skupine 224.2.2.2. Nastavimo še TTL-opcijo na 10. TTL predstavlja število skokov skozi usmerjevalnike. Sedaj imamo vse potrebne parametre za oddajo podatkovnega toka. Ko kliknemo OK, se začne promet oddajati na želeni naslov.

11.8 NASTAVITEV ODJEMALCA TER PREJEMANJE PODATKOVNEGA TOKA MULTICAST

Odjemalec je prenosni računalnik PCLenovo, ki tudi poganja testne usmerjevalnike. PCLenovo ima do navideznega okolja (štirih usmerjevalnikov) dve povezavi. Ena povezava gre preko oblaka C0 do klientovega usmerjevalnika RA4CE, ki je speljana preko vmesnika Microsoft loopback. Vmesnik je bilo potrebno namestiti. IP-vmesnika na PCLenovo je 172.16.0.50, vmesnika IP ethernet na RA4CE pa je 172.16.0.1, ki je tudi privzeti prehod MS loopback adapterja na PCLenovo. Drugi vmesnik na PCLenovo je fizični vmesnik ethernet. Ta vmesnik je povezan preko oblaka C1 do robnega usmerjevalnika RA1PE in je namenjen kot »most« med strežnikom PCToshiba in robnim usmerjevalnikom vmesnika RA1PE. IP ethernet na PCLenovo je 10.5.0.2.



Slika 11-12: Pregled poti na PCLenovo - Klientu

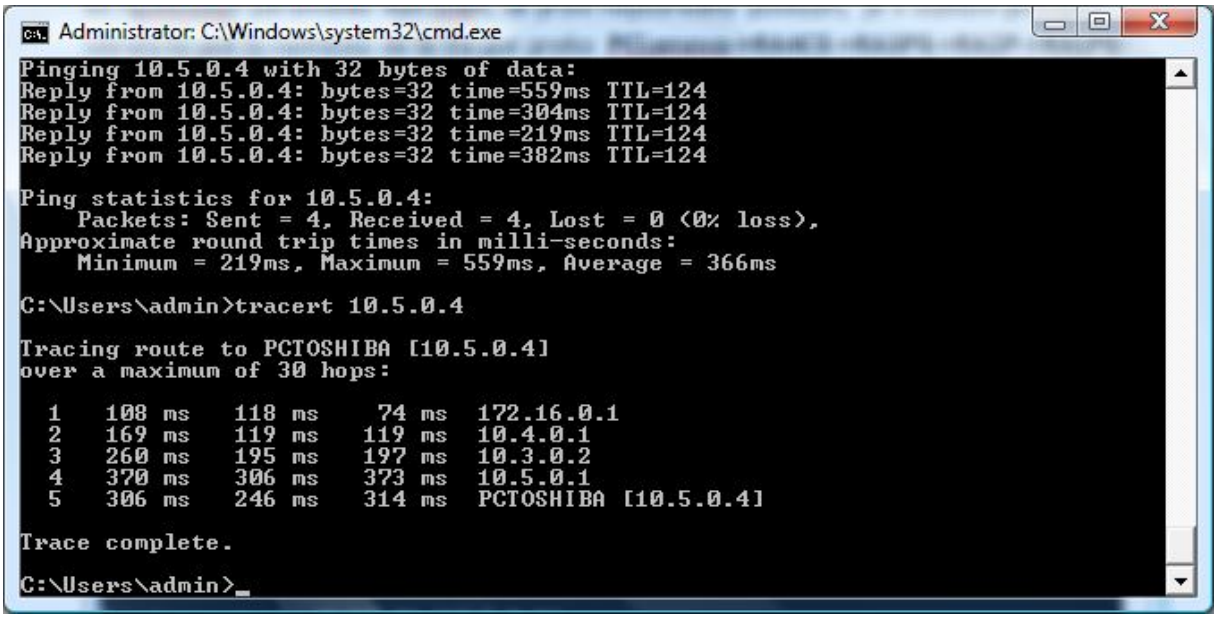
Ker sta zaradi potreb LABA fizična vmesnika ethernet na obeh PC-jih v istem podomrežju – to je **10.5.0.0/24**, je bilo potrebno nekaj »igranja« z routingom. Na primer: če sem iz CMD (command prompta) na odjemalcu PCLenovo preverjal dosegljivost strežnika **PCToshiba** (**ping 10.5.0.4**) ali prehoda do labovega usmerjevalnika **RA1PE** (**10.5.0.1**), je izbralo najboljšo pot. Ker je bil »gateway« parameter »on-link«, se pravi neposredno povezan, je v vsakem primeru izbralo to pot in namesto da bi šla pot preko **PCLenovo->RA4CE->RA3PE->RA2P->RA1PE->PCToshiba**, je bila pot do IP-vmesnika na PCToshiba **10.5.0.4** neposredna povezava **PC-Lenovo->PCToshiba**. To pa za naše potrebe nikakor ni prava pot.

Potrebna je bila odstranitev poti 10.5.0.0/24 iz gateway »on link« in to pot usmeriti na vmesnika gateway ethernet labovega usmerjevalnika RA4CE – 172.16.0.1.

To sem naredil z ukazoma:

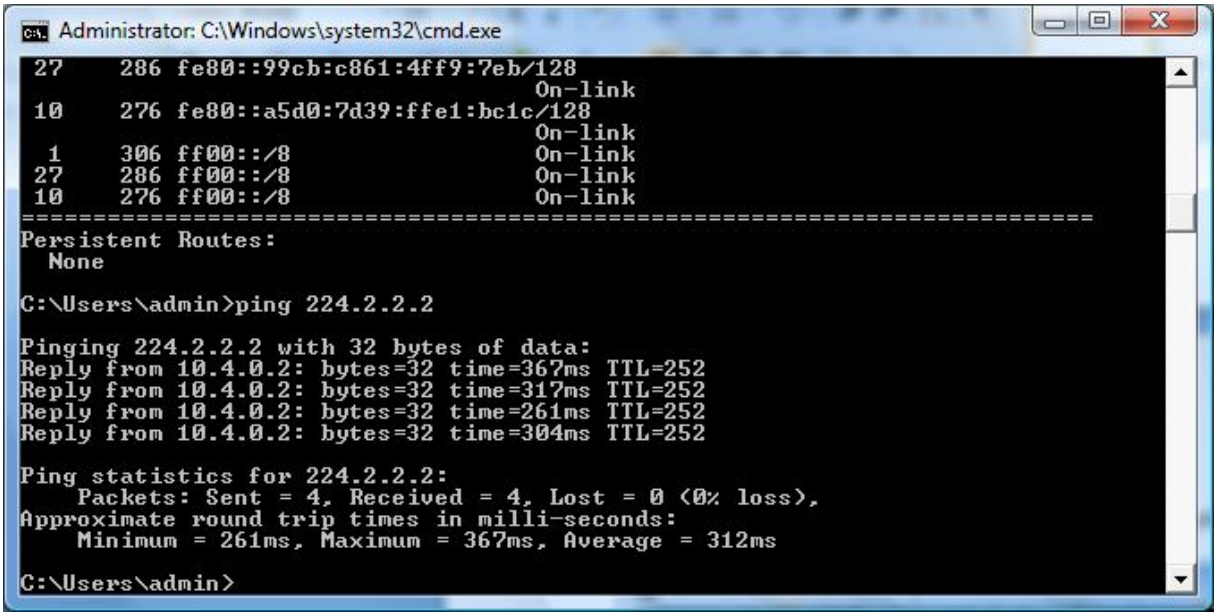
route delete 10.5.0.0 ; route add 10.5.0.0. mask 255.255.255.0 172.16.0.1 metric 10

Da se prepričamo, ali je tokrat pot pravilna, izvedemo ukaz ***tracert 10.5.0.4:***



Slika 11-13: Pregled poti do strežnika PCtoshiba

Preverimo še dosegljivost gostitelja skupine multicast 224.2.2.2:



Slika 11-14: Preverjanje dosegljivosti naslova skupine

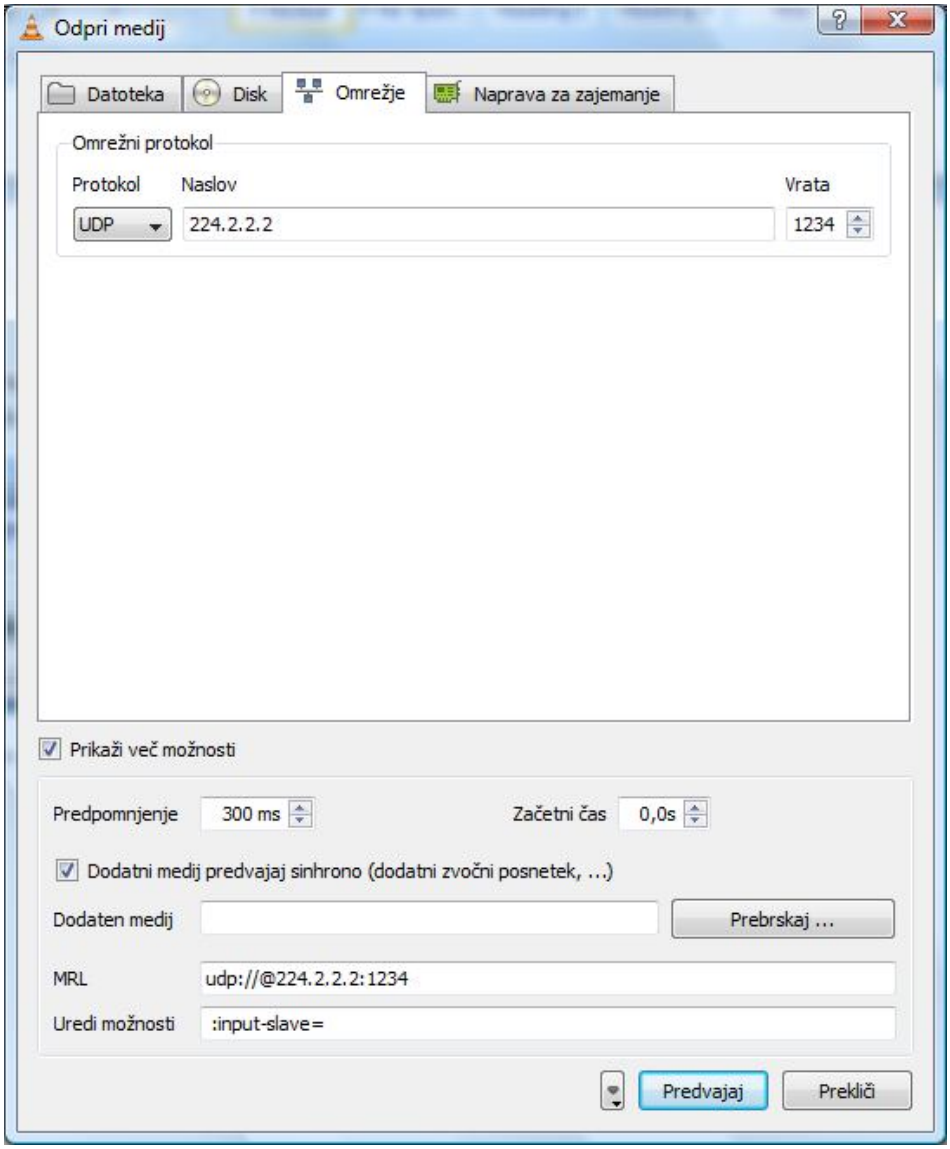
Deluje. Sedaj Lahko nastavimo predvajalnik na odjemalcu.

11.8.1 NASTAVITEV ODJEMALCA IN PREJEMANJE PODATKOVNEGA TOKA MULTICAST

Tako kot v primeru strežnika tudi na odjemalcu uporabimo predvajalnik VLC . Predvajalnik na odjemalcu je novejše izvedbe, zato tudi malo drugačen pogled.

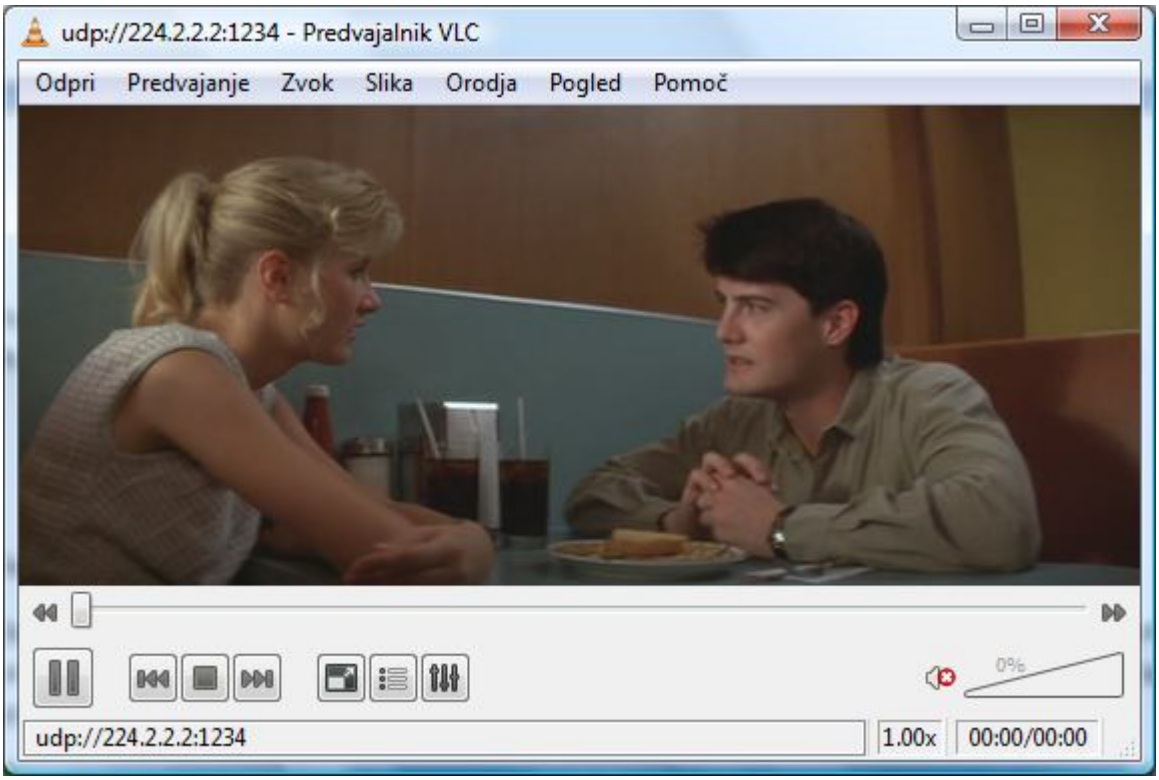
V zavihku »odpri« izberemo »odpri omrežni pretok«:

Slika 11-15: Predvajalnik VLC na odjemalcu



Slika 11-16: Konfiguracija predvajalnika VLC na odjemalcu

Pod možnostjo »protokol« izberemo UDP ter vnesemo naslov skupine multicast – 224.2.2.2. Pritisnemo na »Predvajaj« in začnemo s predvajanjem filma ali glasbene datoteke.



Slika 11-17: Prikaz predvajanja video datoteke

Kakovost slike predvajanih datotek je presenetljivo dobra, občasno se pojavi zatikanje (»zmrzovanje«), kar je posledica procesorske obremenitve na odjemalcu, ki mora poleg predvajanja skrbeti še za poganjanje štirih usmerjevalnikov.

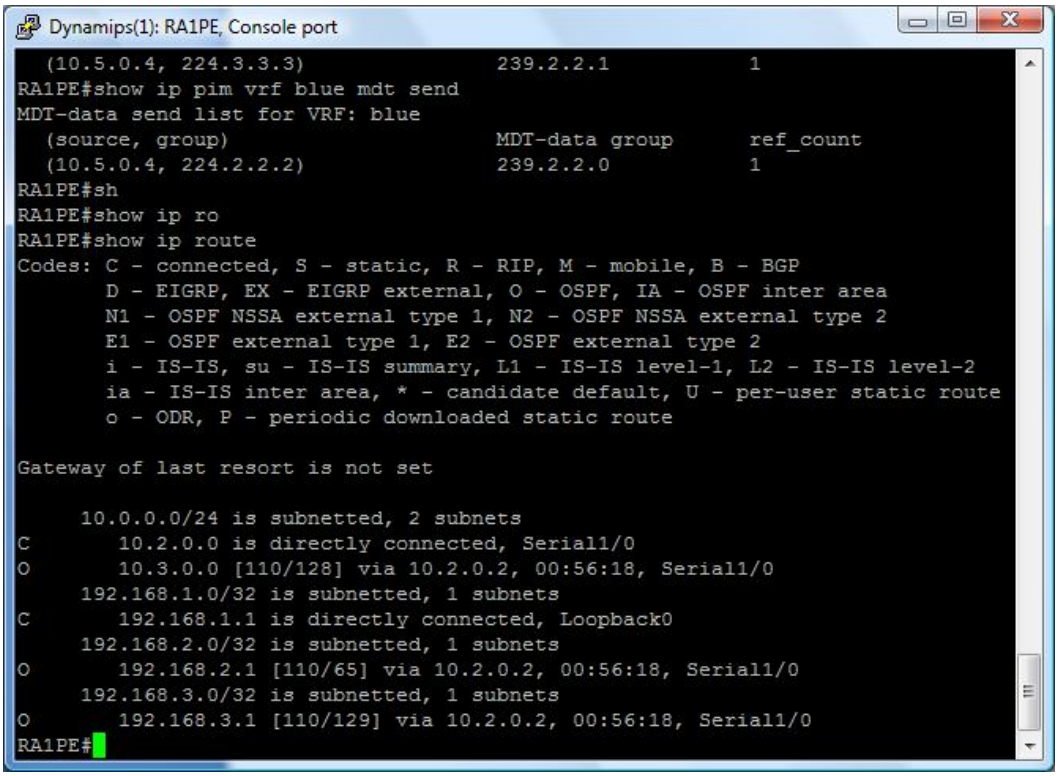
11.9 PRIMERJAVA DELOVANJA Z IMPLEMENTACIJO NAČINA mVRF IN BREZ

Pošiljanje toka multicast sem izvedel na oba načina, z implementacijo multicast VPN ter brez njega. Oba načina sta bila uspešna v tem pogledu, da sem uspešno pošiljal in prejemal multicast promet. Razlika v konfiguraciji je že omenjena, konfiguracija potrebna za izvedbo mVPN je označena z rdečo barvo. Prikazal bom še delovanje v obeh načinih.

11.9.1 PRIKAZ DELOVANJA Z IMPLEMENTACIJO mVPN

Izpis poti na robnem usmerjevalniku RA1PE

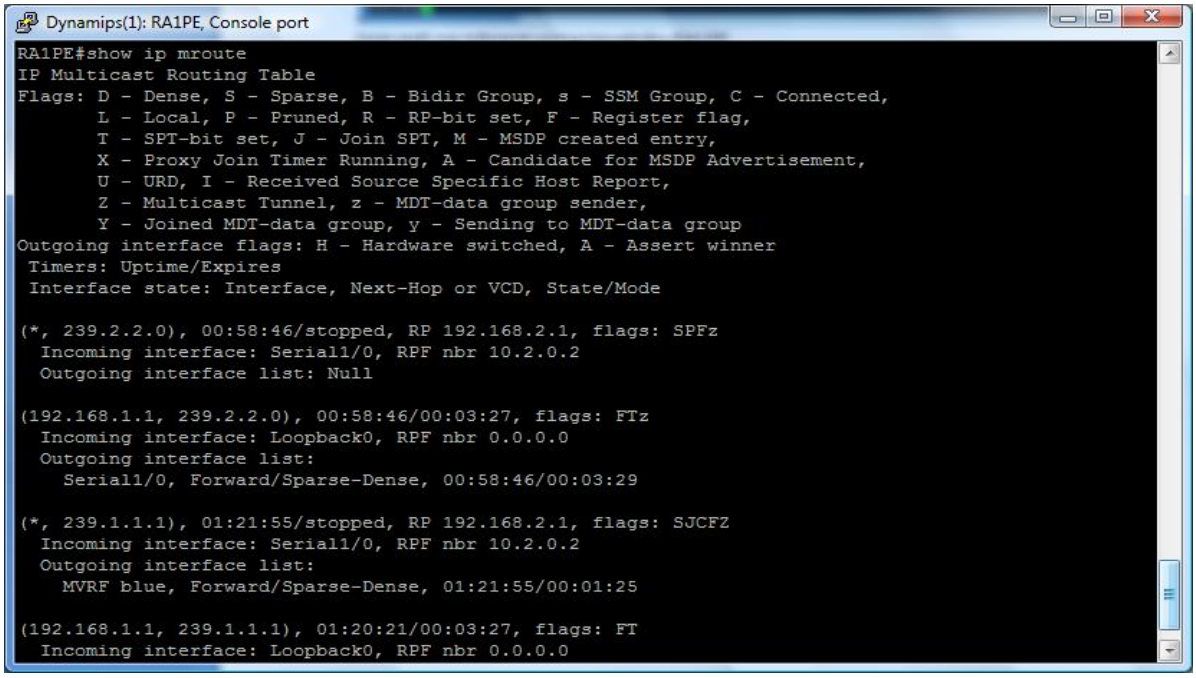
Z ukazom ***show ip route*** preverimo globalno usmerjevalno tabelo.



Slika 11-18: Pregled globalne usmerjevalne tabele na robnem usmerjevalniku

Tukaj se vidijo samo IPv4-poti. Te prikazujejo neposredno povezane vmesnike in vmesnike dostopne preko usmerjevalnega protokola OSPF.

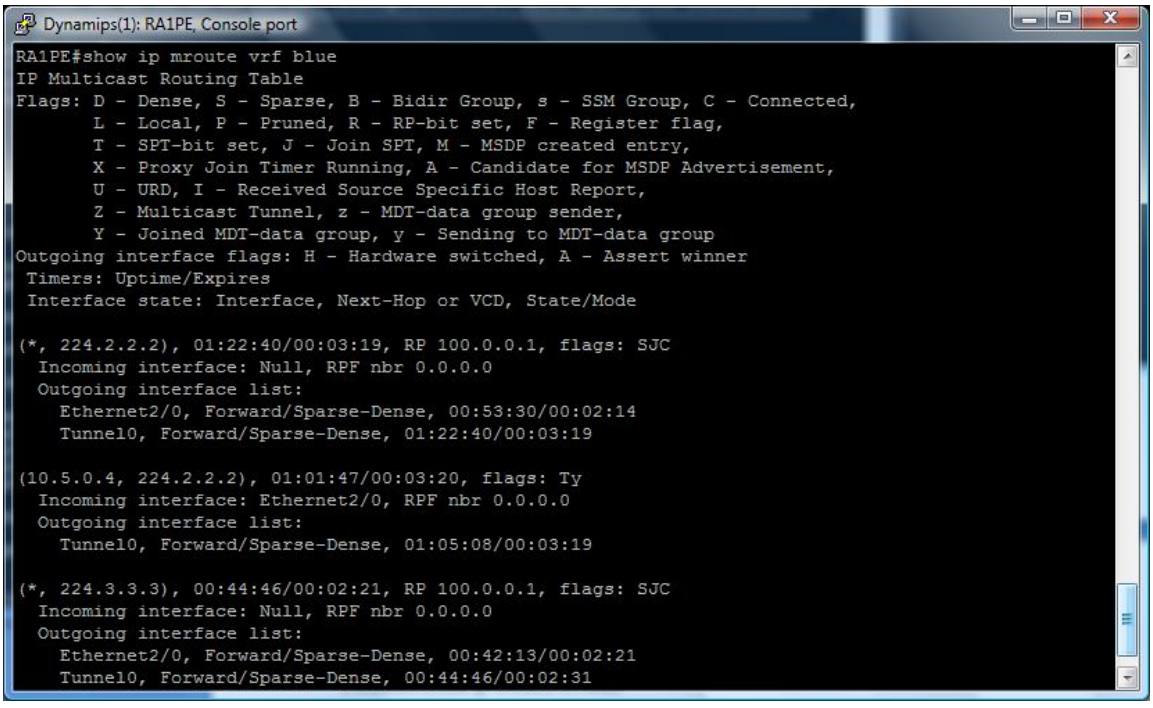
Z ukazom show ***ip mroute*** se nam izpiše globalna usmerjevalna tabela IP multicast.



Slika 11-19: Globalna usmerjevalna tabela multicast na robnem usmerjevalniku

S tem ukazom preverimo dosegljivost vmesnikov, na katerih je omogočen multicast. To velja samo za vmesnike, ki nimajo omogočenega VPN-a.

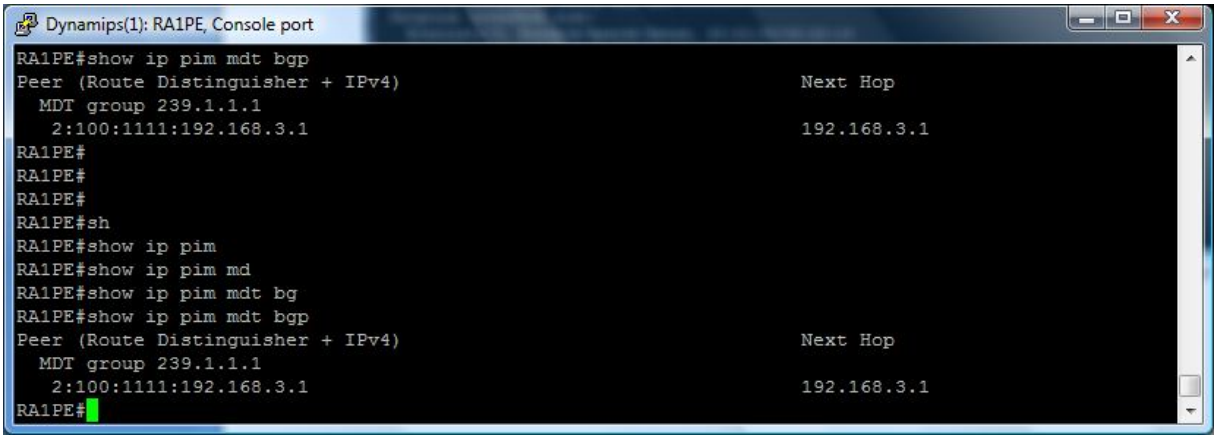
Z ukazom show ***ip mroute vrf blue*** se nam izpiše IP-multicast-usmerjevalna tabela vrf-ja.



Slika 11-20: Usmerjevalna tabela multicast VPN na robnem usmerjevalniku

V označeni vrstici je v našem primeru vir (S,G) – S - PCToshiba z ipjem 10.5.0.4, skupina multicast –G 224.2.2.2. Izhodni vmesnik je *Tunnel0* – to je logična VPN- povezava med obema robnima usmerjevalnikoma RA1PE ter RA3PE.

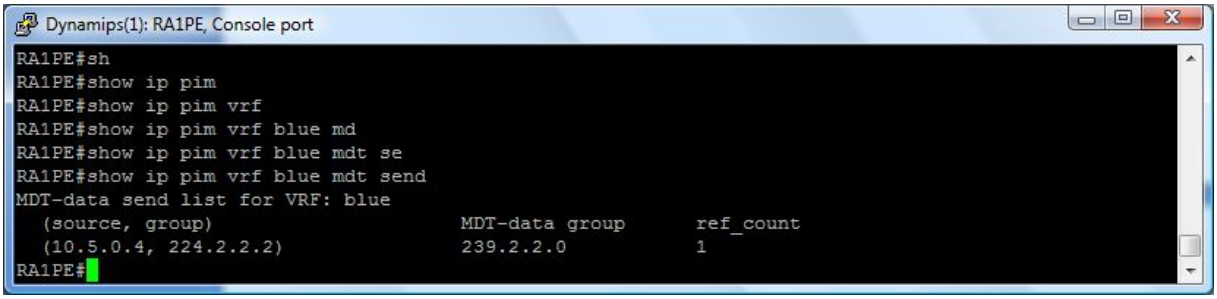
Ukaz ***show ip pim mdt bgp*** nam prikaže BGP-oglaševanje RD-poti za privzeto MDT-skupino.



Slika 11-21: BGP-oglaševanje za privzeto MDT-skupino

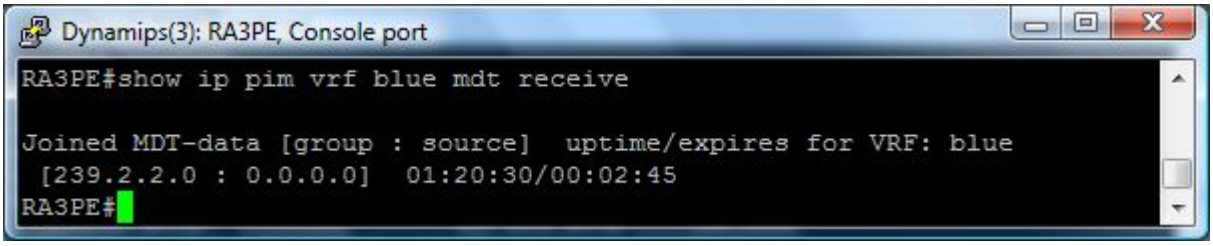
Privzeta MDT-skupina ima multicast ip 239.1.1.1, IP naslednjega skoka pa je 192.168.3.1, to je naslov loopback drugega robnega usmerjevalnika RA3PE.

Ukaz ***show ip pim vrf blue mdt sent*** nam prikaže MDT-usmerjevalnikovo oglaševanje v VRF-blue na robnem usmerjevalniku RA1PE.



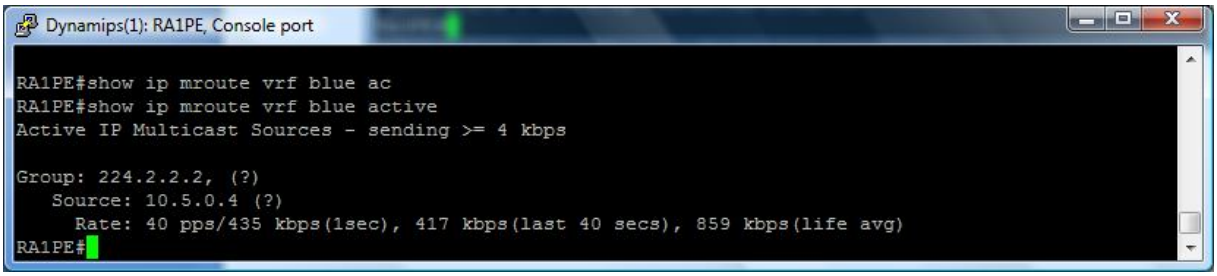
Slika 11-22: MDT-oglaševanje na robnem usmerjevalniku

Na drugem robnem usmerjevalniku RA3PE z ukazom ***show ip pim vrf blue receive*** prikažemo MDT-oglaševanje, prejeto preko usmerjevalne instance **blue.**



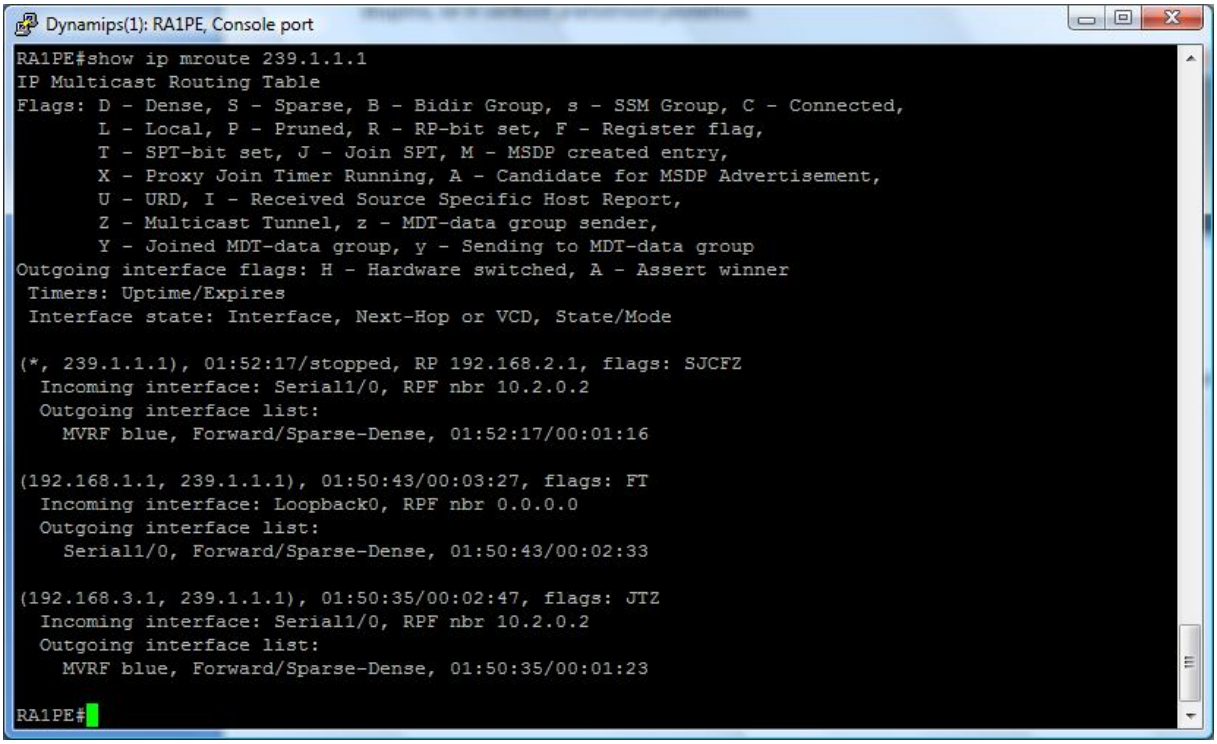
Slika 11-23: MDT-oglaševanje na drugem robnem usmerjevalniku

Ukaz show ***ip mroute vrf blue active*** na usmerjevalniku RA1PE nam prikaže aktivno skupino VRF-multicast, vir prometa multicast in prenos podatkov.



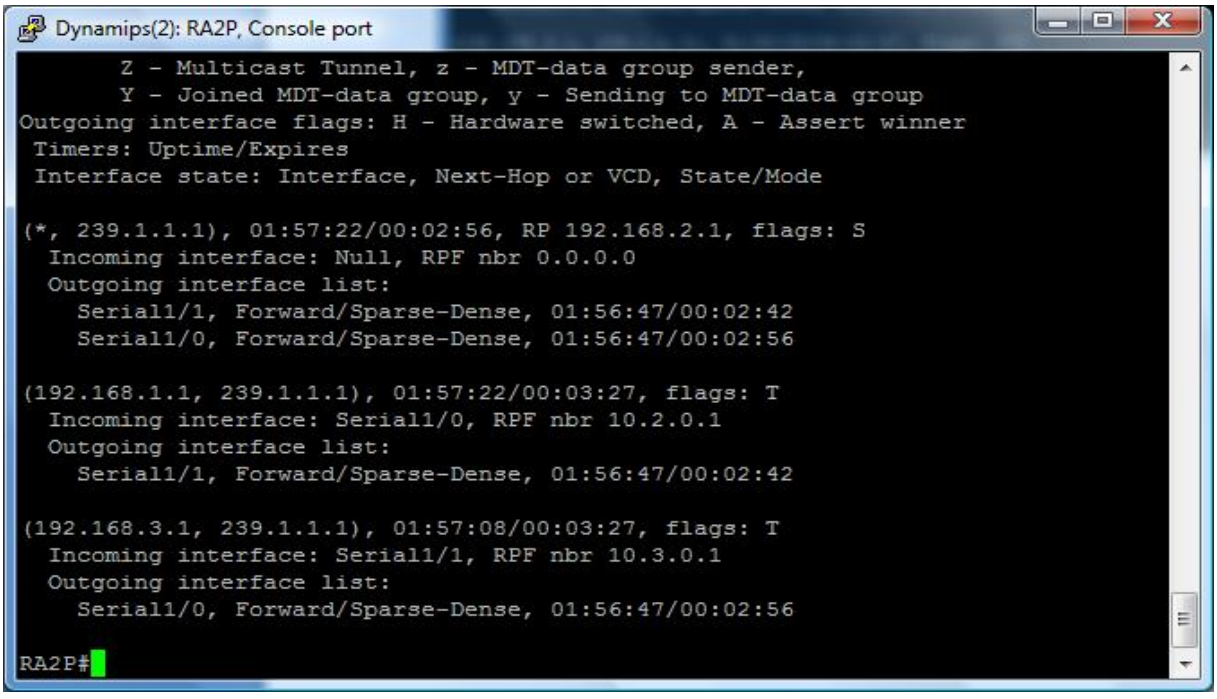
Slika 11-24: Aktivni promet se pošilja na skupino multicast

Na RA1PE preverimo globalno multicastno usmerjevalno tabelo za privzeto multicastno distribucijsko drevo (default MDT) z ukazom ***show ip mroute 239.1.1.1.***



Slika 11-25: Pot multicast do 239.1.1.1

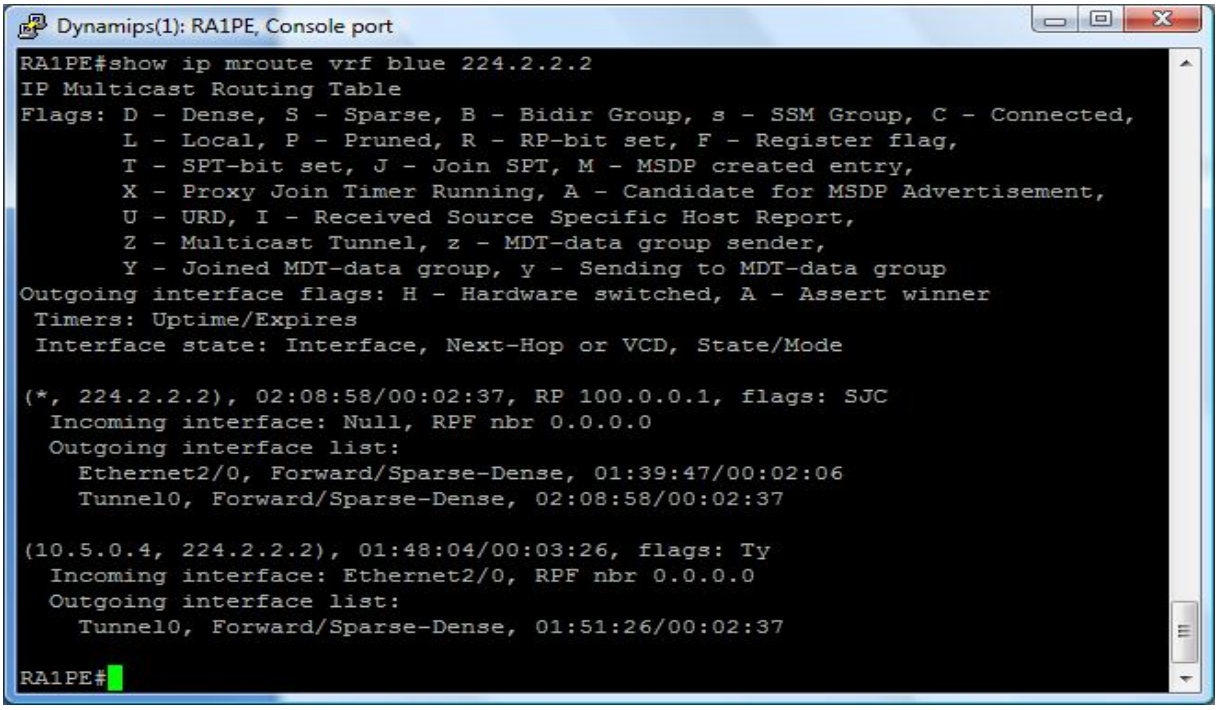
Enak ukaz izvedemo še na jedrnem usmerjevalniku RA2P.



Slika 11-26: Pot multicast do 239.1.1.1 na jedrnem usmerjevalniku

Če primerjamo izpis na obeh usmerjevalnikih, opazimo razliko na »Outgoing interface list«. Na RA1PE se globalna tabela zapiše v mVRF blue, jedrni usmerjevalnik RA2P pa ne »prepozna« omenjene usmerjevalne instance in skrbi za usmerjanje med obema robnima usmerjevalnikoma. Zato nam tudi ne prikaže naslova skupine 224.2.2.2, na katerega pošiljamo multicastni podatkovni tok. Naslov skupine je viden samo na PE-usmerjevalnikoma, RA1PE ter RA3PE, ki imata omogočen mVPN.

Na RA1PE preverimo multicast pot v usmerjevalni instanci za našo skupino multicast 224.2.2.2. To storimo z ukazom: ***show ip mroutevrf blue 224.2.2.2***



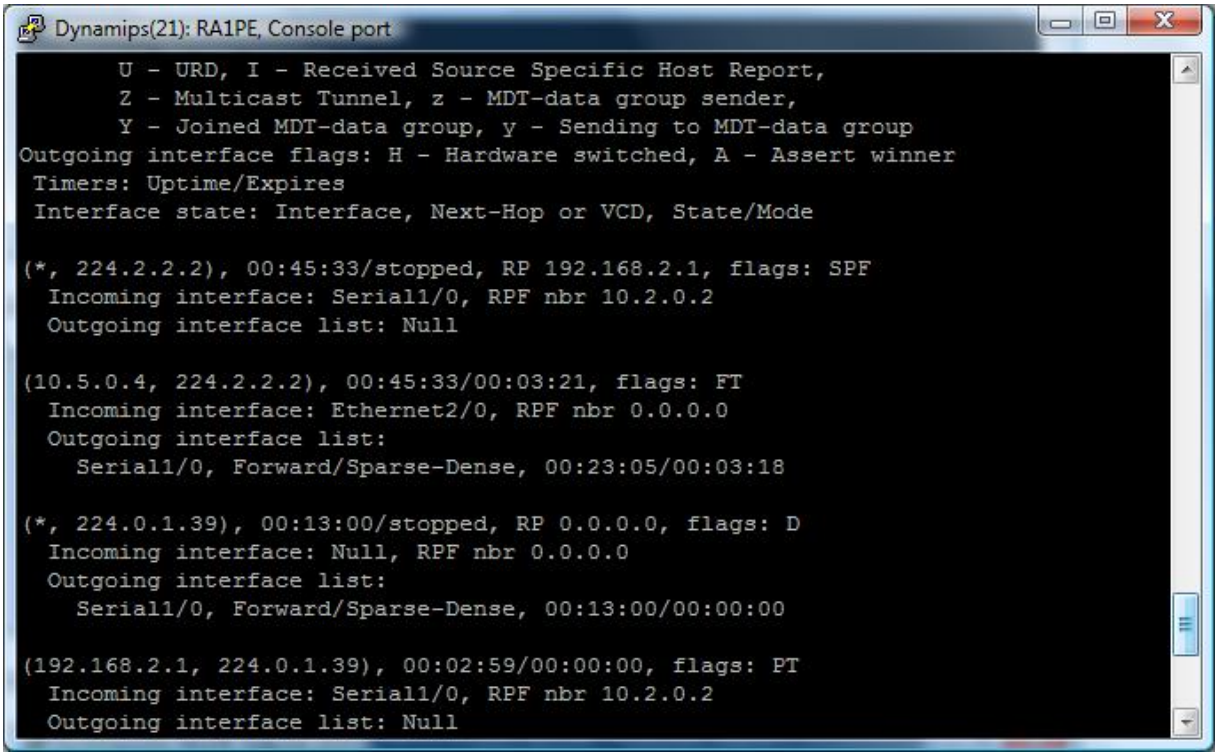
Slika 11-27: Pot do multicastne skupine 224.2.2.2

Na zgornji sliki se nazorno vidi naslov vira in naslov skupine v VPN-usmerjevalni instanci »blue«. Naslov vira je 10.5.0.4, ki je naslov vmesnika na strežniku PCToshiba.

11.9.2 PRIKAZ DELOVANJA BREZ IMPLEMENTACIJE mVPN.

V tem primeru smo iz zgoraj prikazane konfiguracije odstranili del, ki je bil pobarvan rdečo. Na vseh vmesnikih ostane omogočeno usmerjanje multicast, onemogočili oziroma odstranili pa smo VPN-podporo obema PE-usmerjevalnikoma. To povzroči, da se poti multicast, ki so bile prej oglaševane samo znotraj določenega VPN (v našem primeru VPN-instanca »blue«), začnejo oglaševati tudi v globalni multicastni tabeli.

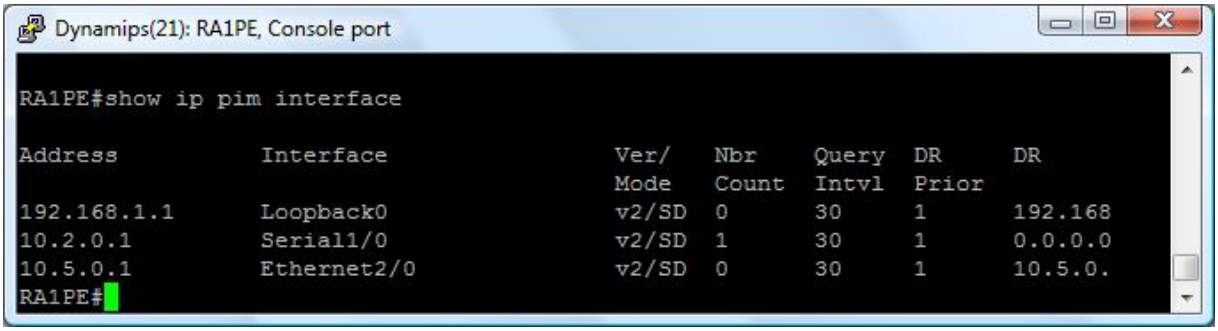
Z ukazom ***show ip mroute*** se prikaže globalna multicastna usmerjevalna tabela.



Slika 11-28: Globalna tabela multicast na robnem usmerjevalniku

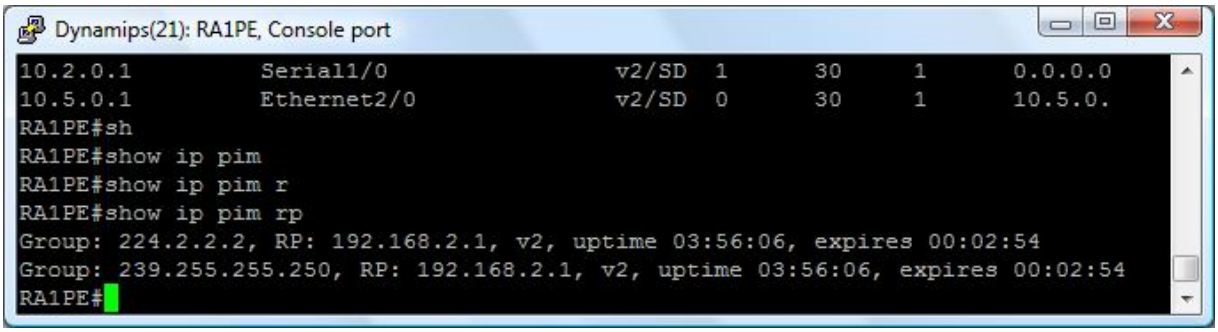
Izpis poti multicast na RA1PE. V tem primeru je skupina 224.2.2.2 v privzeti tabeli multicast poti. Skupina 224.2.2.2 je sedaj v globalni multicastni usmerjevalni tabeli. Do nje se da dostopati preko vseh multicastno omogočenih vmesnikov (prej samo prek VPN-instance »blue«). To da je določena skupina multicast vidna v globalni multicastni tabeli, povzroča tudi nepotrebno »obremenitev« jedrnega usmerjevalnika RA2P in globalne multicastne tabele. Pošiljanje prometa (multicast) znotraj VPN-instance je tudi bistveno bolj varna, ker promet ni viden navzven.

Z ukazom show ***ip pim interface*** vidimo vse PIM-vmesnike na lokalnem usmerjevalniku.



Slika 11-29: PIM-vmesniki na robnem usmerjevalniku

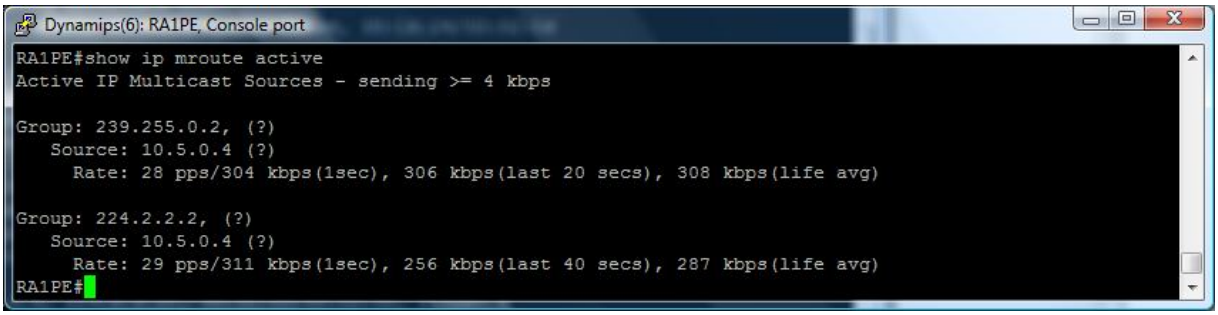
Z izvedbo ***show ip pim rp*** lahko vidimo IP-usmerjevalnika, ki je bil izbran za RP.



Slika 11-30: Za RP je bil izbran jedrni usmerjevalnik

Za RP je izvoljen usmerjevalnik RA2P z naslovom loopback 192.168.2.1.

Ukaz ***show ip mroute active*** aktivne multicastne poti.



Slika 11-31: Aktivni promet multicastne skupine 224.2.2.2

Na zgornji sliki lahko vidimo aktivno multicastno pot, naslov skupine ter vir prometa multicast. Prikazuje tudi poslano število paketov in kilobitov na sekundo. V tem primeru sem pošiljal iz vira 10.5.0.4 na dva naslova multicastne skupine. Skupina 224.2.2.2 je v globalni multicastni usmerjevalni tabeli. Do nje se da dostopati preko vseh multicastno omogočenih vmesnikov. V primeru implementacije multicast VPN, je bil naslov te skupine samo v določeni VPN instanci.

12 SKLEP

S praktičnim primerom sem vsaj delno potrdil dano teorijo. Namreč, če želimo pošiljati promet multicast med dvema ali več VPN-lokacijami, je potrebna implementacija multicast VPN na ponudnikovem omrežju. Ker sem imel dva računalnika, sem »simuliral« samo eno VPN-instanco z dvema lokacijama, ob večjem omrežju pa bi lahko imel dve ali več VPN-instanc ter več lokacij, kjer bi omenjena teorija še bolj prišla do izraza.

Tehnologija Multicast VPN je torej primerna za večje oziroma bolj zahtevne (enterprise) stranke, ki uporabljajo multicastne aplikacije znotraj svojega VPN preko hrbtenice omrežja internetnega ponudnika. Uporablja se predvsem za videokonference in občutljive realnočasovne aplikacije, kot tudi za navaden prenos podatkov.

Na platformi cisco drugega načina za zagotavljanje te storitve (z vidika ponudnika) zaenkrat ni. Za stranke sicer obstaja možnost implementacije ipv4 GRE-tunelov med VPN- lokacijami, vendar ta rešitev je kompleksna, še posebej če ima uporabnik več kakor dve takšni lokaciji. Izvirni multicast ni dovolj, če želimo to storitev zagotavljati različnim klientom. V takšnem primeru bi prejemali multicastni podatkovni tok iz strankine lokacije preko robnega PE-usmerjevalnika do jedrnega P-usmerjevalnika, to pa vsekakor ni dobro, saj se s tem nepotrebno obremenjuje jedrni usmerjevalnik, problem pa bi tudi povzročalo upravljanje s temi skupinami (nepreglednost).

Glavno prednost izvedbe mVPN vidim v tem, da lahko klienti uporabljajo poljubne naslove skupin multicast, brez bojazni, da bi se ti naslovi prekrivali med seboj v globalni multicastni tabeli. Tako imata lahko dve različni stranki isti naslov skupine multicast, vendar se ta dva naslova ne bosta videla med seboj, ker sta v dveh ločenih VPN-instancah. Se pravi, da so naslovi teh skupin nevidni za jedrne usmerjevalnike in tako ne obremenjujemo globalne multicastne tabele na jedrnem P-usmerjevalniku. Še ena izmed prednosti je razmeroma nekompleksna implementacija na PE-usmerjevalnikih, impelentiramo jo lahko v že obstoječi VPN-instanci.

Tehnologija multicast VPN še ni povsem standardizirana, tako da se lahko pojavlja več različnih rešitev (Cisco ima v uporabi predlogo rosen-draft - [draft-rosen-vpn-mcast-11.txt]).

V prihodnosti lahko pričakujemo standardizacijo mVPN na različnih platformah, bodoči razvoj se lahko tudi pričakuje skupaj z IPv6-tehnologijo.

Sama konfiguracija mi ni predstavljala posebnih problemov, saj sem navajen okolja Cisco, na katerem delam vsakodnevno. Do sedaj tudi nisem imel veliko izkušenj z tehnologijo multicast, precej več delam na MPLS VPN, ki je ena izmed storitev v ponudbi poslovnim strankam. Multicast VPN v našem podjetju zaenkrat (še) ne ponujamo, pojavljajo pa se povpraševanja, tako da je vprašanje časa, kdaj bomo začeli ponujati tudi to storitev.

13 UPORABLJENI VIRI:

[1] Sherlia Shi: Design of Overlay Networks for Internet Multicast , 2002.
http://www.arl.wustl.edu/~sherlia/thesis/chap1/node3.html

[2] Beau Williamson, Developing IP Multicast Networks, Cisco Press, 2000.

[3] Edwards, Giuliano, Wright: Interdomain Multicast Routing, Addison Wesley, 2002.

[4] Arnes: Osnove ip naslavljanja, 2002.
http://www.arnes.si/dokumenti/filtri/node38.html

[5] Juniper networks: JUNOS 6.0 Internet Software Configuration Guide: Multicast.
http://www.juniper.net/techpubs/software/junos/junos60/swconfig60-multicast/html/

[6] Cisco IOS Multicast configuration guide
http://cisco.biz/en/US/docs/ios/ipmulti/configuration/guide/12_4/imc_12_4_book.html

[7] RFC 3376: Internet Group Management Protocol, Version 3
http://www.ietf.org/rfc/rfc3376.txt

[8] Protokol IGMPv3: http://www.javvin.com/protocolIGMP.html

[9] Dragoslav Petrovič, Boštjan Vlaovič: Orodja za uporabo omrežja MBone, 2001.
http://routemyworld.com/2009/01/22/bsci-ip-multicast-pim-routing-protocol/

[10] RFC 4271: A Border Gateway Protocol 4 (BGP 4), 2006
http://tools.ietf.org/html/rfc4271

[11] RFC 2547: BGP/MPLS VPNs, 1999
http://tools.ietf.org/html/rfc2547

[12] RFC 3031: Multiprotocol Label Switching Arhitecture, 2001
http://tools.ietf.org/html/rfc3031

[13] Juniper Networks: JUNOS 5.3 Internet Software Configuration Guide: MPLS Applications
http://www.juniper.net/techpubs/software/junos/junos53/swconfig53-mpls-apps/html/

[14] Cisco Systems: Internetworking Technology Overview, 1999.

[15] Peter Grošelj: Multicast Ipv6 preko MPLS: Diplomsko delo, F.E., 2008.

[16] Alberto Ornaghi: Protokol IGMPv3 http://alor.antifork.org/talks/**IGMP**-**v3**.ppt

[17] http://www.javvin.com/protocolMPLS.html

[18] LDP internet draft: http://tools.ietf.org/html/draft-ietf-mpls-ldp-07

[19] RFC 2547: BGP/MPLS VPNs http://www.ietf.org/rfc/rfc2547.txt

[20] MPLS Virtual Private Networks Configuration, Cisco Systems

[21] Multicast VPN Data Sheet, Cisco Systems

[22] Juniper Networks PIM-SSM,:
http://www.juniper.net/techpubs/software/junos/junos60/swconfig60-multicast/html/pim-intro7.html

[23] Cisco Systems – Bidirectional PIM
http://www.cisco.com/en/US/docs/ios/12_1t/12_1t2/feature/guide/dtbipim.html

[24] Ivan Pepelnjak, Jim Guichard – MPLS and VPN Architectures, Ciscopress, 2003.

[25] Cisco Systems – Multicast VPN data sheet [Layer 3 VPN]

[26] Za seznam kratic sem uporabljal naslednji naslov: http://slovar.ltfe.org/

14 UPORABLJENE KRATICE

KRATICA	ANGLEŠKI PREVOD	SLOVENSKI PREVOD
(S,G)	(Source, Group)	Vir, skupina
AS	Authonomous System	Avtonomni sistem
ATM	Asynchronous Transfer Mode	Asinhroni prenosni način
BGP	Border Gateway Protocol	Protokol mejnih usmerjevalnikov
BIDIR-PIM	Bidirectional Protocol Independent Multicast	Dvosmerni protokol neodvisno oddajanje več prejemnikom
CBT	Core Based Trees	Jedrna drevesa
CDP	Cisco Discovery Protocol	Cisco-ov protokol odkrivanja omrežja
CE	Customer Edge Router	Robni usmerjevalnik pri uporabniku
CEF	Cisco Express Forwarding	Cisco hitro odpošiljanje
CIDR	Classless Inter-Domain Routing	Brezrazredno meddomensko usmerjenje
CoS	Class of Service	Storitveni razred
CR-LDP	Constraind-based LDP	Protokol za izmenjevanje oznak z omejitvami
DNS	Domain Name Server	Strežnik domenskih imen
DVMRP	Distance Vector Multicast Routing Protocol	Usmerjevalni protokol za oddajanje več prejemnikom na osnovi vektorske razdalje
EIGRP	Enhanced Interior Gateway Routing Protocol	Izpopolnjen protokol za izmenjavo usmerjevalnih informacij znotraj domen
EBGP	Exterior Gateway Protocol	Protokol zunanjih usmerjevalnikov
FEC	Forward Error Correction	Vnaprejšnje popravljanje napak
FR	Frame Relay	Blokovno posredovanje
GRE	Generic Routing Encapsulation	Generično ovijanje pri usmerjanju
IBGP	Internal BGP	Notranji BGP
ICMP	Internet Control Message Protocol	Protokol internetnega krmilnega sporočila
IETF	Internet engineering task force	Delovna skupina za internetno inženirstvo
IGP	Interior Gateway Protocol	Protokol notranjih usmerjevalnikov
IGMP	Internet Group Management Protocol	Internetni protokol za upravljanje skupin
IOS	Internetwork Operating System	Medomrežni operacijski sistem
IPSEC	Internet Protocol Security	Varnostni protokol IP
IP	Internet Protocol	Internetni protokol
IPv4	Internet Protocol version 4	Internetni protokol verzije 4
IPv6	Internet Protocol version 6	Internetni protokol verzije 6
IPTV	Internet Protocol Televison	Televizija na osnovi internetnega protokola
ISP	Internet Service Provider	Ponudnik internetnih storitev
ISO OSI	ISO Open System Interconect	Odprti sistem povezovanja ISO
L2F	Layer-2 Forwarding	Posredovanje na drugem sloju
L2TP	Layer-2 Tunneling Protocol	Tunelski protokol na drugem sloju
LAN	Local Area Network	Lokalno omrežje
LDP	Label Distribution Protocol	Protokol za izmenjavo oznak
LSP	Label Switched Path	Označeno komutirana pot
LSR	Label Switched Router	Usmerjevalnik s komutacijo oznak

MAC	Media Access Control	Krmiljenje dostopa do medija
MBGP	Multicast Border Gateway Protocol	Večprejemniški protokol mejnih usmerjevalnikov
MBone	Multicast backbone	Hrbtenično omrežje z oddajanjem več prejemnikom
MDT	Multicast Distribution tree	Multicastno distribucijsko drevo
MIB	Management Information Base	Baza upravljavskih informacij
MLD	Multicast Listener Discovery Protocol	Multicastni protokol za odkrivanje poslušalcev
MOSPF	Multicast Open Short Path First	Multicastna prosta najkrajša pot naprej
MPLS	Multiprotocol Label Switching	Večprotokolna komutacija z zamenjavo oznak
MTI	Multicast Tunnel Interface	Multicastni vmesnik tunel
MVPN	Multicast Virtual Private Network	Multicastno navidezno privatno omrežje
MVRF	Multicast Virtual Routing and forwarding table	Multicastna usmerjevalna in posredovalna tabela VPN
NAT	Network Address Translation	Prevajanje omrežnih naslovov
NMS	Network Management System	Sistem za nadzor in upravljanje omrežja
OIL	Outgoing Interface List	Seznam izhodnih vmesnikov
OSPF	Open Short Path First	Prosta najkrajša pot najprej
OSI	Open System interconnect	Odprti sistem povezovanja
P	Provider Core (Router)	Jedrna naprava (usmerjevalnik) ponudnika
PDU	Protocol Data Unit	Protokolno podatkovna enota
PE	Provider Edge (Router)	Robna naprava (usmerjevalnik) ponudnika
PIM	Protocol Independed Multicast	Protokolno neodvisen multicast
PIM-DM	PIM-Dense Mode	PIM-zgoščeni način
PIM-SM	PIM-Sparse Mode	PIM-raztreščeni način
PIM-SSM	PIM-Source Specific	PIM- protokol neodvisno oddajanje
QoS	Quality of Service	Kakovost storitve
RD	Route Distinguishers	Usmerjevalnik razločevalnih smeri
RFC	Request For Comments	Poziv za komentarje
RIP	Routing Information Protocol	Usmerjevalni informacijski protokol
RP	Rendezvous Point	Točka stičišča
RPF	Reverse Path Forward	Metoda povratne poti
RPT	Rendezvous Point Trees	Multicastna drevesa točke stičišča
RSVP	Resource Reservation Protocol	Protokol z rezervacijo virov
RSVP-TE	RSVP Extensions for Traffic Engineering	RSVP z dodatkom za prometni inženiring
RT	Route Target	Cilj usmerjanja
SNMP	Simple Network Management Protocol	Preprosti protokol za upravljanje omrežja
SPT	Shortest Path Trees	Drevesa najkrajše poti
STP	Spanning Tree Protocol	Protokol vpetega drevesa
TCP	Transfer Control Protocol	Protokol za krmiljenje transporta
TTL	Time To Live	Življenjski čas paketa
TVL	Time Value Length	Tip – vrednost – dolžina
UDP	User Datagram Protocol	Uporabniški datagram protokol
VC	Virtual Circuit	Navidezni vod
VLSM	Variable Length Subnet Mask	Maska podomrežja spremenljive dolžine

VRF	Virtual Routing and Forwarding	Virtualno usmerjanje in posredovanje
VRRP	Virtual Router Redundancy Protocol	Virtualni usmerjevalni redundantni protokol
VPN	Virtual Private Network	Navidezno zasebno omrežje
VTP	Vlan Trunking protocol	Vlan povezovalni protokol
WAN	Wide Area Network	Prostrano omrežje