

**/Zavod za
telekomunikacije**

Diplomski studij FER2

Informacijska i komunikacijska tehnologija

Telekomunikacije i informatika

Obradba informacija

Komunikacijski protokoli

Radna inačica udžbenika v1.0

Ignac Lovrek, Maja Matijašević, Gordan Ježić, Dragan Jevtić

Akademска година 2021./2022.



SVEUČILIŠTE U ZAGREBU

**Fakultet
elektrotehnike i
računarstva**

Predgovor

Radna inačica udžbenika „Komunikacijski protokoli” namijenjena je studentima diplomskog studija informacijske i komunikacijske tehnologije na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu, a sadržajno se nastavlja na radnu inačica udžbenika „Komunikacijske mreže”. Knjiga u izradi, pod naslovom „Komunikacijske mreže i protokoli”, kao što sam naslov kaže, obuhvatit će i mreže i protokole, a bavit će se općim postavkama komunikacijskih mreža i protokola, a posebice mrežnim arhitekturama i komunikacijskim protokolima s naglaskom na Internetu, pri čemu će se obraditi temeljni koncepti i odabrani praktički primjeri.

Očekujemo da će već ova radna inačica pomoći studentima da prošire osnovno te steknu cjelovito i sustavno znanje o komunikacijskim protokolima.

Autori

Sadržaj

1. MREŽNI PROTOKOL IPV6	1
1.1 Osnovna obilježja protokola IPv6	2
1.1.1 Format osnovnog zaglavlja	3
1.1.2 Dodatna zaglavlja	5
1.2 Adresni prostor	9
1.2.1 Jednoodredišne adrese	10
1.2.2 Višeodredišne adrese	12
1.2.3 Adresa bilo kojeg iz skupa odredišta	13
1.2.4 Adrese računala i usmjeritelja	14
1.3 Upravljački protokoli za IPv6	14
1.3.1 Protokol ICMPv6	15
1.3.2 Protokol NDP	17
1.3.3 Protokol DHCPv6 i autokonfiguracija s pomoću poslužitelja	18
1.3.4 Samostalna autokonfiguracija adrese	19
1.4 Uvođenje protokola IPv6 u mrežu i postupni prijelaz s protokola IPv4 na IPv6	21
1.4.1 IPv6-adrese s uključenim IPv4-adresama	21
1.4.2 Tranzicijski mehanizmi	22
1.5 Zadaci	27
2. POKRETLJIVOST U IP-MREŽI	29
2.1 Protokol Mobile IP	30
2.1.1 Adrese i funkcionalni entiteti	32
2.1.2 Otkrivanje agenta	34
2.1.3 Registracija i deregistracija pokretnog čvora	36
2.1.4 Usmjeravanje datagrama	40
2.2 Protokol Mobile IPv6	42
2.2.1 Adrese i funkcionalni entiteti	42
2.2.2 Otkrivanje usmjeritelja i promjene poveznice	43
2.2.3 Registracija i deregistracija pokretnog čvora	44
2.2.4 Optimizacija usmjeravanja	45
2.3 Ostali modeli pokretljivosti	48
2.4 Zadaci	49

3. PROTOKOLI USMJERAVANJA U INTERNETU	51
3.1. Besklasno usmjeravanje	52
3.2. Protokol RIP	52
3.2.1. Format zaglavlja	53
3.2.2. Nedostaci protokola	53
3.2.3. Poboljšanja protokola	54
3.2.4. Primjeri rada protokola	54
3.2.5. Proširenje protokola za rad u mreži IPv6	59
3.3. Protokol OSPF	59
3.3.1. Format zaglavlja	61
3.3.2. Primjeri rada protokola	61
3.3.3. Proširenje protokola za rad u mreži IPv6	64
3.4. Protokol BGP	64
3.4.1. Poruke	65
3.4.2. Atributi	66
3.4.3. Algoritam odabira staze	68
3.4.4. Komunikacija usmjeritelja	70
3.4.5. Regionalni internetski registar	71
3.5. Zadaci	72
4. SIGNALIZACIJSKI PROTOKOLI U INTERNETU	75
4.1. Protokol SIP	75
4.1.1. Poruke	78
4.1.2. Zahtjevi	79
4.1.3. Odgovori	81
4.1.4. Međudjelovanje mrežnih elemenata	83
4.2 Zadaci	85
LITERATURA	87

1. Mrežni protokol IPv6

Mrežni protokol IP u inačici IPv4 temeljni je protokol Interneta, kao i svih drugih IP-mreža. Protokol IPv4, specificiran početkom 1980-tih godina¹, mrežni je protokol koji pruža nespojnu uslugu bez potvrde izvedenu datagramski: svaki se paket usmjerava zasebno kroz mrežu, svaki usmjeritelj odluku o usmjeravanju pojedinog datagrama donosi neovisno o usmjeravanju ostalih datagrama.

Protokol IPv4 sadrži minimalni skup funkcija za dostavu datagrama s kraja na kraj mreže, a moguće probleme u komunikaciji prepušta na rješavanje višem, transportnom sloju. To se odnosi na povremeni gubitak paketa zbog pogreške, smetnji ili kvarova na nekoj od poveznica na putu, povremeni gubitak paketa zbog zagušenja u nekom od mrežnih čvorova ili dostavu paketa s narušenim redoslijedom u slučaju kad se tijekom komunikacije promijeni izbor puta kroz mrežu. Takve situacije stvaraju dodatne probleme s kvalitetom usluge. Retransmisija datagrama koju pokreće transportni sloj s kraja na kraj mreže kako bi ispravio pogrešku može izazvati veće kašnjenje, a slaganje paketa u izvorni slijed isto tako utječe na kašnjenje. Nadalje, pošiljatelj paketa nema povratnu informaciju o ishodu komunikacije, tj. o isporuci datagrama na odredištu.

Odlika protokola IPv4 koja je pridonijela njegovoj dominaciji nad drugim paketskim mrežnim protokolima je način dostave datagrama na odredište: najbolje moguće („best effort“) s obzirom na uvjete u mreži, tj. najbrže, s najmanjim mogućim kašnjenjem, ali bez ikakvih jamstava kad će i hoće li datagram stići na odredište. Druga je njegova važna odlika neovisnost o izvedbi nižih slojeva i njihovih protokola, čime je omogućena primjena protokola IP u različitim mrežama, fiksnim i pokretnim, žičnim, optičkim i bežičnim, od širokog do lokalnog područja, u općim i specifičnim područjima primjene. Takve su se početne postavke pri oblikovanju i specifikaciji protokola IP pokazale izvrsnima za koncept izgradnje Interneta (međusobno povezivanje (pod)mreža) te prihvat tehnoloških inovacija kojima se postižu sve veće brzine prijenosa podataka (od početnih Kbit/s do današnjih Gbit/s).

Međutim, inačica protokola IPv4 postaje ograničavajuća, jer svakim danom novi korisnici žele pristup Internetu, tako da je adresni prostor postao premalen, a ujedno se javljaju nove aplikacije i usluge veće složenosti, s novim zahtjevima. U početcima Interneta, TCP/IP se brinuo za jednostavne podatkovne aplikacije prijenosa datoteka, elektroničke pošte i rada na udaljenom računalu. U međuvremenu, Internet je postao okružje bogato aplikacijama i uslugama poput multimedije i hipermedije. Sve je veća potreba za komunikacijom između više krajnjih točaka u skupini te zahtjevnim višekorisničkim i višemedijskim uslugama i aplikacijama poput IP-telefonije i govora putem IP, višemedijske konferencije, strujanja višemedijskih podataka, i drugih, kod kojih treba postići odgovarajuću kvalitetu usluge. Internet dobiva ogroman broj novih korisnika – različitih objekata (stvari, strojeva i uređaja) za razlike primjene, što je obuhvaćeno konceptom Interneta stvari (engl. *Internet of Things*, skr. IoT). Nadalje, Internet postaje sve više poslovna mreža sa zahtjevima na sigurnost i pouzdanost, a pri pružanju informacijskih i komunikacijskih usluga treba voditi računa o zaštiti podataka i privatnosti korisnika. Složenost problema upotpunjavaju zahtjevi

¹ „Internet Protocol DARPA Internet Program Protocol Specification“, RFC 791, IETF, rujan 1981.

na pokretljivost: korisnici i uređaji moraju moći komunicirati u pokretu bez prekidanja veze, a usluge se moraju moći pružati bez prostornih i vremenskih ograničenja.

Takav razvoj Interneta nije neočekivan, tako da se pri oblikovanju i specifikaciji „novog“ protokola IP, odnosno početne inačice IPv6 već u 1990-tim godinama o tome vodilo računa^{2,3,4}. Uz IPv6, razvijani su i različiti alternativni protokoli nove generacije koji nisu prihvaćeni, primjerice IPv5⁵ i IPv7⁶.

Ograničenja uočena u primjeni protokola IPv4 rješavaju se u okviru IPv6, a posebice sljedeća:

- premalo raspoloživih adresa (32 bitne adrese),
- prevelike tablice usmjeravanja uzrokovane početnom podjelom adresnog prostora (klase adresa A, B i C), naknadno uvedenim besklassnim usmjeravanjem⁷ i nemogućnošću dodjele kompaktnog adresnog prostora svim novim korisnicima,
- nedovoljni sigurnosni mehanizmi na mrežnom sloju,
- nedovoljni mehanizmi pokretljivosti na mrežnom sloju,
- nedovoljna potpora za prijenos podataka u stvarnom vremenu te
- složeno upravljanje mrežom.

Ipak, nedostatak internetskih adresa osnovna je motivacija za uvođenje protokola IPv6 u mrežu, uz postojeći IPv4.

1.1 Osnovna obilježja protokola IPv6

Protokol IPv6⁸ zadržava dobra svojstva prethodne inačice IP-a (IPv4), a ispravlja nedostatke i unosi poboljšanja koja se mogu sažeti na sljedeće:

- veći adresni prostor (128 bitne adrese),
- pojednostavljenje formata zaglavla (fiksna duljina, manje polja),
- unaprijeđeno usmjeravanje (združivanje – agregiranje adresa sukladno potrebama davatelja usluga, organizacija i korporacija, kao i zemljopisnih područja, omogućuje jedan smjer – rutu prema njihovoj mreži, ili malo njih; uvedeni dodatni načini usmjeravanja),
- mogućnost označavanja toka, odnosno paketa koji pripadaju istom toku,
- potpora za kvalitetu usluge,
- bolja potpora za sigurnost i pokretljivost.

Kako bi se mogao adresirati veći broj krajnjih sustava (računala i drugih), IPv6 koristi 128-bitno adresiranje umjesto 32-bitnog. Osnovno zaglavlje paketa ima manje polja i fiksnu

² „Towards the Future Internet Architecture“, RFC 1287, IETF, prosinac 1991.

³ „The Recommendation for the IP Next Generation Protocol“, RFC 1752, IETF, siječanj 1995.

⁴ „Internet Protocol, Version 6 (IPv6) Specification“, RFC 1883, IETF, prosinac 1995.

⁵ „ST - A Proposed Internet Stream Protocol“, [Internet Experiment Note](#) IEN-119, IETF, rujan 1979.

⁶ „TP/IX: The Next Internet“, RFC 1475, IETF, lipanj 1993.

⁷ „Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan“, RFC 4632, IETF, kolovoz 2006.

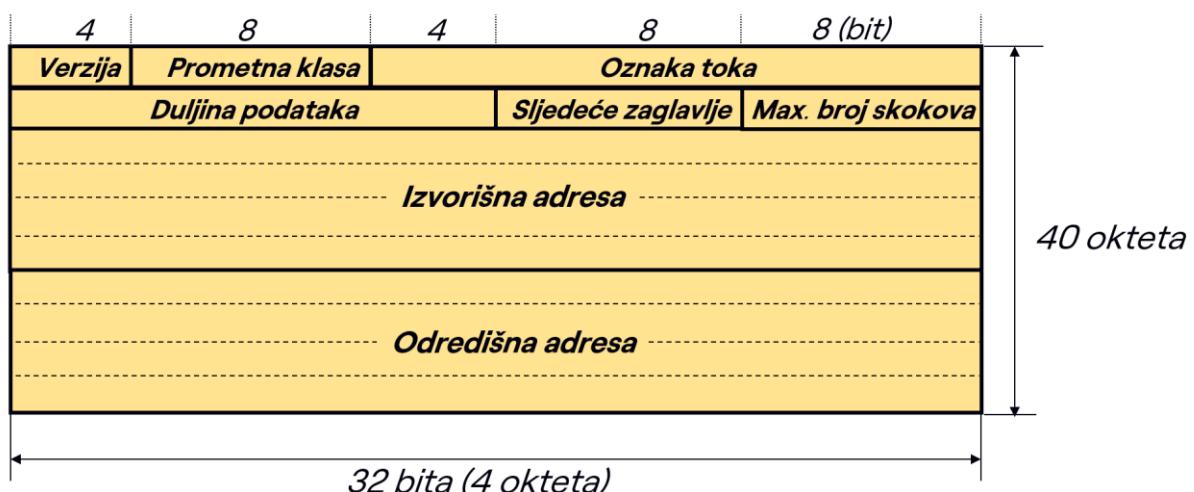
⁸ „Internet Protocol, Version 6 (IPv6) Specification“, RFC 8200, IETF, prosinac 1998.

duljinu od 40 okteta, a izbačeno je izračunavanje zaštitne sume zaglavlja, čime je omogućena brža obrada paketa u usmjeriteljima. Uvedena su posebna dodatna zaglavlja kako bi se unaprijedilo usmjeravanje i rješavali drugi specifični zahtjevi. Nadalje, fragmentacija se može vršiti isključivo na izvorišnom čvoru. Zatim, postoje mogućnost označavanja tokova paketa. Uvedeni su mehanizmi kvalitete usluge koji posebno dolaze do izražaja kod prijenosa podataka u stvarnom vremenu. Potpora za sigurnost (IPsec) i pokretljivost (Mobile IP) je unaprijedena i uključena u IPv6.

1.1.1 Format osnovnog zaglavlja

Zaglavje protokola IPv6 predočeno na sl. 1.1 sadrži sljedeća polja, s izvornim nazivima:

- Verzija (engl. *Version*) označava protokol, tj. IPv6;
- Prometna klasa (engl. *Traffic Class*) određuje rukovanje paketima ovisno o stanju mreže, tj. zagušenju;
- Oznaka toka (engl. *Flow Label*) određuje niz paketa iz nekog izvorišta namijenjenih nekom odredištu koji pripadaju istoj usluzi ili aplikaciji, a za koji se zahtijeva posebno rukovanje u usmjeriteljima (npr. rezervacija resursa);
- Duljina podataka, tj. korisnog tereta (engl. *Payload Length*);
- Sljedeće zaglavje (engl. *Next Header*) označava dodatno zaglavje koje slijedi iza osnovnog zaglavљa;
- Ograničenje broja skokova (engl. *Hop Limit*) određuje najveći broj usmjeritelja koji datagram može prijeći na putu od izvora prema odredištu;
- Izvorišna adresa (engl. *Source Address*), 128-bitna internetska adresa;
- Odredišna adresa (engl. *Destination Address*), 128-bitna internetska adresa.

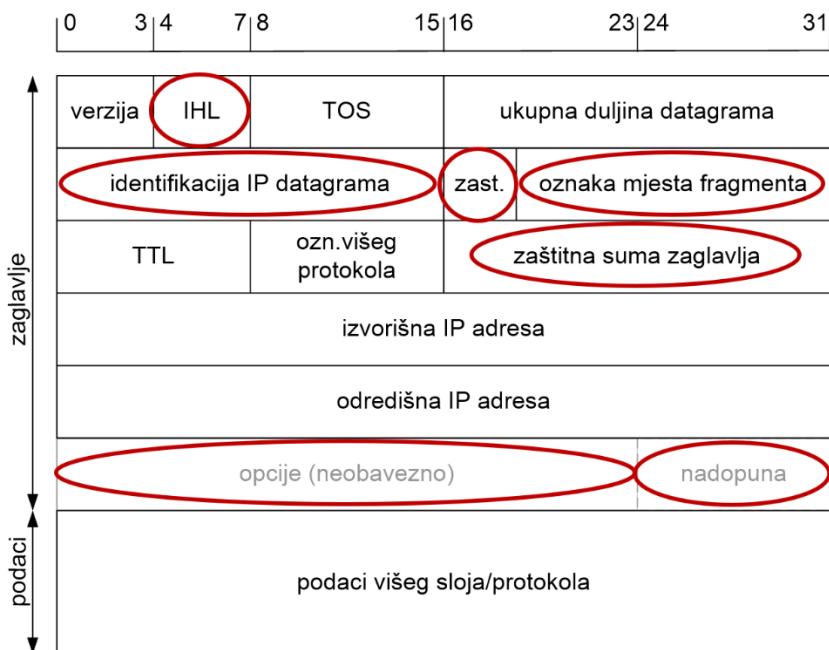


Slika 1.1 – Format zaglavja IPv6

Svi formati zaglavja u nastavku prikazivat će se u duljini 32-bitne riječi, kao što je napravljeno i na sl. 1.1. Osnovno zaglavje IPv6 fiksne je duljine od 40 okteta, a sadrži 8 polja, za razliku od zaglavja IPv4 s 14 polja (sl. 1.2). U usporedbi sa zaglavljem IPv4, zaglavje IPv6 je fiksne duljine, tako da nije potrebno označavati duljinu zaglavja (engl. *Internet Header Length*, IHL), a kako se fragmentacija provodi samo na izvoru nisu potrebna ni fragmentacijska polja za identifikaciju IP-datagrama (engl. *identification*), zastavice (engl. *flags*) i oznaku mesta fragmenta (engl. *fragment offset*). Ne provodi se niti zaštitno kodiranje zaglavja (engl.

header checksum), a posebne mogućnosti rješavaju se dodatnim zaglavljima tako da otpada i to polje (engl. *options*), kao i potreba za nadopunu zaglavja do pune duljine riječi (engl. *padding*).

Pojednostavljenja formata zaglavja omogućuju bržu obradu datagrama u usmjeriteljima i drugim mrežnim čvorovima. Detaljnije treba razmotriti izmijenjena i nova polja.



Slika 1.2 – Format zaglavja IPv4 s označenim poljima koja su izbačena iz zaglavja IPv6

Prometna klasa u IPv6 zamjenjuje vrstu usluge (engl. *Type of Service*, TOS) definiranu u IPv4. Značenje tih polja se višekratno mijenjalo u odnosu na početne specifikacije, tako da je postalo polje koje označava diferencirani uslužni razinu (engl. *Differentiated Service field*, DS field)⁹, za obje inačice protokola IP. Time se omogućuje različito postupanje s paketima („diferenciranje“), ovisno o zahtjevima usluge.

Oznaka toka omogućuje označavanje više uzastopnih paketa iz jednog izvora. Internetska adresa čvora i oznaka toka jednoznačno identificiraju svaki pojedinačni tok paketa.

Ograničenje broja skokova ekvivalentno je vremenu života paketa u IPv4 (engl. *Time To Live*, TTL) koje se isto tako mjerilo brojem skokova.

Najveća je razlika, a koja je omogućila pojednostavljenje i fiksiranje duljine zaglavja, uvođenje dodatnih zaglavja (engl. *extension header*) koja proširuju osnovno, a primjenjuju se po potrebi. Drugim riječima, IPv6-datagram s osnovnim zaglavljem putovat će mrežom bez dodatne obrade u čvorovima, za razliku od protokola IPv4 kod kojeg je obvezna provjera mogućih opcija usporavala proslijđivanje paketa u usmjeriteljima. Ako nema dodatnih

⁹ „Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers“, RFC 2474, IETF, prosinac 1998.

zaglavlja, u polju „sljedeće zaglavljje“ u osnovnom IPv6-zaglavljtu upisana je oznaka protokola višeg sloja, tj. transportnog protokola TCP ili UDP.

1.1.2 Dodatna zaglavljia

Nakon osnovnog zaglavljua fiksne duljine od 40 okteta, u protokolu IPv6 je moguće nizati dodatna zaglavljia, koja nisu obvezna, a to su:

- zaglavje skok po skok (engl. *hop-by-hop header*),
- zaglavje usmjeravanja (engl. *routing header*),
- zaglavje fragmenta (engl. *fragment header*),
- zaglavje namijenjeno odredištu (engl. *destination header*),
- zaglavje za provjeru autentičnosti (engl. *authentication header*),
- zaglavje za sigurnosno ovijanje podataka (engl. *encapsulating security payload*).

Poredak zaglavljia u IPv6-datagramu je određen, pri čemu je samo prvo obvezno, a ostala se mogu primjenjivati pojedinačno ili kombinirati uvažavajući ovakav redoslijed:

1. Zaglavje IPv6
2. Zaglavje skok po skok (engl. *Hop-by-Hop Options header*)
3. Zaglavje namijenjeno odredištu (1) (engl. *Destination Options header*)
4. Zaglavje usmjeravanja (engl. *Routing header*)
5. Zaglavje fragmenta (engl. *Fragment header*)
6. Zaglavje za provjeru autentičnosti (engl. *Authentication header*)
7. Zaglavje za sigurnosno ovijanje podataka (engl. *Encapsulating Security Payload h.*)
8. Zaglavje namijenjeno odredištu (2)
9. Zaglavje transportnog sloja (TCP, UDP)

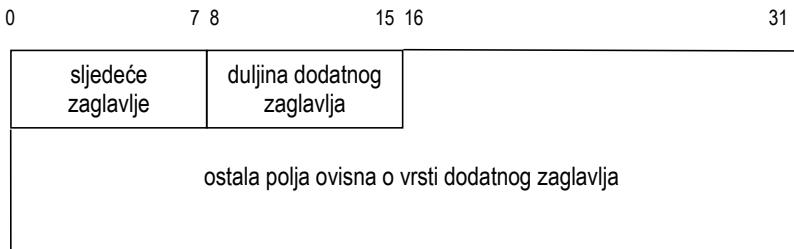
Primjeri IPv6-datograma su na sl. 1.3. Ako dodatna zaglavljia nisu potrebna, primjerice kod pristupa javnim informacijama na webu, u osnovnom zaglavljtu će se kao sljedeće zaglavje označiti TCP. Ako se datagrame želi usmjeriti posebno odabranim putem do određinskog poslužitelja, trebat će se primijeniti dodatno zaglavje usmjeravanja koje će se označiti kao sljedeće zaglavje u osnovnom zaglavljtu, a u zaglavju usmjeravanja navesti TCP-zaglavljje kao sljedeće zaglavljje.

IPv6 zaglavje slj. zaglavje = TCP	TCP zaglavje	podaci	
IPv6 zaglavje slj. zag. = zaglavje usmjereavanja	zaglavje usmjeravanja slj. zag. = TCP	TCP zaglavje	podaci

Slika 1.3 – Primjeri IPv6-datograma bez dodatnog zaglavljia i s njim

Dodatna zaglavljia mogu biti fiksne ili varijabilne duljine. Format dodatnih zaglavljia (sl. 1.4)¹⁰ uključuje polja s oznakom sljedećeg zaglavljia (8 bita) i duljinom dodatnog zaglavljia (8 bita) ako je riječ o zaglavljiju varijabilne duljine te ostala polja ovisna o vrsti zaglavljia. Duljina dodatnog zaglavljia mjeri se brojem riječi od 8 okteta (64 bita), pri čemu se prvih 8 okteta nebroji.

¹⁰ „A uniform format for IPv6 extension headers“, RFC 6544, IETF, travanj 2012.



Slika 1.4 – Format dodatnih zaglavlja

Objasnit će se značenje i primjena zaglavlja skok po skok, zaglavlja usmjeravanja, zaglavlja fragmenta i zaglavlja namijenjenih odredištu.

Zaglavljе skok po skok

Zaglavljе skok po skok je zaglavljе varijabilne duljine koje sadrži informaciju namijenjenu svakom čvoru na putu dostave datagrama. Zaglavljе skok po skok sadrži podatke o sljedećem zaglavljу, duljini samog dodatnog zaglavljа i opcиско polje s definicijom akcija koje poduzima čvor na putu datagrama. Opcиско polje sadrži jednu ili više opcija od kojih svaku definiraju sljedeći podaci:

- vrsta opcije (engl. *option type*) duljine 8 bita,
- duljina opcисkih podataka (engl. *option data length*) duljine 8 bita koja označava broj okteta opcисkih podataka te
- opcисke podatke (engl. *option data*).

Primjer primjene ovog dodatnog zaglavljа je prijenos veoma velikih paketa, npr. s video sadržajem, većih od 2^{16} okteta (tzv. "jumbogram")¹¹ na putu s velikom maksimalnom transmisijском jedinicом (MTU). Ova vrsta opcije je označena s C2 (sl. 1.5).

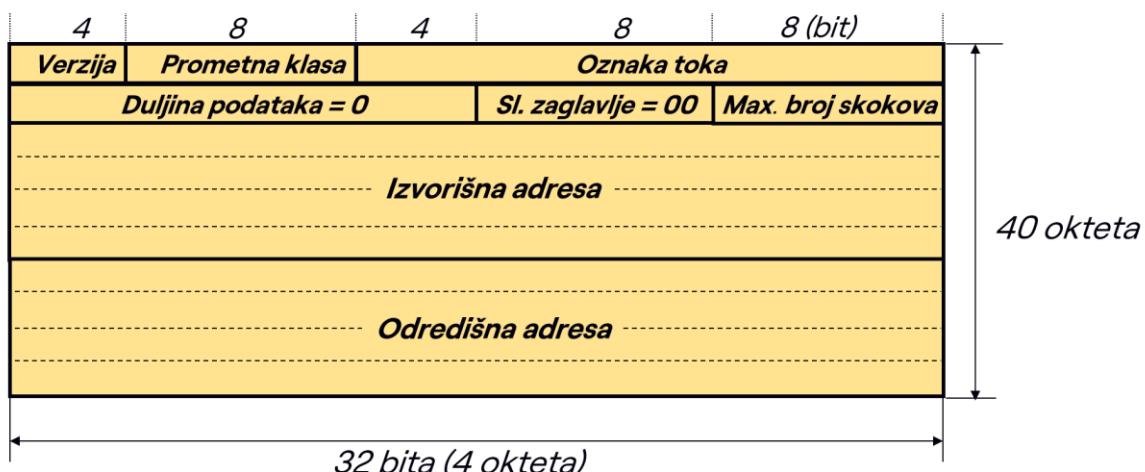
The diagram shows the structure of a Jumbo Option Extension Header. It includes fields for the next header (index 0), the length of the extension header (indices 7-8), the option type (C2, index 15), the length of options (index 16), and the payload (index 17 onwards, labeled as the length of a very large packet ("jumbogram")).

sljedeće zaglavljе	duljina dodatnog zaglavljа = 0	vrsta opcije = C2	duljina opcиских podataka = 4
duljina veoma velikog paketa ("jumbogram")			

Slika 1.5 – Dodatno zaglavljе skok po skok s opcijom prijenosa veoma velikih paketa

U ovom se slučaju u osnovnom IPv6-zaglavljу polje "duljina podataka" postavlja na „0“, a „sljedeće zaglavljе“ na „00“ čime se označava dodatno zaglavljе skok po skok s opcijom za prijenos veoma velikih paketa (sl. 1.6).

¹¹ „IPv6 Jumbograms“, RFC 2675, IETF, kolovoz 1999.



Slika 1.6 – Osnovno zaglavje iza kojeg slijedi zaglavje skok po skok

Duljina ovog dodatnog zaglavja je „0“, jer sadrži samo 8 okteta, odnosno 64 bita. Duljina opcijskih podataka je 4 (4 okteta duljine veoma velikog paketa). Duljina veoma velikog paketa (32-bitni cijeli broj) odgovara broju okteta sadržanih u paketu, isključujući njegovo IPv6-zaglavje, dok se zaglavje skok po skok i sva ostala dodatna zaglavja broje.

Čvor koji ne može rukovati takvim paketima, izvijestiti će o tome izvořišni čvor ICMP-porukom o pogrešci.

Zaglavje usmjeravanja

Zaglavje usmjeravanja je zaglavje varijabilne duljine koje omogućuje usmjeravanje datagrama po unaprijed određenom putu od izvora do odredišta. Zaglavje usmjeravanja sadrži podatke o sljedećem zaglavju, veličini samog zaglavja, vrsti usmjeravanja i popis usmjeritelja koje paket treba prijeći prije nego što dođe do odredišta.

Početna specifikacija zaglavja usmjeravanja pokazala se nesigurnom za mrežu, jer dopušta definiranje puta na kojem datogrami osciliraju između dva čvora. Stoga je takvo usmjeravanje obustavljeno i ne primjenjuje se¹². Naime, zlonamjernim usmjeravanjem velikog broja datagrama na neki čvor izaziva se zagušenje mreže i uskraćuje usluga. Definiranjem usmjeravanja koje izaziva kruženje datagrama u petlji između dva čvora postiže se upravo taj učinak!

Međutim, primjenjuje se druga vrsta usmjeravanja i to onog prema pokretnom čvoru (*Mobile IPv6*).

Zaglavje fragmenta

Zaglavje fragmenta je zaglavje fiksne duljine koje se primjenjuje za slanje datagrama većih od MTU-a puta. Treba napomenuti da IPv6 propisuje minimalni MTU od 1280 okteta. Početni dio izvornog paketa koji se ne smije fragmentirati su IPv6-zaglavje i dodatna zaglavja koja

¹² „Deprecation of Type 0 Routing Headers in IPv6“, RFC 5095, IETF, prosinac 2007.

se obrađuju na putu prije krajnjeg odredišta, a to su zaglavljे skok po skok i zaglavljе usmjeravanja. Preostali dio paketa se može fragmentirati.

Paket se formira tako da se u zadnjem zaglavljу nefragmentiranog dijela označi zaglavljе fragmenta kao sljedeće, a zatim dolazi dodatno zaglavljе fragmenta i sam fragment. Zaglavljе fragmenta (sl. 1.7) sadrži podatke o sljedećem zaglavljу i polja koja opisuju fragmente:

- polje s mjestom fragmenta (engl. *fragment offset*) koje pokazuje dio originalnog paketa mјeren u riječima od 8 okteta (64 bita) kojeg sadrži fragment,
- zastavicu M koja označava slijedi li još segmenata (bit = 1) ili je riječ o zadnjem segmentu (bit = 0) i
- identifikacijsko polje koje jednoznačno označava fragmentirani paket.

To je ista upravljačka informacija za fragmentiranje koju sadržava i zaglavljе IPv4. Međutim, datagrami se mogu fragmentirati samo na izvoru, a ako se pojavi potreba za fragmentacijom na nekom usmjeritelju na putu, takav se datagram odbacuje i izvoru šalje ICMP-poruka o prevelikom datagramu.

sljedeće zaglavljе	rezervirano (8 bit)	mjesto fragmenta (13 bit)	rez. (2 bit)	M. (1)
identifikacija				

Slika 1.7 – Dodatno zaglavljе fragmenta

Očevidno je da izvor treba ustanoviti veličinu MTU kako bi mogao provesti fragmentiranje, a to se provodi protokolom ICMPv6.

Zaglavljе namijenjeno odredištu

Zaglavljе namijenjeno odredištu je varijabilne duljine i istog formata kao zaglavljе skok po skok, a sadrži informacije namijenjene odredišnom čvoru. S obzirom na položaj, odnosno redoslijed, može biti smješteno prije zaglavljа usmjeravanja (1) ili neposredno prije zaglavljа transportnog sloja (2):

- Zaglavljе namijenjeno odredištu (1): sadrži informaciju za prvo odredište i sva odredišta sadržana u zaglavljу usmjeravanja.
- Zaglavljе namijenjeno odredištu (2): sadrži informaciju samo za krajnje odredište.

Zaglavljа namijenjena odredištu sadrže podatke o sljedećem zaglavljу, veličini samog zaglavljа te opcisko polje s jednom ili više definicija akcije koju poduzima odredišni čvor. Primjer primjene je Mobile IPv6.

1.2 Adresni prostor

Adresiranje u IPv6^{13,14} zasniva se na 128-bitnim adresama, četiri puta duljima od onih u IPv4. Povećanje adresnog prostora je enormno:

- IPv4: 4 294 967 296 čvorova, a
- IPv6: 340 282 366 920 938 463 463 374 607 431 768 211 456 čvorova,

što omogućuje gustoću internetskih adresa od 655 570 793 348 866 943 898 599 na 1 m² površine Zemlje. Međutim količina adresa nije jedina prednost: velika raspoloživost adresa omogućuje učinkovitije usmjeravanje, jer dopušta združivanje – agregiranje adresa sukladno potrebama davatelja usluga, organizacija i korporacija, kao i zemljopisnih područja. Usmjeravanje se olakšava, jer se jednom entitetu i njegovoj mreži može dodijeliti kompaktan blok adresa, tako da sve raspoložive adrese mogu imati isti mrežni dio (prefiks). To je moguće postići i za neko zemljopisno područje.

Promjene vezane uz adrese izazivaju i promjene – proširenja u sustavu imenovanja domena (engl. *Domain Name System*, skr. DNS), kako bi se omogućilo preslikavanje simboličkih naziva na IPv6-adrese.

Za razliku od IPv4-adrese koja se sastoji od 32 bita koji se korisniku predočuju kao 4 decimalna broja odvojena točkama, IPv6-adresa sastoji se od 128 bita, koji se predočuju kao 8 grupa 16-bitnih brojeva zapisanih heksadekadskom notacijom, odvojenih dvotočkama, primjerice:

EFD1:0989:AB02:7654:C4ED:890B:DE65:1240

„Stare“ IP adrese (IPv4) pretvaraju se u IPv6-adrese dodavanjem niza od 96 „0“ ispred adrese, dok će zadnja 32 bita moći ostati u dekadskom ili heksadekadskom obliku, primjerice:

IPv4: 161.53.19.201 (dekadski zapis)

IPv6: 0000:0000:0000:0000:0000:161.53.19.201 (dekadski zapis)

ili

IPv4: A135:13C9 (heksadekadski zapis)

IPv6: 0000:0000:0000:0000:0000:A135:13C9 (heksadekadski zapis)

Kako bi se olakšalo pisanje takvih adresa, uvodi se mogućnost kraćenja, zamjenom niza „0“ znakom :: (dvije dvotočke), što će biti čest slučaj pri pretvorbi 32-bitnih adresa u 128-bitne, primjerice:

:: 161.53.19.201 (dekadski zapis)

:: A135:13C9 (heksadekadski zapis)

¹³ „IP Version 6 Addressing Architecture“, RFC 4291, IETF, veljača 2006.

¹⁴ „Special Use IPv6 Addresses“, RFC 5156, IETF, travanj 2008.

Pritom se znakom :: može zamijeniti samo jedan niz "0", a da bi se adresa mogla jednoznačno interpretirati.

Nekoliko primjera sažimanja okteta koji sadrže same „0“ slijedi:

1080:0:0:0:0:8:800:200C → 1080::8:800:200C
FF01:0:0:0:0:0:101 → FF01::101
0:0:0:0:0:0:1 → ::1
0:0:0:0:0:0:0 → ::

Zamjena dvaju ili više nizova „0“ onemogućuje jednoznačnu identifikaciju adrese, jer se ne može ustanoviti koliko „0“ sadrži koji niz, kao u ovom primjeru:

1080:0:0:8:800:0:0:200C → ? 1080::8:800::200C ?

Stoga se oznaka :: može pojaviti samo jednom u adresi.

Kao i kod IPv4 adresa, postoji podjela na mrežni i računalni dio adrese, koji se koriste kod usmjeravanja paketa, a mrežni prefiks označava ovako:

IP-adresa/prefiks

Primjerice, notacija FEDC:BA98:7600::/40 definira skup adresa čiji je mrežni dio FEDC:BA98:76, odnosno prvih 40 bitova zapisanih binarno:

1111 1110 1101 1100 1011 1010 1001 1000 0111 0110.

Protokol IPv6 podržava sljedeće tri vrste adresa:

- jednoodredišna adresa (engl. *unicast*) koja određuje jedno sučelje čvora – računala ili usmjeritelja. Paket poslan na *unicast* adresu, bit će dostavljen samo sučelju kojem je dodijeljena ta IP-adresa.
- višeodredišna adresa (engl. *multicast*) koja određuje skup sučelja, obično na različitim čvorovima. Paket poslan na *multicast* adresu bit će dostavljen na sva sučelja u skupini.
- adresa bilo kojeg u skupu odredišta (engl. *anycast*) kojom se određuje samo jedno od sučelja u skupu sučelja. Paket poslan na *anycast* adresu bit će dostavljen samo jednom, najčešće najbližem članu skupa. Ta mogućnost ne postoji u IPv4.

1.2.1 Jednoodredišne adrese

Jednoodredišne adrese mogu biti definirane kao:

- globalne (engl. *global unicast*),
- lokalne na razini podatkovne poveznice (engl. *link local unicast*) ili
- lokalne na razini mjesta (engl. *site local unicast*).

Lokalnost adresa je novost uvedena s IPv6. Uz opće, primjenjuju se i posebne vrste jednoodredišnih IPv6-adresa. To su:

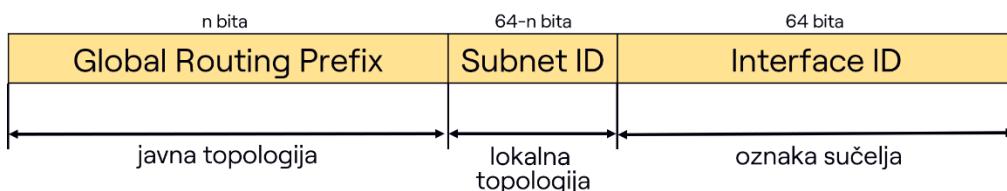
- nespecificirana adresa (engl. *unspecified address*): sastoji se od niza „0“ i kraće zapisuje kao ::. Koristi se kao i adresa 0.0.0.0 kod IPv4, najčešće kao izvorišna adresa paketa u kojima računala pokušavaju provjeriti jednoznačnost traženih adresa (npr. kod autokonfiguracije). Ta se adresa nikad ne smije dodijeliti mrežnom sučelju ili koristiti kao odredišna adresa.
- povratna adresa (engl. *loopback*): ima vrijednost ::1. Koristi se za označavanje *loopback* sučelja, čime se čvoru omogućuje da šalje podatke sam sebi kroz svoj protokolni stog. Ekvivalentna je IPv4 adresi 127.0.0.1. Paketi poslani na tu adresu ne smiju se naći na poveznici.

Globalna jednoodredišna adresa

Globalna jednoodredišna adresa globalno je jednoznačna i dostupna, a koristi se za adresiranje u javnom Internetu¹⁵. Ona označava jedinstveno sučelje mrežnog čvora. Organizirana je u agregacijske razine koje predočuju javnu i lokalnu topologiju te samo sučelje (sl. 1.8).

Značenja oznaka polja su sljedeća:

- globalni prefiks usmjeravanja (engl. *global routing prefix*) – najviši dio mrežne adrese koji omogućuje usmjeravanje do mjesta na kojem se pristupa mreži davatelja usluga, organizacije ili korporacije kojoj je globalni prefiks dodijeljen;
- identifikator podmreže (engl. *subnet ID*) – dio mrežne adrese kojim se identificira podmreža, a služi za usmjeravanje unutar mreže davatelja usluga, organizacije ili korporacije;
- identifikator sučelja (engl. *interface ID*) – identifikator sučelja u formatu IEEE EUI-64¹⁶ koji mora biti jedinstven na poveznici kojoj pripada.



Slika 1.8 – Format globalne jednoodredišne adrese

Za sve mreže osim onih kojima adrese počinju s 000, tj. koje su izvedene iz adresa IPv4, mrežni dio adrese čine globalni prefiks usmjeravanja i identifikator podmreže, ukupne duljine 64 bita, a računalni dio adrese određen je identifikatorom sučelja iste duljine. Najviša

¹⁵ „IPv6 Global Unicast Address Format“, RFC 3587, IETF, kolovoz 2003.

¹⁶ „Guidelines for 64-bit Global Identifier (EUI-64™) Registration Authority“, IEEE Standards Association

razina, tj. globalni prefiks usmjeravanja, određuje javnu topologiju mreže, a sljedeća, razina podmreže njenu lokalnu topologiju.

Podsjetimo da adresnim prostorom na razini cijelog Interneta upravlja tijelo IANA (*Internet Assigned Numbers Authority*)¹⁷ koje djeluje kao odjel neprofitne organizacije ICANN (*Internet Corporation for Assigned Names and Numbers*)¹⁸, te da je način dodjele adresa delegirajući – IANA dodjeljuje slobodne dijelove adresnog prostora regionalnim internetskim registrima (engl. *Regional Internet Registry*, skr. RIR) koji ih dalje raspoređuju nacionalnim i lokalnim internetskim registrima te davateljima internetske usluge.

Kod globalnih jednoodredišnih adresa globalni prefiks usmjeravanja strukturiraju RIR-ovi i ISP-ovi, dok je polje koje identificira podmrežu na raspolaganju mrežnom administratoru za daljnje strukturiranje.

Lokalna adresa na razini podatkovne poveznice

Ova se adresa izvodi iz MAC-adrese, dodavanjem prefiksa FE80:: (sl. 1.9) i koristi isključivo za komunikaciju čvorova na lokalnoj poveznici. Pojam „lokalne poveznice“ obuhvaća medij ili uređaj sloja podatkovne poveznice kojim se, primjerice, ostvaruje lokalnu mrežu ili više njih povezanih na sloju lokalne poveznice (most, komutator drugog sloja), ili bilo koja druga izvedba podatkovne poveznice u (pod)mreži. Lokalne adrese na razini poveznice potrebne su za autokonfiguraciju adresa i postupak otkrivanja susjednih čvorova. Usmjeritelj s potporom za IPv6 ne smije prosljeđivati pakete adresirane na takvu adresu.

10 bita	54 bita	64 bita
1111 1110 10	0000...0000	Interface ID

Slika 1.9 – Format lokalne adrese na razini podatkovne poveznice (FE80::/10)

Lokalna adresa na razini mjesta

Lokalne adrese na razini mjesta koje su predviđene u početnoj specifikaciji nisu u uporabi. Ove adrese bile su zamišljene za organizacije ili korporacije na „mjestu“ na kojem raspolažu privatnom IP-mrežom i primjenjuju TCP/IP skup protokola za komunikaciju unutar privatne mreže, analogno privatnim adresama IPv4 iz adresnog prostora 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16.

1.2.2 Višeodredišne adrese

Format višeodredišne adrese predočen je na sl. 1.10.

8 bita	4 bita	4 bita	112 bita
1111 1111	F	S	Group ID

Slika 1.10 – Format višeodredišne adrese (FF00::/8)

¹⁷ IANA – Internet Assigned Number Authority (<http://www.iana.org>)

¹⁸ ICANN – Internet Corporation for Assigned Names and Numbers (<http://www.icann.org>)

Značenja oznaka su sljedeća:

- „1111 1111“ – formatni prefiks koji označava višeodredišnu adresu;
- F (*Flags*) – zastavice ORPT, od kojih je definirana samo zastavica T (*Transient*) koja koristi krajnji desni od 4 bita tog polja;
 - T = 0, trajno dodijeljena višeodredišna adresa koju određuje organizacija IANA.
 - T = 1, privremeno dodijeljena višeodredišna adresa.
- S (*Scope*) – označava doseg adrese, odnosno domenu na koju se odnosi i u koju će se dostavljati paket, npr.:
 - S = 1, doseg čvora, odnosno sučelja čvora (engl. *interface-local scope*), određuje samo jedno sučelje koje se koristi za prijenos višeodredišnih paketa putem *loopback* adrese.
 - S = 2, doseg poveznice (engl. *link-local scope*).
 - S = E, globalni doseg (engl. *global scope*).
- *Group ID* – oznaka grupe unutar definiranog dosega. Veličina polja je 112 bitova. Zbog načina na koji se adrese IPv6 preslikavaju u *Ethernet*-adrese, preporučuje se *Group ID* kreirati od donja 32 bita, a prvih 80 bitova popuniti nulama.

Višeodredišno razašiljanje kod IPv6-mreža radi kao i kod IPv4-mreža. Paketi upućeni na višeodredišnu adresu dostavljaju se svim sučeljima unutar grupe definirane tom adresom. Višeodredišna adresa ne može se koristiti kao izvorišna adresa paketa. Za definiranje svih sučelja i usmjeritelja u dosegu sučelja ili poveznice koriste se posebne višeodredišne adrese:

FF01::1 – svi čvorovi u dosegu sučelja (engl. *interface-local scope all-nodes multicast*)

FF02::1 – svi čvorovi u dosegu poveznice (engl. *link-local scope all-nodes multicast*)

FF01::2 – svi usmjeritelji u dosegu sučelja (engl. *interface-local scope all-routers multicast*)

FF02::2 – svi usmjeritelji u dosegu poveznice (engl. *link-local scope all-routers multicast*)

FF05::2 – svi usmjeritelji u dosegu mjesta (engl. *site-local scope all-routers multicast*)

1.2.3 Adresa bilo kojeg iz skupa odredišta

Adresa *anycast* dodjeljuje se većem broju sučelja, a paketi adresirani na takvu adresu prosljeđuju se do „najbližeg“ sučelja kojem je ta adresa dodijeljena. „Blizina“ sučelja određuje se u smislu metrike usmjeritelja, tj. brojem skokova. Motivacija za uvođenje mogućnosti adresiranja bilo kojeg iz skupa odredišta je odabir najbližeg čvora koji može poslužiti neki zahtjev, npr. najbliži usmjeritelj ili najbliži poslužitelj.

Nema načina da se na temelju formata odredi je li neka adresa *anycast* ili ne, budući da se te adrese dodjeljuju iz adresnog prostora namijenjenog jednoodredišnim adresama i njihov je doseg ekvivalentan dosegu jednoodredišnih adresa na osnovu kojih su dodijeljene. Ako se adresa *anycast* dodijeli višestrukim sučeljima, čvorovi kojima je dodijeljena moraju se eksplicitno konfigurirati kako bi „znali“ da je sučelju dodijeljena adresa *anycast*. Za svaku adresu *anycast* mora postojati odgovarajući unos u tablicama usmjeravanja.

Unaprijed definirana *anycast* adresa je *Subnet-Router anycast* koja se dodjeljuje samo usmjeriteljima, a stvara se od prefiksa podmreže za pojedino sučelje (sl. 1.11).

n bita	128 - n bita
Subnet prefix	0000...0000

Slika 1.11 – Format adrese Subnet-Router anycast

Takva adresa omoguće čvoru izravno komuniciranje s jednim od usmjeritelja u toj podmreži, primjerice pokretnom čvoru kad želi kontaktirati vlastitu domaću mrežu iz udaljene gostujuće mreže. Adresa *Subnet-Router* stvara se tako da se navedu bitovi koji označavaju prefiks podmreže (engl. *subnet prefix*), dok se svi ostali bitovi popune nulama.

Prema specifikaciji, svi usmjeritelji IPv6 moraju podržavati, odnosno odgovarati na tu adresu, za sve podmreže prema kojima imaju sučelja.

1.2.4 Adrese računala i usmjeritelja

Obrazlaganje adresnog prostora zaključit će se pregledom svih vlastitih adresa koje moraju moći prepoznati svaki čvor – računalo i svaki usmjeritelj (sl. 1.12). Svaki čvor treba moći prepoznati sljedeće adrese kao vlastite:

- lokalne adrese na razini poveznice za svako od svojih sučelja;
- sve jednoodredišne adrese dodijeljene nekom od svojih sučelja;
- povratnu adresu;
- višeodredišnu adresu svih čvorova u dosegu sučelja i u dosegu poveznice;
- *Solicited-Node multicast* adrese za svaku svoju *unicast* i *anycast* adresu, za potrebe protokola NDP kod dobivanja adresa na sloju podatkovne poveznice;
- višeodredišne adrese svih skupina kojima čvor pripada.

Svaki usmjeritelj treba dodatno, uz sve adrese obvezne za čvor, prepoznati kao vlastite i sljedeće adrese:

- *Subnet-Router anycast* i druge *anycast* adrese za sučelja za koja je konfiguriran kao usmjeritelj, kojima se omoguće komunikacija s usmjeriteljem iz udaljenih mreža;
- *All Routers multicast* adrese namijenjene svim usmjeriteljima u dosegu.

1.3 Upravljački protokoli za IPv6

Slično kao protokolu IPv4, tako su i protokolu IPv6 pridruženi upravljački protokoli mrežnog sloja koji obavljaju funkcije razmjene upravljačkih poruka, komunikacije u skupini i dinamičkog konfiguriranja računala. Upravljački protokoli za IPv4 su:

- ICMP (*Internet Control Message Protocol*)¹⁹,
- IGMP (*Internet Group Message Protocol*)²⁰,

¹⁹ „Internet Control Message Protocol”, RFC 792, IETF, rujan 1981.

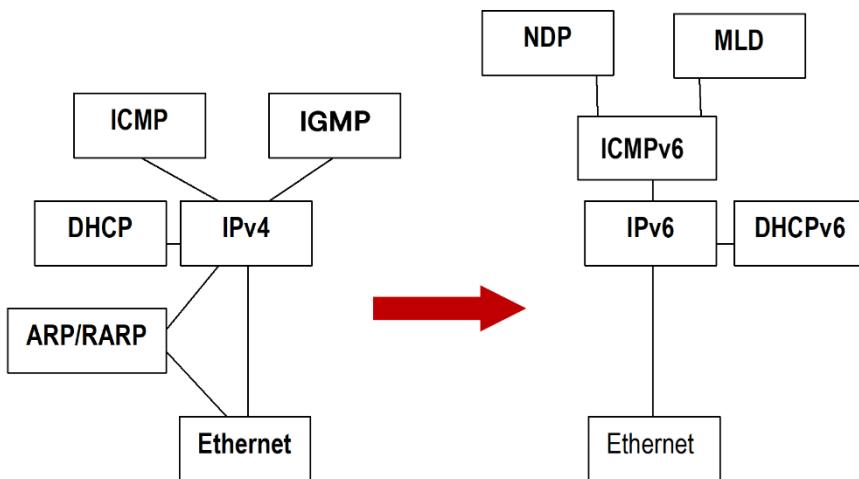
²⁰ „Internet Group Message Protocol, Version 3”, RFC 3376, IETF, listopad 2002.

- DHCP (*Dynamic Host Configuration Protocol*)²¹ te
- ARP (*Address Resolution Protocol*)²² i RARP (*Reverse Address Resolution Protocol*)²³.

kao što prikazuje sl. 1.12.

Istovrsne i proširene funkcije za IPv6 obavljaju protokoli:

- ICMPv6 (*Internet Control Message Protocol version 6*) koji prenosi poruke dva protokola:
 - NDP (*Neighbor Discovery Protocol*) s potporom za lociranje susjednih čvorova, tj. usmjeritelja, računala i poslužitelja na istoj poveznici te pribavljanje konfiguracijskih podataka,
 - MLD (*Multicast Listener Discovery*) s potporom za komunikaciju u skupini i višeodredišno razašiljanje te
- DHCPv6 (*Dynamic Host Configuration Protocol version 6*) kojim se čvorovima omogućuje konfiguracija putem poslužitelja DHCPv6.



Slika 1.12 – Upravljački protokoli za IPv4 i IPv6

U nastavku se neće razrađivati protokol MLD²⁴, jer se u ovoj knjizi ne razmatra višeodredišno razašiljanje, već samo protokoli ICMPv6, NDP i DHCPv6.

1.3.1 Protokol ICMPv6

Kao što protokol ICMP služi za razmjenu upravljačkih poruka kod IPv4, kao što su dojave o pogrešci (povratna informacija pošiljatelju o nekom problemu u mreži) ili zahtjevi za informacijom (traži se informacija vezana za stanje u mreži), tako i protokol ICMPv6²⁵ to

²¹ „Dynamic Host Configuration Protocol”, RFC 2131, IETF, ožujak 1997.

²² „An Ethernet Address Resolution Protocol or Converting Network Protocol Address to 48. bit Ethernet Address for Transmission over Ethernet Hardware”, RFC 826, IETF, studeni 1982.

²³ „A Reverse Address Resolution Protocol”, RFC 903, IETF, lipanj 1984.

²⁴ „Multicast Listener Discovery Version 2 (MLDv2) for IPv6”, RFC 3810, IETF, lipanj 2004.

²⁵ „Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)”, RFC 4443, IETF, ožujak 2006.

obavlja za IPv6. Prigodom definiranja IPv6, specificiran je i ICMPv6. Razvijen je na iskustvima protokola ICMP za IPv4, ali oni nisu kompatibilni, niti po funkcionalnosti ni po formatu poruka. Funkcije koje se nisu koristile u protokolu ICMP su izbačene, a dodane su upravljačke funkcije vezane uz višeodredišno razašiljanje koje su bile sadržane u protokolu IGMP te uvedene nove funkcije vezane uz otkrivanje susjednih čvorova i konfiguriranje adresa.

Poruke protokola ICMPv6 prenose se IPv6-datagramom s vrijednošću polja sljedećeg zaglavlja 58. Te poruke, uz oznaku vrste poruke i kôd, imaju zaštitnu sumu (16 bita), čime se izbjegava njihova pogrešna interpretacija koja bi mogla izazvati neželjene reakcije i stvoriti dodatne probleme u mreži (sl. 1.13). Ovo je primjer kako se, izvan zaglavlja protokola IPv6, ugrađuje zaštitno kodiranje za slučajeve kad je to posebno važno!

vrsta poruke	kod	zaštitna suma
Tijelo poruke		

Slika 1.13 – Format poruke ICMPv6

Vrsta poruke (8 bita) označava specifičnu poruku, a kôdom (8 bita) se može dodatno specificirati njen značenje. ICMPv6 rukuje sljedećim porukama:

- poruke o pogreškama (engl. *error messages*),
- informativne poruke (engl. *informational messages*) i
- specifične poruke vezane uz druge protokole, kao na primjer NDP i MLD.

Poruke o pogreškama prema izvorišnom čvoru šalje čvor koji izbacuje paket iz mreže. Četiri su vrste takvih poruka koje se šalju u sljedećim situacijama, a paket odbacuje:

- 1 odredište nedostupno (engl. *Destination Unreachable*), jer nema puta do odredišta, administrativno je zabranjena komunikacija s odredištem, nedostupna je adresa ili vrata;
- 2 paket prevelik (engl. *Packet Too Big*);
- 3 isteklo vrijeme (engl. *Time Exceeded*), paket predugo putuje mrežom tako da je istekao dozvoljeni broj skokova, ili dopušteno vrijeme;
- 4 problem s parametrom (engl. *Parameter Problem*), jer vrsta zaglavlja ili dodatnog zaglavlja nije poznata, ili je vrijednost polja u zaglavlju nepoznata.

Programski alat *ping* kojim se omogućuje provjera dostupnosti odredišta riješen je na način poznat iz IPv4, s porukama:

128 *Echo Request* i 129 *Echo Reply*.

Protokol ICMPv6 primjenjuje se za određivanje maksimalne transmisijske jedinice, odnosno MTU-puta, od izvora do odredišta. MTU-puta odgovara najvećem paketu koji se može prenijeti mrežom, a određuje ga poveznica s najmanjim MTU-om na putu²⁶.

Izvor može otkriti MTU-puta tako da šalje paket maksimalne veličine prema MTU vlastite mreže. Ako takav paket prođe do odredišta, fragmentiranje nije potrebno. Ako paket dođe do nekog usmjeritelja koji ne može proslijediti tako veliki paket, on će ga odbaciti i izvor obavijestiti porukom ICMPv6 da je paket prevelik i navesti koliko manji paket može proslijediti. Izvor će tad poslati manji paket i postupak smanjivanja ponavljati tako dugo dok paket ne stigne do odredišta, čime će odrediti MTU-puta i na takvu veličinu fragmentirati pakete.

1.3.2 Protokol NDP

Protokol NDP²⁷ je upravljački protokol koji je preuzeo dio funkcija protokola ICMP i ARP iz IPv4 i uveo nove kojima se omogućuje jednostavnije otkrivanje usmjeritelja, olakšava administriranje mrežom i omogućuje autokonfiguraciju adresa. Pojam „susjeda“ odnosi se na čvorove, usmjeritelje ili računala, koji se nalaze na istoj poveznici ili u istoj (pod)mreži.

Primjer specifičnih poruka protokola NDP su sljedeće vrste poruka:

- 133 Router Solicitation,
- 134 Router Advertisement,
- 135 Neighbor Solicitation,
- 136 Neighbor Advertisement
- 137 Redirect Message.

Da bi se pospješilo otkrivanje usmjeritelja (engl. *Router Discovery*), tj. pronalaženje nadležnog usmjeritelja, čvor po aktiviranju može pokrenuti funkciju pobuđivanja usmjeritelja (engl. *Router Solicitation*) istoimenom porukom. Po prijemu takve poruke, usmjeritelj će se odmah odazvati porukom oglašavanja (engl. *Router Advertisement*), umjesto po definiranom vremenskom rasporedu oglašavanja. Ovakvim otkrivanjem usmjeritelja svako računalo može jednostavno locirati usmjeritelja u svojoj mreži. Iz poruke *Router Advertisement* može se saznati prefiks poveznice i drugi parametri, primjerice MTU, način autokonfiguracije adrese i drugo.

Usmjeravanje se dodatno može pospješiti tako da usmjeritelj izvijesti čvor porukom preusmjeravanja (engl. *Redirect Message*) o najboljem prvom skoku za odabranu odredište, odnosno omogući preusmjeravanje paketa već na početku puta.

Druga funkcija odnosi se na pobuđivanje susjednog čvora (engl. *Neighbour Solicitation*). Istoimena poruka omogućuje određivanje adrese sloja podatkovne poveznice susjednog čvora (čvora na istoj poveznici), otkrivanje dvostrukе adrese, kao i provjeru dostupnosti tog čvora putem prethodno zapamćene adrese. Po prijemu takve poruke, čvor će se odmah odazvati porukom oglašavanja (engl. *Neighbour Advertisement*). Isto tako, čvor može

²⁶ „Path MTU Discovery for IPv6“, RFC 1981, IETF, kolovoz 1996.

²⁷ „Neighbor Discovery in IPv6“, RFC 4861, IETF, rujan 2007.

poslati poruku oglašavanja nakon promjene adrese u sloju podatkovne poveznice kojom o tome izvještava susjedne čvorove.

Primjenom navedenih poruka protokol NDP omogućuje rješavanje problema usmjeravanja i adresiranja kao što su:

- otkrivanje usmjeritelja (engl. *router discovery*);
- otkrivanje prefiksa (engl. *prefix discovery*): računalo ustanovljava kojoj mreži pripada;
- otkrivanje parametara (engl. *parameter discovery*): računalo ustanovljava parametre lokalne mreže, kao što je MTU, ili parametre usmjeritelja, npr. ograničenje skokova;
- autokonfiguracija adrese (engl. *address autoconfiguration*): automatska konfiguracija adrese računala;
- rezolucija adrese (engl. *address resolution*): određivanje adrese susjednog čvora na lokalnoj povezniци;
- određivanje sljedećeg skoka (engl. *next-hop determination*): usmjerava li se izravno na odredište ili putem usmjeritelja, ako čvorovi nisu u istoj lokalnoj mreži;
- nedostupnost susjednog čvora (engl. *neighbour unreachability detection*): utvrđivanje je li susjedni čvor (usmjeritelj ili računalo) dostupan;
- prepoznavanje dvostrukе adrese (engl. *duplicate address detection*): ustanavljanje koristi li drugi čvor odabranu adresu.

Navedene funkcije mogu se grupirati u dvije skupine, prve četiri funkcije na relaciji računalo-usmjeritelj (engl. *host-router*), a druge četiri funkcije na relaciji računalo-računalo (engl. *host-host*).

Protokol NDP može biti izvor potencijalne sigurnosne prijetnje: ako zlonamjerni napadač uspije preuzeti identitet čvora, mogao bi saznati informacije o drugim čvorovima i usmjeriteljima na istoj povezniци, odnosno istom djelu mreže.

1.3.3 Protokol DHCPv6 i autokonfiguracija s pomoću poslužitelja

Protokol DHCPv6²⁸ unaprijeđeni je protokol DHCP sa širokom primjenom u IP-mrežama u kojima se većina čvorova – DHCPv6-klijenata konfigurira upravo s tim protokolom putem DHCPv6-poslužitelja. Pritom se IP-adrese mogu dodjeliti statički (stalna dodjela iste adrese) ili dinamički (dodjela jedne od raspoloživih adresa na određeno vrijeme). Uz to, protokolom DHCPv6 omogućene su i druge konfiguracijske informacije, primjerice one vezane uz DNS. Kod dodjele adrese, DHCP-poslužitelj pohranjuje i održava informaciju o stanju čvora (engl. *stateful autoconfiguration*).

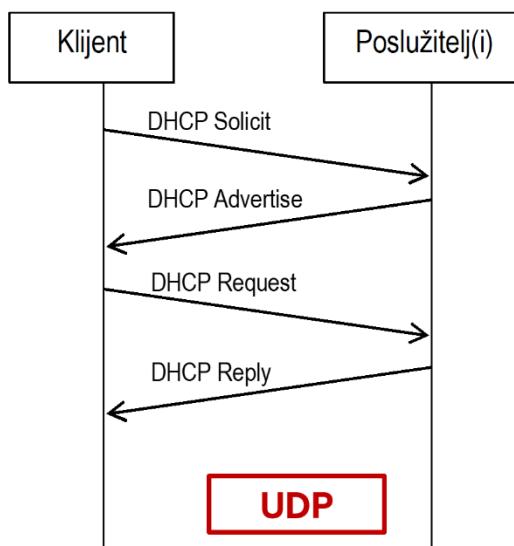
Autokonfiguraciju zasnovanu na stanju provodi čvor – klijent koji zahtijeva uslugu DHCPv6-poslužitelja, pri čemu klijent i poslužitelj komuniciraju transportnim protokolom UDP:

- DHCPv6-klijent koji nema IPv6-adresu šalje višeodredišnom adresom na razini poveznice zahtjev svim susjednim poslužiteljima i njihovim posrednicima (engl. *relay*) koji su članovi iste višeodredišne skupine.

²⁸ „Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC 3315, IETF, srpanj 2003.

- Posrednik prosljeđuje zahtjev višeodredišnom adresom na razini poveznice svim poslužiteljima koji su članovi iste višeodredišne skupine, a čije jednoodredišne adrese mu nisu poznate.
- DHCPv6-poslužitelj odgovorom na zahtjev snabdijeva klijenta IPv6-adresom i konfiguracijskim parametrima.

Primjer razmjene poruka je na sl. 1.14. Da bi locirao poslužitelja, klijent šalje poruku *Solicit* kojom traži DHCPv6-poslužitelja ili posrednika. U ovom primjeru oglašavaju se bez posredovanja jedan ili više poslužitelja porukom *Advertise*. Klijent odabire jednog od poslužitelja koji su se oglasili i zahtijeva konfiguracijske parametre porukom *Request*. Poslužitelj dostavlja klijentu adresu IPv6 i druge zahtijevane parametre (npr. vrijeme valjanosti, adresu poslužitelja DNS-a) porukom *Reply*. Osim za početnu dodjelu IP-adrese, moguća je autokonfiguracija u drugim okolnostima (npr. obnavljanje dodijeljene adrese po isteku vremena valjanosti), kao i drugi ishodi autokonfiguracije (npr. odbijanje u slučaju kad se adresa već koristi).



Slika 1.14 – Autokonfiguracija s četiri poruke zasnovana na stanju čvora

1.3.4 Samostalna autokonfiguracija adrese

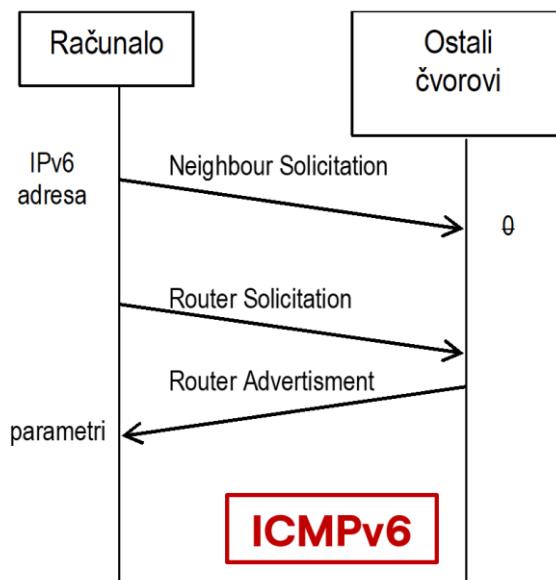
Autokonfiguraciju adrese bez poznavanja stanja (engl. *stateless autoconfiguration*) provodi čvor samostalno, što je velika prednost u odnosu na IPv4 i postupke koji zahtijevaju ručnu konfiguraciju i sudjelovanje mrežnog administratora, ili posebne poslužiteljske sustave, kao DHCP. Ručna konfiguracija preostaje kao rješenje samo u slučaju dvostrukih adresa. Zbog mogućnosti autokonfiguracije adrese bez poznavanja stanja, u male mreže nije potrebno uvoditi konfiguracijske poslužitelje, a u velikima se može izbjegći konfiguracija zasnovana na stanju čvora koja zahtijeva složeno održavanje. Olakšana je i promjena adresa dodijeljenih čvorovima, odnosno renumeracija. Nakon što čvor samostalno konfigurira adresu, za ostale parametre, npr. DNS, može se koristiti DHCP bez poznavanja stanja.^{29,30}

²⁹ „IPv6 Stateless Address Autoconfiguration”, RFC 4863, IETF, rujan 2007.

³⁰ „Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6”, RFC 3736, IETF, travanj 2004.

Postupkom autokonfiguracije čvor stvara lokalnu adresu na razini poveznice (engl. *link-local address*) i globalnu adresu te provodi provjeru jedinstvenosti adresa na poveznici. Autokonfiguracija je zasnovana na MAC-adresi predočenoj EUI-64 bitnim brojem izvedenim iz eternetske 48 bitne adrese, a njena temeljna je postavka jedinstvenost EUI-64 adrese čvora, odnosno sučelja, u sloju podatkovne poveznice. Postupak prikazan na sl. 1.15 teče ovako:

- Čvor prvo stvara lokalnu adresu na razini poveznice prigodom inicijalizacije mrežnog sučelja, iz MAC-adrese predočene EUI-64 bitnim brojem.
- Čvor provjerava jedinstvenost te adrese primjenom protokola NDP slanjem poruke *Neighbour Solicitation*. Ako već postoji čvor s istom adresom, on će se odazvati i automatska autokonfiguracija se prekida, a moguće je nastaviti samo s ručnom konfiguracijom. Ako je adresa jedinstvena, postupak se nastavlja, jer čvor može komunicirati sa svima drugima na istoj poveznici.
- Čvor potom određuje informaciju potrebnu za autokonfiguraciju globalne adrese. Pribavlja je protokolom NDP od usmjeritelja, osluškuje poruku *Router Advertisement*, ili odmah šalje višeodredišnu poruku *Router Solicitation* kako bi potaknuo usmjeritelja da je pošalje.
- Usmjeritelj oglašava kakva je konfiguracija moguća, zasnovana na stanju ili bez poznavanja stanja, i koji se konfiguracijski parametri mogu pribaviti kojim načinom konfiguracije, npr. IP-adresa bez poznavanja stanja, a mrežni parametri zasnovani na stanju. Ako se usmjeritelj ne oglašava, preostaje samo autokonfiguracija zasnovana na stanju, putem poslužitelja DHCPv6.



Slika 1.15 – Samostalna autokonfiguracija adrese

Autokonfiguracija bez poznavanja stanja predmet je istraživanja i rasprave upravo zbog jedinstvenosti EUI-64 adrese čvora: kako je „vlasnika“ adrese lako moguće identificirati, tako da se javlja problem privatnosti!

1.4 Uvođenje protokola IPv6 u mrežu i postupni prijelaz s protokola IPv4 na IPv6

Protokoli IPv4 i IPv6 nisu međusobno kompatibilni. Protokol IPv6 postupno se uvodi u mrežu, tako da je potrebno planirati prijelaz s protokola IPv4 na IPv6. Koncepcijski, polazište su temeljne postavke Interneta:

- globalni adresni prostor definiran je različitim adresnim arhitekturama protokola IPv4 i IPv6 te
- protokolni stog TCP/IP izveden je u dvije inačice, TCP/IPv4 i TCP/IPv6.

U razdoblju uvođenja IPv6 i postupnog prijelaza s protokola IPv4 na IPv6 u mreži koegzistiraju obje inačice protokola, uz heterogenost čvorova (računala i usmjeritelja), od kojih neki podržavaju samo IPv4, a neki IPv4 i IPv6. Očekuje se da potpuni prelazak na IPv6 neće biti brz, tako da su za komunikaciju IPv6-čvorova preko infrastrukture IPv4 razvijeni posebni tranzicijski mehanizmi.

Isto tako, sustav imenovanja domena, DNS, dograđuje se za IPv6 tako da obuhvaća sljedeće zapise:

- A zapis za pretvorbu simboličko ime → IPv4-adresa (za IPv4-čvor i IPv6/IPv4-čvor)
- AAAA zapis za pretvorbu simboličko ime → IPv6-adresa (za IPv6-čvor i IPv6/IPv4-čvor)
- PTR zapis za pretvorbu IPv4-adresa → simboličko ime (za IPv4-čvor i IPv6/IPv4-čvor)
- PTR zapis za pretvorbu IPv6-adresa → simboličko ime (za IPv6-čvor i IPv6/IPv4-čvor).

1.4.1 IPv6-adrese s uključenim IPv4-adresama

Kako bi se olakšao prijelaz s protokola IPv4 na IPv6, specificirane su posebne IPv6-adrese za primjenu u prijelaznom razdoblju:

- IPv4 preslikane IPv6-adrese (engl. *IPv4 mapped IPv6 addresses*) te
- adrese „6to4“ (engl. *6to4 addresses*).

IPv4 preslikana IPv6-adresa (:FFFF:0:0/96) koristi se isključivo za interni prikaz čvora koji podržava samo IPv4, čvoru koji podržava samo IPv6. Ta se adresa nikad ne koristi kao izvođena ili odredišna adresa IPv6-paketa. Preslikana se IPv4 adresa čvora a.b.c.d. interna zapisuje ovako:

0:0:0:0:FFFF:a.b.c.d ili ::FFFF:a.b.c.d.

Drugi oblik adresa je „6to4“ formata 2002::/16 koja se koristi za komunikaciju između dva IPv6-čvora koji podržavaju funkcionalnost 6to4, a komuniciraju automatskim tuneliranjem putem mrežne infrastrukture s IPv4³¹. Čvor s funkcionalnosti 6to4 može tako komunicirati i s „običnim“ IPv6-čvorom, a može omogućiti komunikaciju mreže čiji je on rubni čvor („otok 6to4“) putem IPv4 s drugim IPv6-čvorom ili otokom.

³¹ „Connection of IPv6 Domains via IPv4 Clouds“, RFC 3056, IETF, veljača 2001.

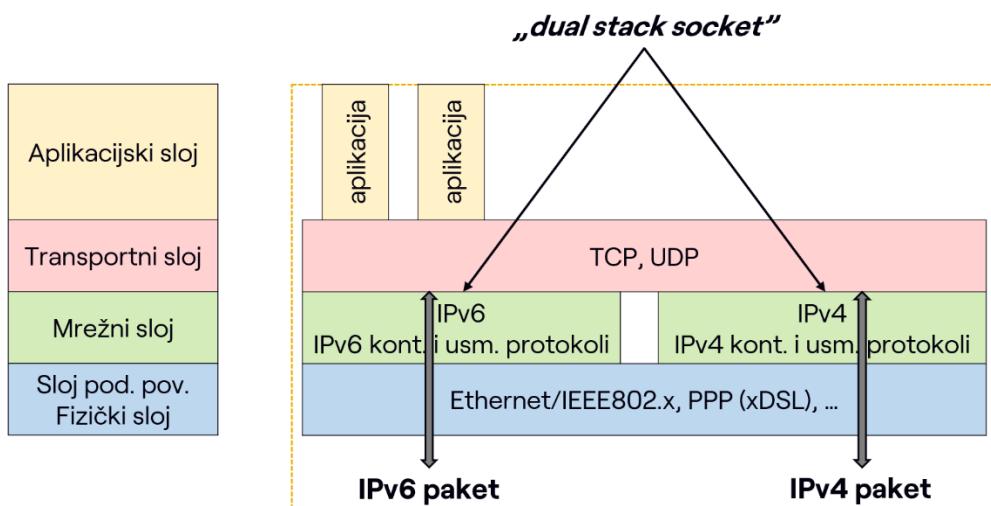
1.4.2 Tranzicijski mehanizmi

Osnovni tranzicijski mehanizmi³² uključuju dva moguća rješenja:

- dvostruki IP-sloj, odnosno dvostruki stog (engl. *dual IP layer, dual stack*), kojim se opremanju čvorovi, što je prikladno posebice za računala – krajnje sustave te
- tuneliranje (engl. *tunneling*) kojim se povezuju mreže s različitim protokolima.

Prevođenje protokola IPv4 u IPv6 je napušteno kao rješenje, zbog različitih tehničkih i operativnih problema.

Dvostruki IP-sloj obilježje je tzv. IPv6/IPv4-čvora. To je IPv6-čvor koji sadrži i izvedbu protokola IPv4 kojom postiže kompatibilnost unatrag (sl. 1.16). Takav čvor razmjenjuje ili IPv6-pakete s mrežnim protokolom IPv6 ili IPv4-pakete s mrežnim protokolom IPv4. Oba protokolna stoga su potpuna, tj. sadrže sve protokole od mrežnog do aplikacijskog sloja, iznad sloja podatkovne poveznice i fizičkog sloja putem kojih pristupaju Internetu ili bilo kojoj IP-mreži. U ovom su primjeru navedeni lokalna mreža (jedna od izvedbi IEEE 802.x) i širokopojasni pristup jednom od izvedbi digitalne korisničke petlje (xDSL) primjenom protokola PPP (*Point to Point Protocol*)³³. U mrežnom sloju izvedeni su i svi potrebni upravljački i usmjeravajući protokoli. Treba napomenuti da kod dvostrukog IP-sloja aplikacije mogu tražiti i od DNS-a dobiti samo jednu ili obje vrste IP-adresa.

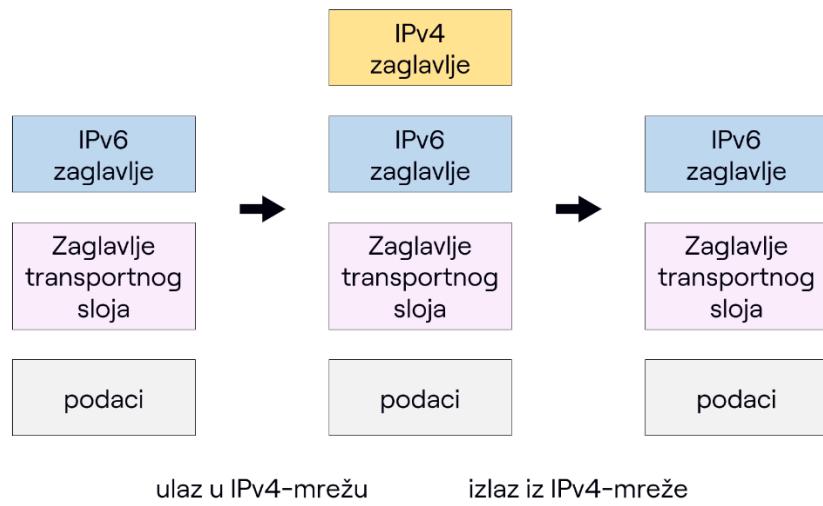


Slika 1.16 – IPv4/IPv6-čvor

Postojeća IPv4 infrastruktura se može koristiti za prenošenje IPv6 prometa tuneliranjem. Na sl. 1.17 prikazano je osnovno načelo tuneliranja IPv6-paketa kroz IPv4-mrežu. To je postupak dodavanja IPv4-zaglavљa na IPv6-paket (omatanje – enkapsulacija paketa) na ulaznom usmjeritelju u IPv4-mrežu. IPv6-paket tako postaje IPv4-paket koji se usmjerava do izlaznog IPv4-usmjeritelja. Na tome usmjeritelju prema IPv6-mreži odbacuje se IPv4-zaglavље (razmatranje – dekapsulacija paketa) i paket prosljeđuje odredištu putem infrastrukture IPv6.

³² „Basic Transition Mechanisms for IPv6 Hosts and Routers”, RFC 4213, IETF, listopad 2005.

³³ „The Point to Point Protocol (PPP)”, RFC 1661, IETF, srpanj 1994.

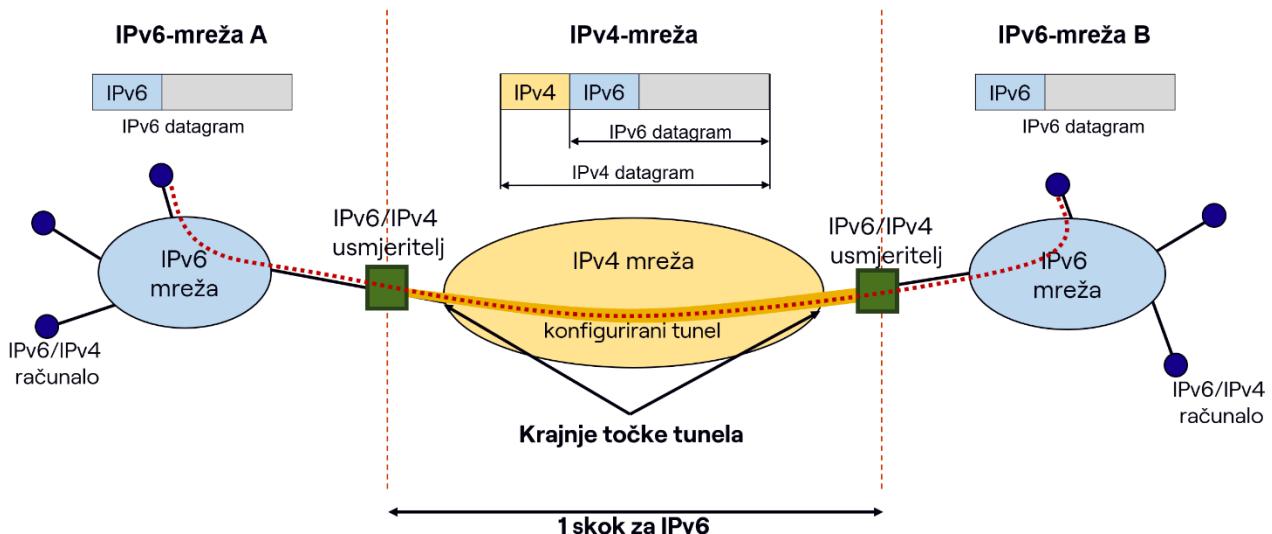


Slika 1.17 – Tuneliranje IPv6-paketa kroz IPv4-mrežu

Tunel može biti konfiguriran ovako:

- ručno, tj. njegov početak i kraj definira administrator mreže (konfiguirani tunel) ili
- automatski, ako usmjeritelj raspolaže jedinstvenim globalnim IPv4 i IPv6 adresama odredišta, ili ih može odrediti (automatski tunel).

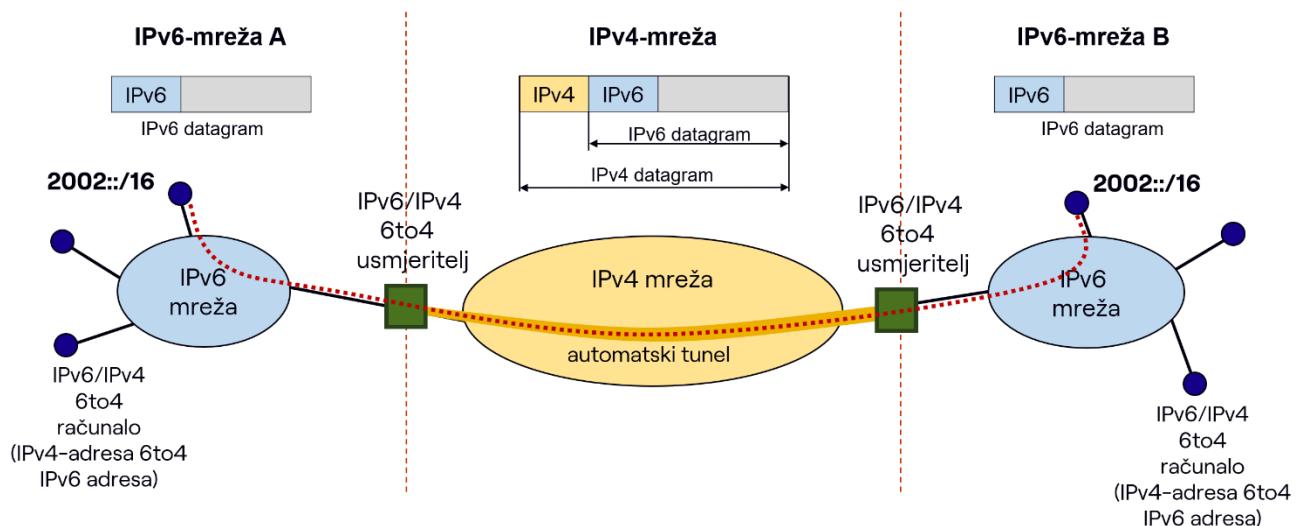
Na sl. 1.18 je primjer tuneliranja na relaciji usmjeritelj-usmjeritelj (engl. *router-to-router*), pri čemu usmjeritelji raspolažu dvostrukim IP-slojem. Takav tunel koji se konfiguriра ručno omogućuje komunikaciju bilo kojeg IPv6-čvora u mreži A s bilo kojim IPv6-čvorom u mreži B.



Slika 1.18 – Tuneliranje IPv6-paketa kroz IPv4-mrežu na relaciji između dva usmjeritelja

Promotrimo na istom primjeru razliku prema automatskom tuneliranju koje se zasniva na adresama 6to4 (sl. 1.19). U tom slučaju čvorovi s funkcionalnošću 6to4, u ovom primjeru usmjeritelji, raspolažu s dvije jedinstvene globalne adrese, IPv4-adresom a.b.c.d i IPv6-adresom 2002::a.b.c.d. Tunel se stvara automatski tako da usmjeritelj na ulazu u IPv4-mrežu omata IPv6-paket u IPv4-paket i šalje ga u IPv4 mrežu, na čijem se izlaznom usmjeritelju

IPv4-paket razmata i dalje isporučuje IPv6-paket. Kako čvorovi raspolažu s obje jedinstvene globalne adrese, a što se prepoznaće po prefiku adresе 6to4, tunel se konfigurira automatski.



Slika 1.19 – Automatsko tuneliranje zasnovano na adresama 6to4

Posebne organizacije pružaju usluge tunelskog brokera (engl. *tunnel broker*) i omogućuju tuneliranje IPv6-datagrama putem IPv4 infrastrukture.³⁴ Uz 6to4, poznate tehnike automatskog tuneliranja su Teredo³⁵ i ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*)³⁶.

Osim tuneliranja na relaciji usmjeritelj–usmjeritelj koja se nalazi na nekoj unutarnjoj dionici puta između izvora i odredišta, moguće su i druge relacije:

- računalo–usmjeritelj (engl. *host-to-router*): računalo s dvostrukim IP-slojem šalje podatke usmjeritelju koji je dostupan samo preko IPv4 infrastrukture. Tunel se nalazi na početnoj dionici puta paketa i prostire se do tog usmjeritelja.
- računalo–računalo (engl. *host-to-host*): računala s dvostrukim IP-slojem izmjenjuju međusobno pakete preko IPv4 infrastrukture. Tunel se ovdje prostire na cijelom putu paketa, od izvora do odredišta.
- usmjeritelj–računalo (engl. *router-to-host*): usmjeritelj s dvostrukim IP-slojem tunelira IPv6-pakete prema konačnom odredištu koje također ima dvostruki IP-sloj. Tunel se nalazi na zadnjoj dionici puta paketa.

Tehnike tuneliranja koje se pritom primjenjuju, konfiguiriranog ili automatskog, razlikuju se po načinu kako čvor koji omata paket određuje adresu čvora na kraju tunela.

Za tuneliranje na dionici računalo–usmjeritelj, odredište tunela je izlazni usmjeritelj koji će razmotati paket i proslijediti ga konačnom IPv6-odredištu. Adresa završnog čvora tunela

³⁴ „IPv6 Tunnel Broker“, RFC 3053, IETF, siječanj 2001.

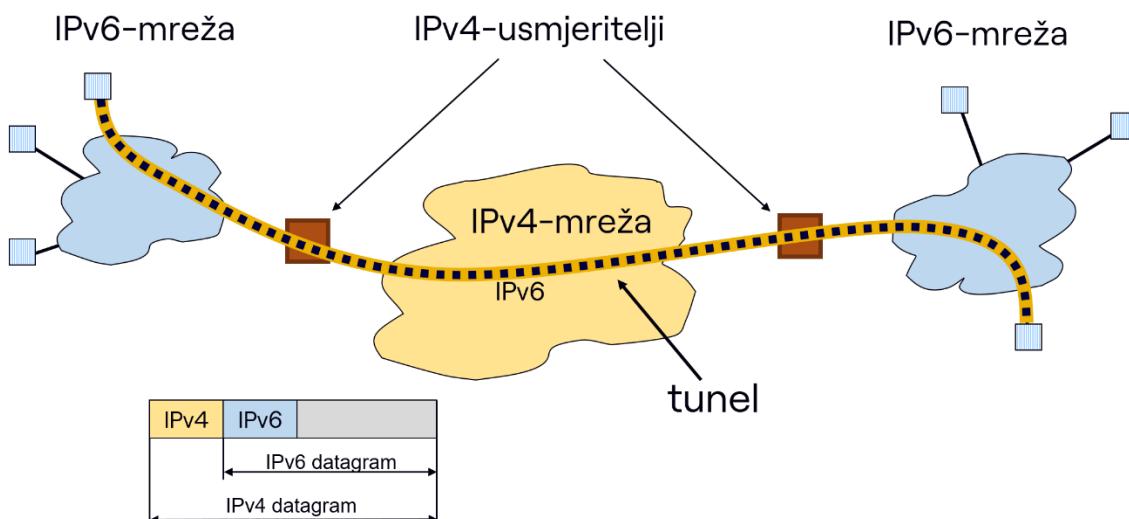
³⁵ „Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)“, RFC 4380, IETF, veljača 2006.

³⁶ „Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)“, RFC 5214, IETF, ožujek 2008.

mora biti konfiguirirana na računalu – početnom čvoru tunela, kao i kod tuneliranja na relaciji usmjeritelj–usmjeritelj. U preostala dva slučaja tuneliranja na dionicama računalo–računalo i usmjeritelj računalo, završni čvor tunela je ujedno i odredište IPv6 paketa, tj. IPv4-adresa i IPv6-adresa zaglavlja pokazuju na isti čvor.

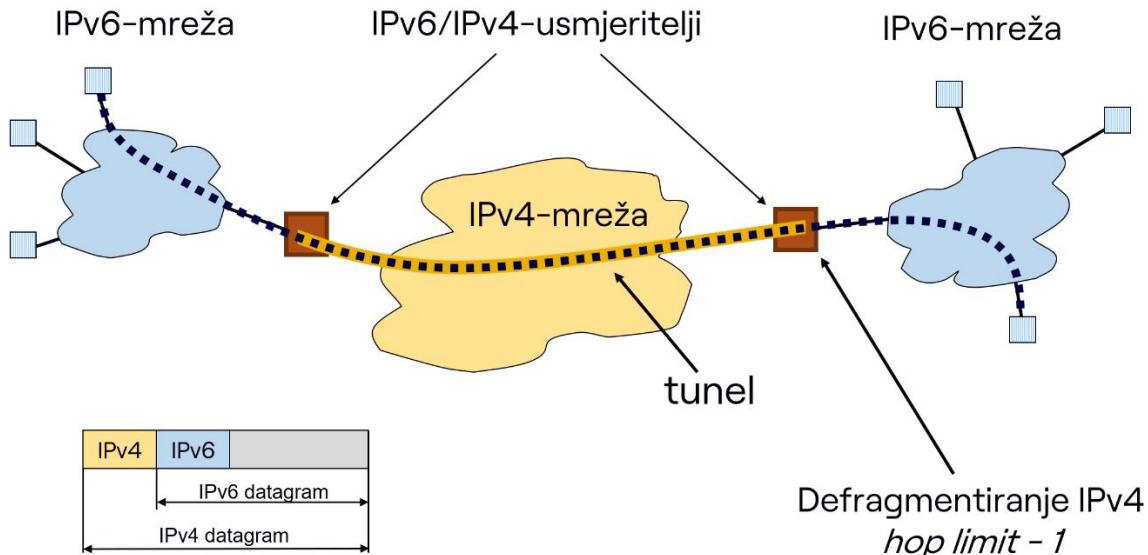
Slika 1.20 prikazuje situaciju u kojoj dva računala s dvostrukim IP-slojem na IPv6-mrežama komuniciraju preko IPv4-mreže posredstvom IPv4-usmjeritelja.

IPv6-paketi omataju se u IPv4-pakete i prenose do druge IPv6-mreže putem IPv4-mreže s usmjeriteljima koji ne podržavaju IPv6. Kako je IPv6 uveden samo na izvorišnom i odredišnom računalu i njihovim mrežama, tunel se uspostavlja na čitavom putu, na relaciji računalo–računalo. To bi bilo rješenje i za povezivanje pojedinačnih računala s protokolom IPv6 putem IPv4-mreže.



Slika 1.20 – Tuneliranje IPv6-paketa kroz IPv4-mrežu na relaciji između dva računala

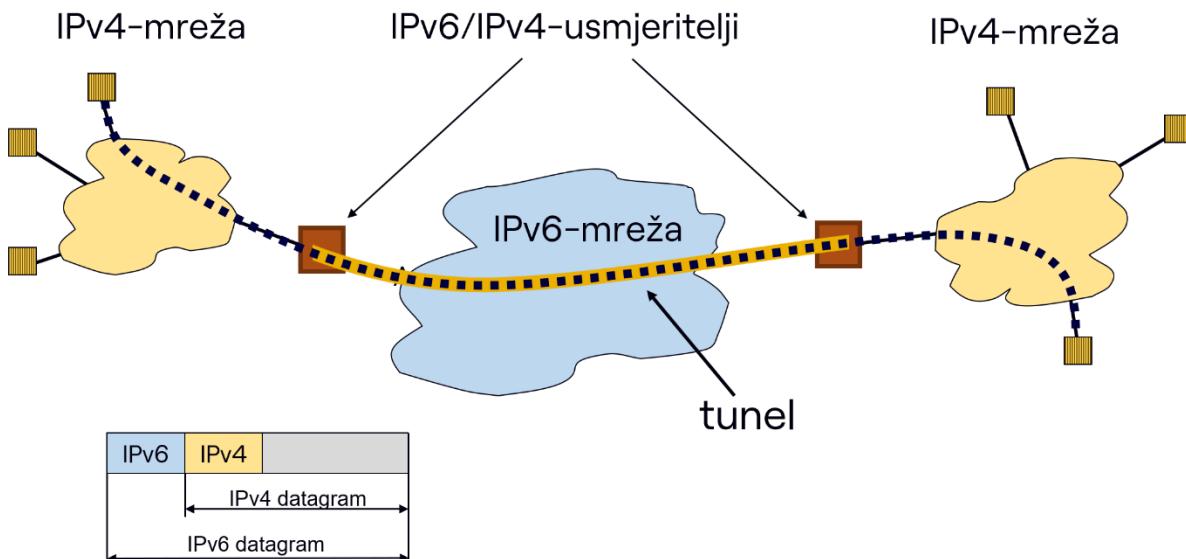
Ako usmjeritelji na rubu IPv4-mreže nisu „stari”, tj. IPv4-usmjeritelji, već imaju dvostruki IP-sloj, bolje je rješenje s tunelom na relaciji usmjeritelj–usmjeritelj, kakvo je već prikazano na sl. 1.19. Razmotrimo detaljnije zadaće čvora na kraju tunela (sl. 1.21). Čvor na kraju tunela provjerava izvorišnu IPv4-adresu i odbacuje paket ako je ona neispravna (npr. *multicast*, *loopback* ili nedefinirana adresa). Ako je izvorišna IPv4-adresa ispravna, eventualni fragmenti IPv4-datagrama se pospajaju, tj. datagram se defragmentira, nakon čega se odbacuje IPv4-zaglavje i razmata IPv6-paket. Provjerava se izvorišna IPv6-adresa i paket odbacuje ako je neispravna. Za IPv6-paket tunel predstavlja samo jedan skok, tako se polje ograničenja skoka smanjuje za 1 po izlasku iz tunela i paket proslijedi dalje prema odredišnom čvoru u IPv6-mreži.



Slika 1.21 – Tuneliranje IPv6-paketa kroz IPv4-mrežu na relaciji između dva računala

Eventualne ICMP-poruke pogreške unutar tunela šalju se čvoru na početku tunela, budući da je on izvor novonastalog IPv4-paketa. Ako je u ICMP-poruci sadržano dovoljno podataka o izvornom IPv6-paketu, taj će čvor generirati ICMPv6-poruku i poslati je izvornom pošiljatelju paketa.

Slika 1.22 prikazuje situaciju kad većina mreža koristiti protokol IPv6, a preostale su mreže-otoci s protokolom IPv4. U takvoj situaciji, računalo s IPv4 odašat će pakete do usmjeritelja s dvostrukim IP-slojem, te će on na IPv4-paket dodati IPv6-zaglavljje i tako omotan paket usmjeriti tunelom prema drugoj IPv4-mreži. Usmjeritelj na drugom kraju IPv6-mreže će odbaciti IPv6-zaglavljje, a IPv4-paket proslijediti prema odredišnom računalu. Ovdje je uspostavljen tunel drukčije vrste, koji IPv4 omata u IPv6.



Slika 1.22 – Tuneliranje IPv4-paketa kroz IPv6-mrežu na relaciji između dva usmjeritelja

1.5 Zadaci

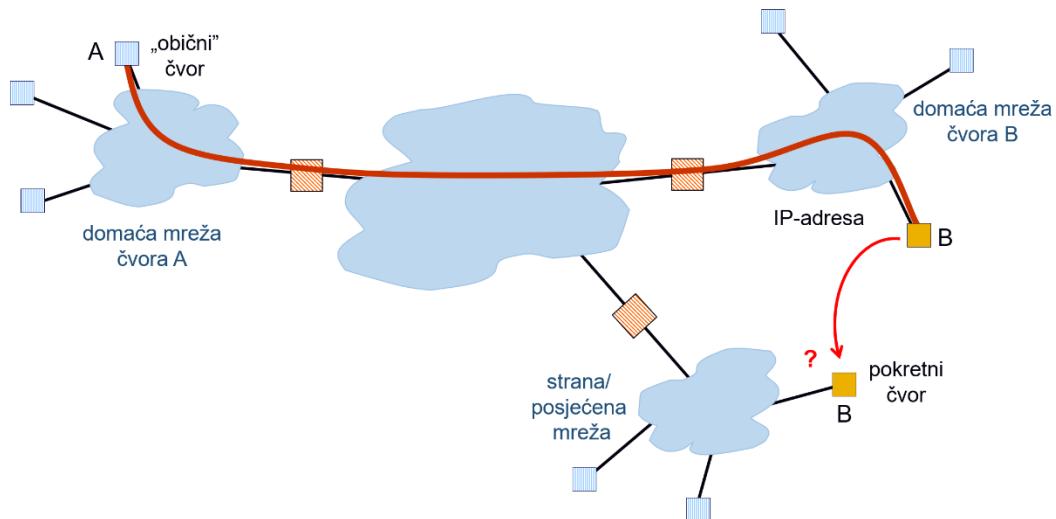
1. Usporedite protokole IPv4 i IPv6 s obzirom na funkcionalnost i performanse.
2. Što se može dogoditi IPv6-datagramu ako tijekom prijenosa smetnje izazovu pogrešku jednog bita u odredišnoj adresi?
3. Koja dodatna zaglavila ima IPv6-datagram kojim se veoma veliki paket ($> 2^{16}$ okteta) usmjerava do odredišta po točno definiranom putu? Kakav je redoslijed zaglavila u takvom datagramu?
4. Kako se provodi fragmentacija za protokol IPv6 i kako se može ustanoviti duljina fragmenata?
5. Koja su polja sadržana u formatu jednoodredišne adrese protokola IPv6?
6. Navedite i objasnite razloge zbog kojih protokol IPv6 omogućuje učinkovitije usmjeravanje u mreži u odnosu na sadašnje stanje koje je proizašlo iz načina adresiranja i usmjeravanja te dodjele IPv4-adresa.
7. U čemu su slični, a u čemu različiti upravljački protokoli ICMP i ICMPv6? Navedite nekoliko primjera!
8. Kojim upravljačkim protokolom svako računalo može locirati usmjeritelja u svojoj IPv6-mreži? Koje se poruke pritom razmjenjuju?
9. Istražite razmjenu poruka protokolom DHCPv6 pri autokonfiguraciji zasnovanoj na stanju čvora u kojoj sudjeluje posrednik te je prikažite slijednim dijagramom UML-a.
10. Istražite autokonfiguraciju bez poznavanja stanja koju provodi čvor samostalno a koja je zasnovana je na MAC-adresi predočenoj EUI-64 bitnim brojem te prikažite primjer tako konfiguirane adrese.
11. U koje su posebne vrste IPv6-adresa uključene IPv4-adrese i kakav je njihov format?
12. Skicirajte primjer tuneliranja IPv6-paketa kroz IPv4-mrežu na relaciji računalo-usmjeritelj, označite protokolni stog svakog čvora te izgled paketa i adrese u zaglavljima na svakoj dionici puta. Može li se na razmatranoj relaciji provesti automatsko tuneliranje i kako?
13. Skicirajte primjer tuneliranja IPv6-paketa kroz IPv4-mrežu na relaciji računalo-računalo, označite protokolni stog svakog čvora te izgled paketa i adrese u zaglavljima na svakoj dionici puta. Može li se na razmatranoj relaciji provesti automatsko tuneliranje i kako?
14. Skicirajte primjer tuneliranja IPv6-paketa kroz IPv4-mrežu na relaciji usmjeritelj-računalo, označite protokolni stog svakog čvora te izgled paketa i adrese u zaglavljima na svakoj dionici puta. Može li se na razmatranoj relaciji provesti automatsko tuneliranje i kako?
15. Kako će se moći pristupiti računalima u zadnjoj mreži koja će ostati povezana na Internet sa „starim“ IPv4-usmjeriteljem?

2. Pokretljivost u IP-mreži

Pokretljivost u IP-mreži odnosi se na pokretljivost u IP-sloju (engl. *IP mobility*), a problem se može sažeti ovako: kako omogućiti razmjenu paketa s čvorom – krajnjim sustavom s globalnom i jednoznačnom IP-adresom, ako i kad mijenja mjesto priključka na Internet, odnosno „otide“ iz „svoje“ mreže i priključi se u nekoj drugoj mreži? Paketi se s izvora usmjeravaju na odredište određeno prethodnom točkom priključka na Internet, a čvor (više) tamo nije priključen!

Pojam pokretnog IP-a se ne smije poistovjetiti s pojmom pokretnog Interneta (engl. *Mobile Internet*). Pojam „pokretnog ili mobilnog Interneta“ se u svakodnevnoj uporabi odnosi na pristup Internetu putem pokretne mreže, ili bežične lokalne mreže. Pokretna mreža pritom omogućuje stvarnu komunikaciju u pokretu (engl. *mobile communication*) i održavanje komunikacije tijekom promjene prostornog položaja. Bežična lokalna mreža omogućuje nomadsku komunikaciju (engl. *nomadic communication*), tj. samo bežično spajanje na prostoru pokrivenom tom mrežom, bez mogućnosti održavanja veze pri promjeni lokacije.

Mreža u kojoj je čvoru dodijeljena globalna i jednoznačna IP-adresa naziva se domaćom mrežom (engl. *Home Network*), a svaka druga mreža za njega je strana mreža (engl. *Foreign Network*). Uzmimo primjer na sl. 2.1 u kojem „obični“ čvor A koji ne mijenja mjesto priključka na mrežu šalje pakete pokretnom čvoru B koji mijenja mjesto priključka tako da iz domaće mreže odlazi u neku drugu, stranu, odnosno posjećenu mrežu. Paketi koje čvor A šalje čvoru B kao izvorišnu adresu imaju IP-adresu čvora A, a kao odredišnu globalnu i jednoznačnu IP-adresu čvora B, prema kojoj će biti usmjereni svi paketi. Ako se pokretni čvor B isključi iz domaće i priključi u stranu mrežu, on neće moći primati pakete, jer će se isti i dalje usmjeravati prema odredišnoj IP-adresi u domaćoj mreži. Pokretljivost u IP-sloju mora omogućiti usmjeravanje paketa prema novom odredištu pokretnog čvora u stranoj, posjećenoj, mreži, uz zadržavanje IP-adrese koja mu je pridijeljena u njegovoj, domaćoj mreži.



Slika 2.1 – Problem pokretljivosti u IP-sloju

Slični problemi javljaju se u svim mrežama u kojima se omogućuje pokretljivost krajnjih uređaja – terminala: kako „pronaći“ terminal koji se kreće, identificirajući ga samo njegovom

adresom ili pozivnim brojem koji su poznati pošiljatelju podataka, odnosno pokretaču komunikacije. Primjerice u pokretnoj mreži, pozivajući korisnik na svojem pokretnom telefonu bira pozivni broj nekog korisnika, a njegovu lokaciju odredit će pokretna mreža postupcima upravljanja pokretljivošću (engl. *mobility management*).

Pokretni terminal u pokretnoj mreži kao i pokretni čvor u IP-mreži mijenjaju „lokaciju“. Lokacija u pokretnoj mreži određena je fizičkim prostorom na kojem se korisnik trenutno nalazi, a promjena lokacije odgovara promjeni položaja u fizičkom prostoru. Lokacija u IP-mreži određena je IP-adresom, a promjena lokacije odgovara promjeni „položaja“ u adresnom prostoru. Pritom pokretljivost u IP-sloju ne treba biti potaknuta ikakvom promjenom fizičke lokacije: iz jedne se mreže može isključiti, a na drugu priključiti na istom mjestu!

Pri kretanju se provodi prebacivanje komunikacije (engl. *handover*, *handoff*) iz jednog područja u drugo, kao i prelaženje iz jedne mreže u drugu (engl. *roaming*). Dok su za pokretnе mreže ta dva pojma potpuno odvojena, tako da se prebacivanje odnosi na dva područja iste mreže, a prelaženje na dva područja različitih mreža, u internetskom okružju se oni često poistovjećuju i ne razlikuju. Tehnički, uvijek je riječ o prebacivanju, a administrativno, kad je regulirano nekim ugovornim odnosom između mreža, riječ je o prelaženju. Glatko prebacivanje (engl. *smooth handover*) označava mali gubitak podataka tijekom prebacivanja, brzo prebacivanje (engl. *fast handover*) da je postignuto malo kašnjenje, a neprekinuto (engl. *seamless handover*) da su i gubici i kašnjenje mali.

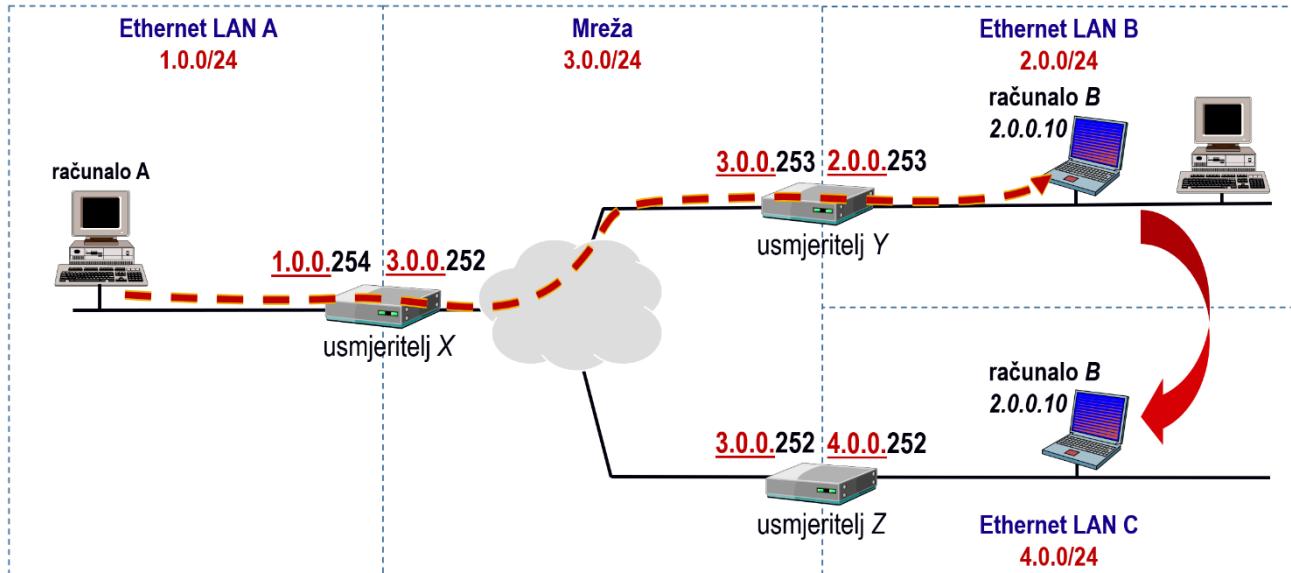
Kod "klasičnog" protokola IP, a time i Interneta, IP-adresa globalno i jednoznačno označuje čvor, odnosno sučelje čvora (računala ili usmjeritelja), na koji se dostavlja paket ili s kojeg se šalje paket. Datagrami se usmjeravaju isključivo na temelju odredišne adrese, koristeći pritom tablice usmjeravanja. IP-adresa sadrži mrežni i računalni dio, tako da se datagram usmjerava prema mreži označenoj mrežnim dijelom adrese (prefiksom), a kad stigne do nje dostavlja se računalu označenom računalnim dijelom adrese. Da bi računalu mogao biti dostavljen datagram, ono mora biti priključeno na odredištu označenom njegovom globalnom i jednoznačnom IP-adresom, u domaćoj mreži.

Pokretljivost u IP-sloju rješava dostavu paketa na odredište na kojem je čvor privremeno priključen u stranoj mreži. Riješena je na istim načelima za protokole IPv4 i IPv6, s boljom funkcionalnosti za *Mobile IPv6* u odnosu na *Mobile IP* koji predstavlja proširenje protokola IPv4.

2.1 Protokol Mobile IP

Promotrimo najprije pokretljivost u IPv4-mreži, a za ilustraciju neka posluži slučaj slanja datagrama s računala A iz mreže mrežnim prefiksom 1.0.0 na prijenosno računalo B u mreži mrežnim prefiksom 2.0.0 (sl. 2.2). Prema tablicama usmjeravanja, datagram prolazi niz usmjeritelja, od usmjeritelja izvorišne mreže X, kako bi došao do usmjeritelja Y odredišne mreže. Kad se računalo B nalazi u toj mreži, datagram se isporučuje. Ako se, međutim, računalo B s istom IP-adresom (2.0.0.10) priključi u mreži C s mrežnim prefiksom 4.0.0, usmjeritelj Y mu više ne može isporučiti datagram. Stoga će usmjeritelj Y poslati ICMP-poruku da je računalo nedostupno (engl. *Host Unreachable*) izvoru datagrama, u ovom primjeru računalu A.

Prijenosno računalo B s IP-adresom 2.0.0.10 promjenom priključka s LAN-a B na LAN C postaje nedostupno. Svaki datagram adresiran na prijenosno računalo bit će usmjerjen preko niza usmjeritelja do krajnjeg usmjeritelja Y, kao odredišnog usmjeritelja za računala s IP-adresama 2.0.0.x. Možemo zaključiti da je u "klasičnom" Internetu promjena priključne točke moguća samo ako računalo pri promjeni priključne točke promjeni i svoju IP-adresu, odnosno barem mrežni prefiks.



Slika 2.2 – Usmjeravanje paketa u IPv4-mreži

Međutim, oba rješenja su sasvim neprikladna za čvorove u pokretu, prvenstveno zbog nemogućnosti održavanja postojećih veza. Treba omogućiti promjenu odredišta tijekom komunikacije, tj. razmjenu paketa bez prekidanja komunikacije nakon promjene odredišta. To je osnovni zahtjev po kojem se pokretna komunikacija razlikuje od nomadske, kod koje čvor ne komunicira tijekom i nakon promjene mjesta priključka, već mora ponovo pokrenuti komunikaciju s novog odredišta.

Zahtjevi na pokretljivost u IP-sloju, a time i u Internetu, na temelju kojih je naknadno oblikovan poseban protokol *Mobile IP*⁸⁷ kao funkcionalno proširenje IPv4 su sljedeći:

- pokretni čvor mora moći komunicirati s drugim čvorovima nakon promjene točke priključka i održati postojeće veze tijekom promjene točke priključka;
- pokretni čvor mora moći komunicirati uporabom svoje stalne IP-adrese, neovisno o trenutnoj točki priključka na mrežu;
- pokretni čvor mora moći komunicirati s drugim čvorovima koji nemaju uvedene funkcije pokretljivosti;
- pokretni čvor ne smije biti izložen dodatnim sigurnosnim rizicima u odnosu na fiksne čvorove.

Mobile IP funkcionalno proširuje protokol IPv4, ali ni na koji način ne izaziva globalne promjene internetskih protokola koje bi za posljedicu imale promjenu programske podrške u

⁸⁷ „IP Mobility Support for IPv4, Revised“, RFC 5944, IETF, studeni 2010.

postojećim usmjeriteljima u mreži. Situacija je drukčija s protokolom IPv6, jer je pokretljivost bila jedan od početnih zahtjeva, tako da je *Mobile IPv6* integriran u rješenje tog mrežnog protokola, s programskom podrškom u novim usmjeriteljima za dvostruki IP-sloj ili samo IPv6.

Mobile IP je rješenje za pokretljivost izvedeno u mrežnom sloju. To znači da je ono potpuno nevidljivo sloju transporta i aplikacijama. Drugim riječima, postojeće TCP veze se održavaju kad je čvor u pokretu, a sve aplikacije rade isto kao i kad je čvor priključen u svojoj domaćoj mreži. Kao rješenje izvedeno u mrežnom sloju, *Mobile IP* je potpuno neovisan i o mediju preko kojeg se vrši prijenos (žično, bežično, optički, ...) i protokolima nižih slojeva. Pokretni čvor mora se moći kretati kako između različitih priključnih točaka na istoj vrsti medija (npr. s jednog *Ethernet LAN*-a na drugi), tako i s jednog medija na drugi (npr. žičnog na bežični LAN) bez gubitka veze na Internet. Na sloju podatkovne poveznice mora se riješiti odabir načina kompresije te zaštite podataka, kao i postupak pri promjeni priključne točke.

2.1.1 Adrese i funkcijski entiteti

Protokol *Mobile IP* uvodi dvije adrese i tri funkcijска entiteta kojima se rješava pokretljivost u IP-službi za protokol IPv4. Domaća adresa (engl. *Home Address*) je IP-adresa stalno dodijeljena pokretnom čvoru u njegovoj domaćoj mreži. Ona se ne mijenja prigodom kretanja čvora. Trenutna adresa (engl. *Care-of Address*) je IP-adresa dodijeljena pokretnom čvoru u stranoj mreži kad je priključen preko neke posjećene točke priključka. Trenutna adresa je jednoznačno određena za svaku točku priključka, što znači da se mijenja s promjenom točke priključka. Ta adresa koristi se kao odredišna adresa za datagrame namijenjene pokretnom čvoru. Primijetimo da je izvorišna adresa datagrama kojeg šalje pokretni čvor i dalje domaća adresa pokretnog čvora.

Mobile IP definira tri funkcijска entiteta (sl. 2.3) u kojima je izvedena podrška pokretljivosti:

- Pokretni čvor (engl. *Mobile Node, MN*): čvor koji mijenja točku priključka na Internetu s jedne poveznice na drugu, pri čemu zadržava sve već uspostavljene veze i koristi svoju stalnu, domaću IP-adresu.
- Domaći agent (engl. *Home Agent, HA*): usmjeritelj sa sučeljem na domaćoj poveznici pokretnog čvora koji pohranjuje i održava informaciju o trenutnoj IP-adresi. Domaći agent presreće datagrame adresirane na pokretni čvor i tunelira ih prema njegovoj trenutnoj adresi.
- Strani agent (engl. *Foreign Agent, FA*): usmjeritelj na posjećenoj poveznici u stranoj mreži gdje je pokretni čvor povezan na trenutnu točku priključka. Strani agent usmjerava datagrame ka pokretnom čvoru i od njega.



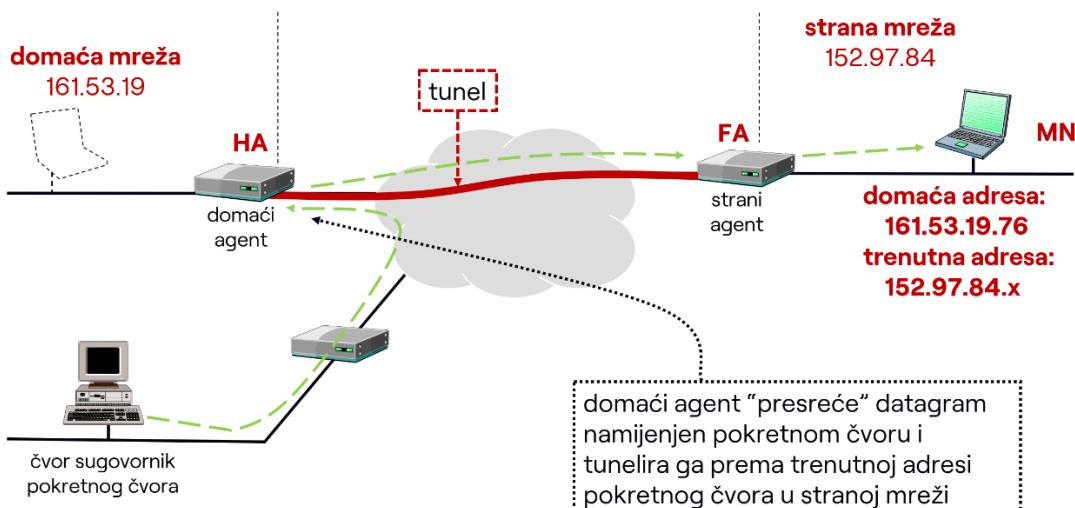
Slika 2.3 – Funkcijski entiteti protokola Mobile IP

Da bi računalo moglo djelovati kao pokretni čvor potrebna je njegova programska nadogradnja, kao i nadogradnja IPv4-usmjeritelja da bi oni mogli obavljati zadaće domaćeg i/ili stranog agenta.

Već je rečeno da domaći agent tunelira datagrame adresirane na stalnu adresu pokretnog čvora prema njegovoj trenutnoj adresi. Tunel je staza kojom prolaze datagradi na putu od domaćeg agenta prema stranom agentu. Tunelirani datagradi adresirani na pokretni čvor se ovijaju datagramom adresiranim na trenutnu adresu. Razlikuju se dvije vrste trenutnih adresa, s obzirom na način dodjeljivanja:

- trenutna adresa posredstvom stranog agenta (engl. *foreign agent care-of address*),
- mjesna trenutna adresa (engl. *co-located care-of address*).

U primjeru na sl. 2.4 pokretni čvor s domaćom adresom 161.53.19.76 priključen je u stranoj mreži koja mu je dodijelila posredstvom stranog agenta trenutnu adresu 152.97.84.x. Čvor sugovornik šalje datagrame pokretnom čvoru koji se usmjeravaju prema njegovoj domaćoj mreži, jer je njihova odredišna adresa 161.53.19.76. Domaći agent presreće datagrade upućene pokretnom čvoru i tunelira ih do stranog agenta koji „vadi“ izvorni datagram upućen od čvora sugovornika i dostavlja ga pokretnom čvoru.



Slika 2.4 – Tuneliranje datagrama do pokretnog čvora

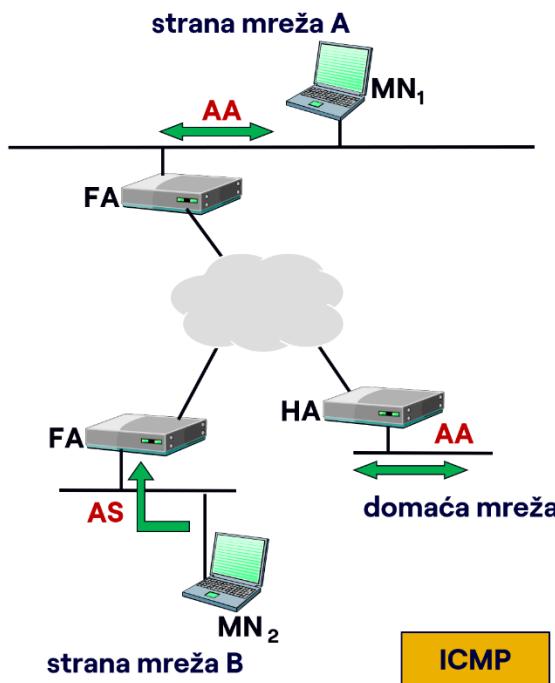
Trenutna adresa posredstvom stranog agenta je IP-adresa "izlazne točke tunela" na stranom agentu, kao što je prikazano na sl. 2.4. Više pokretnih čvorova može koristiti istu trenutnu adresu posredstvom stranog agenta. Mrežni prefiks takve trenutne adrese ne mora biti jednak mrežnom prefiksu strane poveznice na koju je priključen pokretni čvor.

Druga mogućnost, mjesna trenutna adresa, je IP-adresa privremeno dodijeljena sučelju pokretnog čvora, tako da je "izlazna točka tunela" na samom pokretnom čvoru. Takva trenutna adresa koja se koristi kad nema stranog agenta na posjećenoj poveznici, dodjeljuje se protokolom DHCP i može je istovremeno koristiti samo jedan pokretni čvor. Mrežni prefiks te adrese odgovara mrežnom prefiksu strane poveznice.

Prethodno obrazloženje komunikacije s pokretnim čvorom polazilo je od prepostavke da mu je dodijeljena trenutna adresa te da su agenti FA i HA razmijenili informacije o trenutnom priključku pokretnog čvora. Da bi se to obavilo, potrebne su posebne procedure kojima pokretni čvor otkriva agenta i registrira svoju trenutnu adresu.

2.1.2 Otkrivanje agenta

Procedurom otkrivanja agenta (engl. *Agent Discovery*) pokretni čvor određuje je li spojen na domaću ili stranu poveznicu, utvrđuje promjenu poveznice te dobiva trenutnu adresu kad promijeni poveznicu, bilo da se kreće iz domaće u stranu mrežu, bilo da mijenja poveznicu unutar strane mreže, ili iz jedne strane mreže u drugu (sl. 2.5).



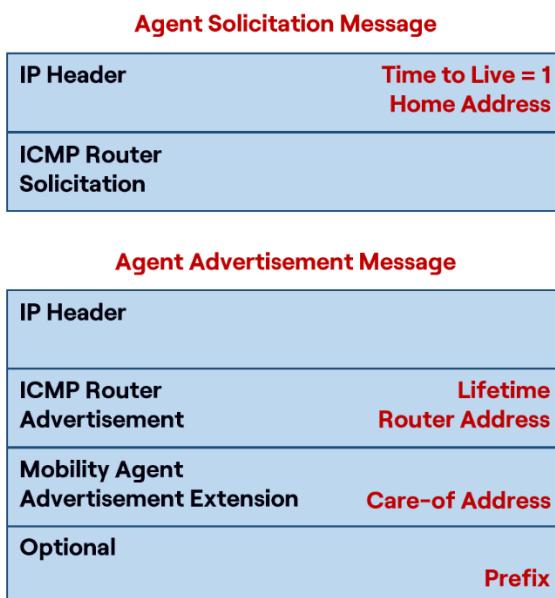
Slika 2.5 – Otkrivanje agenta

Svaki agent na poveznici (može ih biti više) periodički objavljuje da je spremjan služiti kao domaći agent, strani agent, ili oboje, i to na svim poveznicama za koje pruža tu uslugu. Te objave se kao poruke oglašavanja agenta (engl. *Agent Advertisement*, AA) razašilju svim ili skupini čvorova na lokalnoj povezničkoj/poveznici/poveznicama koje agent poslužuje, u ovom primjeru u stranoj mreži A pokretnom čvoru MN_1 .

Druga vrsta poruke je pobuđivanje agenta (engl. Agent Solicitation, AS) koju mogu slati pokretni čvorovi u pokušaju traženja agenta, u ovom primjeru pokretni čvor MN₂ u stranoj mreži B. Po primitku takve poruke, svi agenti odgovaraju s porukom oglašavanja agenta, AA. Taj mehanizam omogućuje brzo pronalaženje agenta za slučaj kada agenti rijetko razašilju poruke AS, kao i kad pokretni čvor brzo mijenja priključne točke.

Poruke oglašavanja i pobuđivanja agenta su ICMP-poruke čiji je format opisan na sl. 2.6. Format poruke pobuđivanja agenta, AS, odgovara formatu ICMP-poruke za pobuđivanje usmjeritelja (engl. Router Solicitation), uz parametar TTL = 1, kako bi se doseglo samo najbližeg agenta. Ta poruka sadrži domaću adresu pokretnog čvora koji traži agenta. Format poruke oglašavanja agenta, AA, proširen je format ICMP-poruke za oglašavanje usmjeritelja (engl. Router Advertisement) s dodatnim poljima sa sljedećim sadržajem:

- vrijeme života (engl. Lifetime) govori pokretnom čvoru za koliko vremena može očekivati sljedeću AA poruku od istog agenta. Kako se AA poruke mogu izgubiti, pogotovo na bežičnim vezama, agenti razašilju AA otprilike trostruko češće nego što bi to bilo određeno vremenom života.
- adresa usmjeritelja (engl. Router Address) koji se oglašava.
- trenutna adresa koju strani agent dodjeljuje pokretnom čvoru za registraciju s domaćim agentom.
- prefiks koji predstavlja masku (pod)mreže i služi za određivanje mrežnog prefiksa, različitog za svaku poveznicu, iz adrese usmjeritelja.



Slika 2.6 – Format poruka za oglašavanje i pobuđivanje agenta

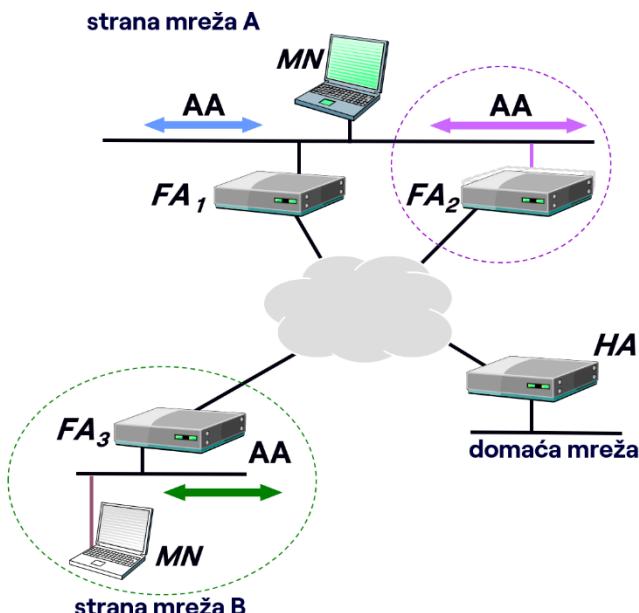
Pokretni čvor može pretpostaviti da je promijenio poveznicu ako u vremenu određenom poljem Lifetime ne primi poruku AA od stranog agenta koji ga je do tada posluživao ili ako ispitivanjem mrežnog prefiksa na temelju polja Router Address i Prefix u poruci AA primljenoj od drugog agenta utvrdi promjenu poveznice. U primjeru na sl. 2.7, kretanjem pokretnog čvora MN iz strane mreže A u stranu mrežu B, čvor dobiva poruku AA od drugog stranog agenta (FA₃), ustanavljava da je riječ o drugom mrežnom prefiku tj. drugoj mreži i zaključuje da je promijenio mrežu.

Kako je moguća nadležnost više agenata za jednu poveznicu, nije dovoljno ustanoviti da su dvije poruke AA u slijedu poslali različiti agenti, već obvezno treba provjeriti mrežni prefiks da bi se ustanovila promjena poveznice! U primjeru s dva agenta (mreža A, agenti FA₁ i FA₂) oglasio se agent FA₂, ali nije došlo do promjene poveznice.

Problemi s otkrivanjem agenta javljaju se ako pokretni čvor ne primi poruku AA nakon nekoliko uzastopnih poruka AS. Tad se može pretpostaviti da je pokretni čvor ili u domaćoj ili stranoj mreži, a da nešto nije u redu.

Ako se pretpostavi da se pokretni čvor nalazi u domaćoj mreži, a domaći agent ne radi (jer bi inače slao AA), pokretni čvor treba pokušati komunicirati s usmjeriteljem na domaćoj povezničkoj porukama ICMP-porukama *Echo Request/Echo Reply*. Ako se usmjeritelj odazove, pretpostavka je potvrđena.

Dalje se može pretpostaviti da je pokretni čvor u stranoj mreži u kojoj nema stranog agenta ili on ne radi. Da bi mogao komunicirati, pokretni čvor, može pokušati dobiti trenutnu adresu od DHCP-poslužitelja, a ako ni to nije moguće, adresu treba konfigurirati ručno.



Slika 2.7 – Utvrđivanje promjene poveznice

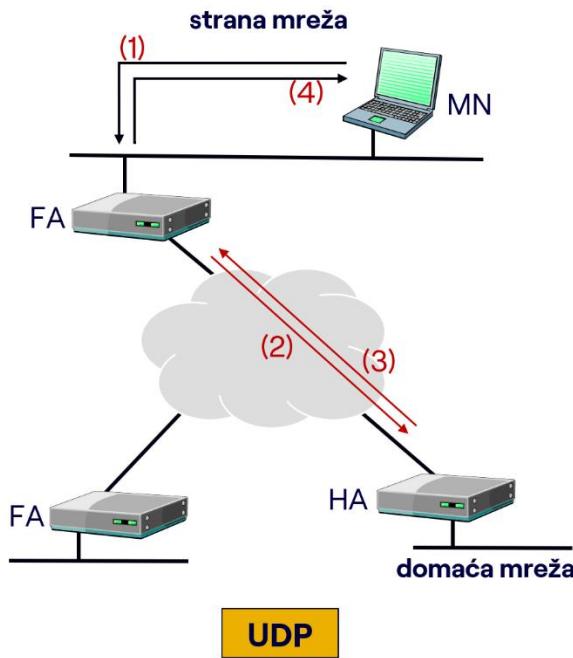
Iz prethodnog izlaganja jasno je da je otkrivanje agenta neophodno da bi pokretni čvor mogao odrediti je li spojen na domaću ili stranu poveznicu, utvrditi promjenu poveznice, kao i pribaviti trenutnu adresu kad promijeni poveznicu. To je preuvjet za registraciju pokretnog čvora.

2.1.3 Registracija i deregistracija pokretnog čvora

Registracija (engl. *Registration*) je postupak kojim pokretni čvor nakon otkrivanja agenta zahtijeva uslugu usmjeravanja od stranog agenta i obavješćuje domaćeg agenta o svojoj trenutnoj adresi. Registracija se periodički obnavlja, a po povratku u domaću mrežu pokretni čvor se odregistruje. U osnovnom scenariju, pokretni čvor se prijavljuje domaćem agentu preko stranog agenta (sl. 2.8).

Postupak teče ovako:

1. pokretni čvor šalje stranom agentu registracijski zahtjev (engl. *Registration Request*) sa svojom trenutnom adresom.
2. strani agent obrađuje registracijski zahtjev i prosljeđuje ga do domaćeg agenta.
3. domaći agent prihvata ili odbija registraciju i šalje registracijski odgovor (engl. *Registration Reply*) stranom agentu.
4. strani agent obrađuje registracijski odgovor i prosljeđuje ga do pokretnog čvora.



Slika 2.8 – Registracija pokretnog čvora

Registracija se obavlja porukama *Registration Request* i *Registration Reply* prikazanim na sl. 2.9. Za razliku od poruka za otkrivanje agenta koje se prenose ICMP-om, registracijske poruke prenose se UDP-datagramima. Pokretni čvor najčešće "zna" adresu domaćeg agenta unaprijed (postavljena ručnom konfiguracijom), a postoji i dinamički postupak otkrivanja te adrese. Vrijeme života obje poruke je ograničeno i mjeri se u sekundama (engl. *Lifetime*).

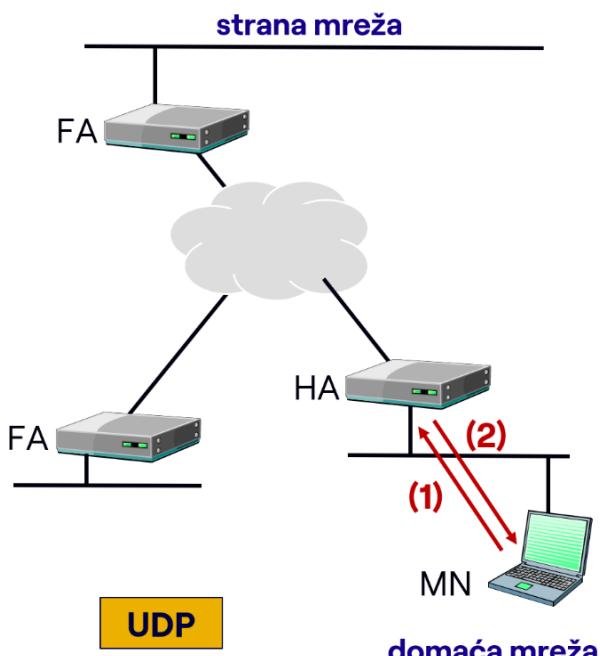
Registration Request	Registration reply
IP Header	IP Header
UDP Header	UDP Header
Type: Reg. Request Lifetime(s) Home Address Home Agent Care-of Address Identification (Reg. Request) Security Extension	Type: Reg. Reply Code (Reg. Reply result) Lifetime(s) Home Address Home Agent Identification (Reg. Reply) Security Extension

Slika 2.9 – Format registracijskog zahtjeva i registracijskog odgovora

Ako nema stranog agenta, tj. u slučaju kad se mjesna trenutna adresa dobije putem DHCP-poslužitelja, postupak registracije može se provesti izravnim slanjem poruke *Registration Request* na domaćeg agenta, koji potvrđuje registraciju s *Registration Reply*. U slučaju da pokretni čvor u određenom roku ne dobije *Registration Reply*, on pokušava ponovno, odnosno sve do isteka nekog unaprijed određenog maksimalnog vremena, nakon čega se registracija smatra neuspješnom.

Deregistracija je postupak koji slijedi po povratku pokretnog čvora u domaću mrežu. Također se provodi porukama *Registration Request* i *Registration Reply*. Po povratku u domaću mrežu pokretni čvor više ne koristi funkcije pokretljivosti. Deregistracija (sl. 2.10) odvija se ovako:

1. pokretni čvor se prijavljuje domaćem agentu po povratku u domaću mrežu deregistracijskim zahtjevom i time odregistriira svoju trenutnu adresu.
2. domaći agent potvrđuje deregistraciju odgovorom pokretnom čvoru



Slika 2.10 – Deregistracija pokretnog čvora

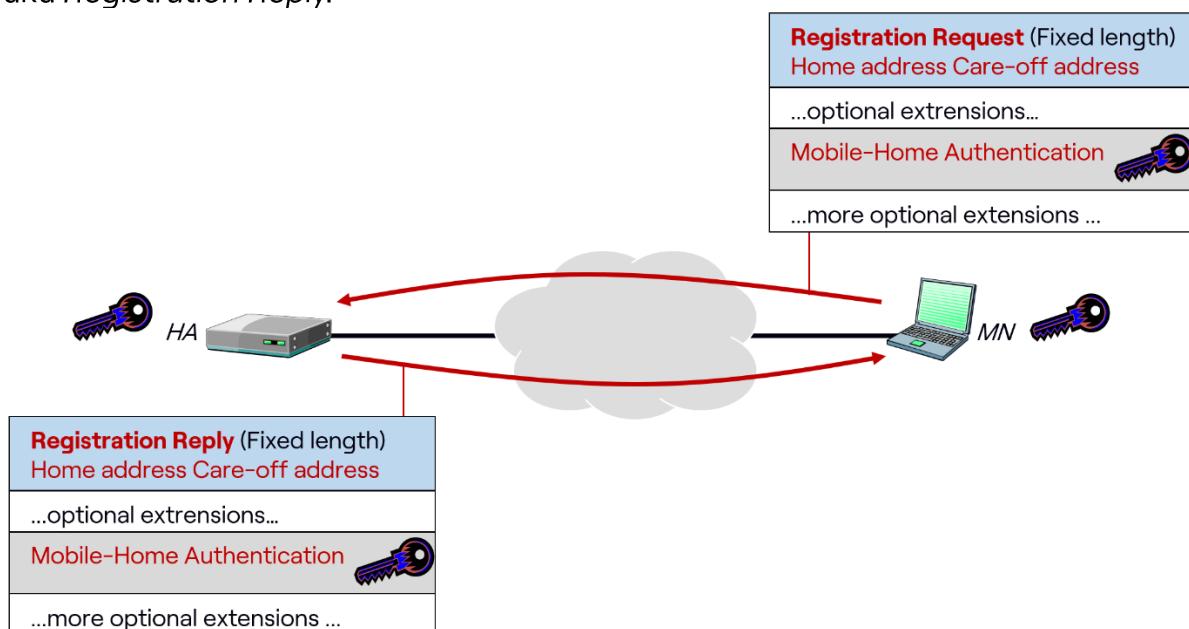
Registracija i deregistracija pokretnog čvora potencijalni je uzrok sigurnosnih problema, i to kako na strani čvora (zlonamjerni čvor), tako i agenata (zlonamjerni agenti). Zlonamjerni čvor mogao bi preuzeti identitet pokretnog čvora tako da preuzme njegovu domaću IP-adresu, registrira se u domaćoj mreži pokretnog čvora i radi mu štetu, primjerice čita povjerljive podatke, provodi različite elektroničke transakcije i drugo. Zlonamjerni agent se može predstaviti kao domaći agent i tako prevariti pokretni čvor te mu nanositi informacijsku i drugu štetu. Stoga je potrebno očuvati sigurnost registracije i deregistracije pokretnog agenta. Primjenjuju se dva sigurnosna postupka: provjera autentičnosti pokretnog čvora i agenta i zaštita cjelevitosti registracijskih poruka.

Mobile IP dopušta primjenu bilo koje dogovorene metode provjere autentičnosti između pokretnog čvora i domaćeg agenta. Propisano je samo da sve izvedbe Mobile IP-a moraju podržavati metodu tajnog ključa koja koristi algoritam sažetka poruke MD5^{38,39}.

Sigurna razmjena registracijskih poruka prikazana je na sl. 2.11:

- Pokretni čvor generira fiksni dio poruke *Registration Request* poruke i proširenje *Mobile Home Authentication* u kojem ostavlja prazno polje za kôd za provjeru autentičnosti.
- Pokretni čvor zatim računa sažetak cijele poruke koristeći tajni ključ koji je poznat pokretnom čvoru i njegovom domaćem agentu. Rezultat upisuje u predviđeno prazno polje *Mobile Home Authentication* i šalje poruku *Registration Request*.
- Na prijamnoj strani, domaći agent izračunava sažetak poruke istim algoritmom i provjerava slaže li se dobivena vrijednost s vrijednošću sažetka u samoj poruci. Ako su izračunata i primljena vrijednost kôda identične, domaći agent "zna" da je pošiljatelj poruke stvarno pokretni agent (autentičnost) te da poruka nije mijenjana pri prolasku kroz mrežu (integritet).

Isti postupak, sa zamijenjenim ulogama pokretnog čvora i domaćeg agenta, vrijedi i za poruku *Registration Reply*.



Slika 2.11 – Sigurna razmjena registracijskih poruka

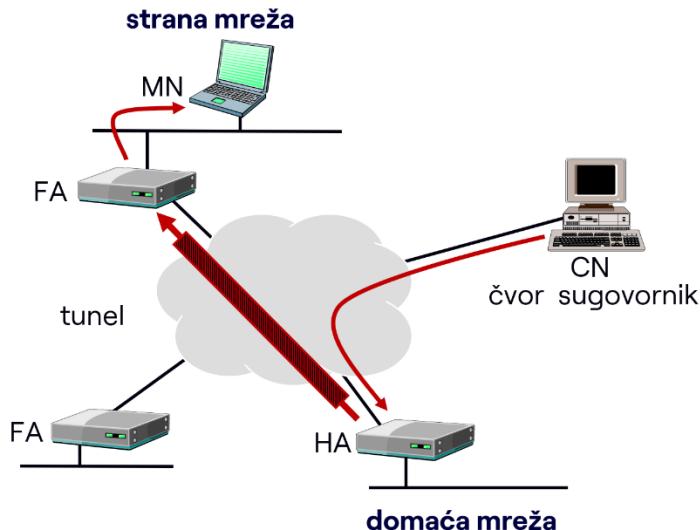
Slično se obavlja i provjera autentičnosti između pokretnog čvora i stranog agenta, te stranog agenta i domaćeg agenta

³⁸ "The MD5 Message-Digest Algorithm", RFC 1321, IETF, travanj 1992.

³⁹ " Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, IETF, ožujak 2011.

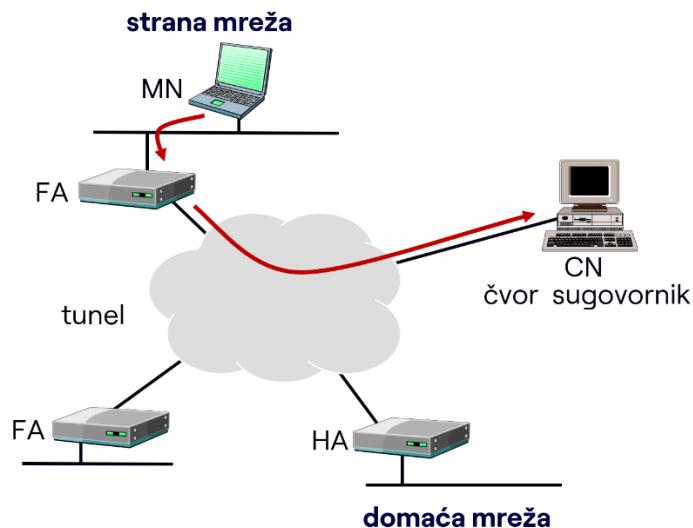
2.1.4 Usmjeravanje datagrama

Primjer na sl. 2.12 ilustrira usmjeravanje datagrama pri komunikaciji pokretnog čvora i čvora sugovornika. Usmjeravanje datagrama na pokretni čvor objašnjeno je ranije: domaći agent, HA, presreće izvorene datagrame upućene na domaću adresu pokretnog čvora i tunelira ih do stranog agenta, FA. Strani agent vadi izvorene datagrame iz tuneliranih i isporučuje ih pokretnom čvoru.



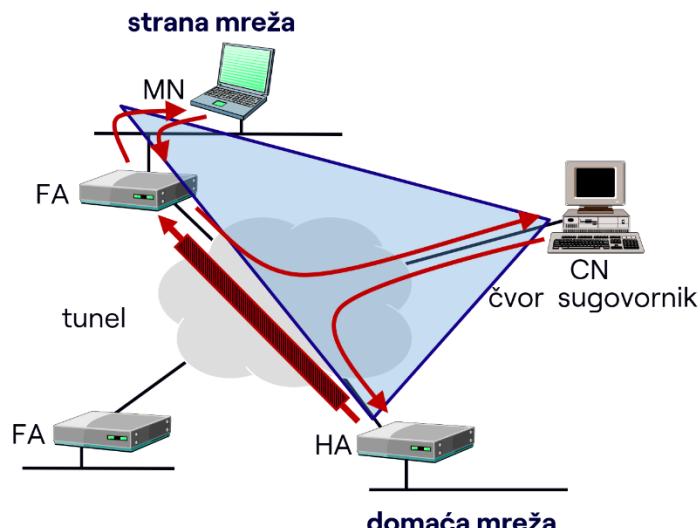
Slika 2.12 – Usmjeravanje datagrama na pokretni čvor

Usmjeravanje datagrama od pokretnog čvora prema čvoru sugovorniku provodi se kao za bilo koji čvor u istoj mreži (sl. 2.13). Kao usmjeritelj služi strani agent ili drugi usmjeritelj naveden u poruci *Agent Advertisement*. Ovdje je potrebno upozoriti na još jedan mogući sigurnosni problem: pokretni čvor koji šalje datagrame iz strane mreže, a kao izvořnu adresu navodi svoju domaću adresu. Usmjeritelj u stranoj mreži koji nadzire i filtrira odlazni promet (engl. *egress filtering*) sprječava slanje takvih paketa kako bi onemogućio zlonamjernog čvora koji se ubacio u mrežu, a koristi nečiju tuđu IP-adresu (engl. *IP address spoofing*) za svoje isto tako zlonamjerne aktivnosti predstavljajući se lažno. To će onemogućiti i komunikaciju pokretnog čvora! Jedno od mogućih rješenja, a to je reverzno tuneliranje od stranog do domaćeg agenta pa dalje do čvora sugovornika, objasnit će se na primjeru *Mobile IPv6*.



Slika 2.13 – Usmjeravanje datagrama s pokretnog čvora

Zbog rješenja zasnovanog na tuneliranju, javlja se problem tzv. trokutastog usmjeravanja, odnosno usmjeravanje u trokutu čvor sugovornik – domaći agent – pokretni čvor, zbog kojeg datagram prolazi dulji put od izvora do odredišta, uz dodatnu obradu datagrama u agentima, što utječe na kvalitetu, posebice stvarnovremenih usluga, zbog povećanog kašnjenja. To jače dolazi do izražaja kad je pokretni čvor daleko od domaćeg agenta, a blizu čvora sugovornika (sl. 2.14).



Slika 2.14 – Trokutasto usmjeravanje

„Ušteda“ vremena mogla se postići izravnim komuniciranjem od čvora sugovornika do pokretnog čvora, međutim potrebna je detaljnija procjena koja uzima u obzir i povećanu složenost radi održavanja sigurnosti. Stoga ovo pitanje nije imalo visok prioritet u razvoju protokola Mobile IP, a riješeno je u Mobile IPv6.

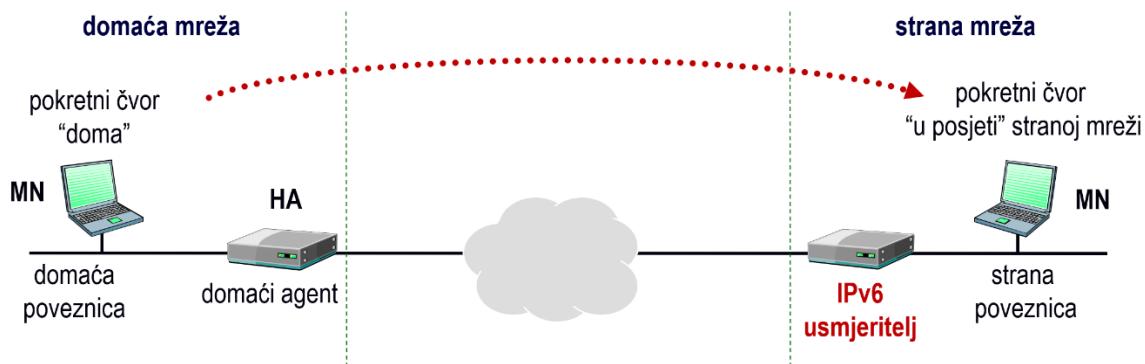
2.2 Protokol Mobile IPv6

Pokretljivost u IP-sloju, *Mobile IPv6*⁴⁰ kao sastavni dio specifikacije protokola IPv6 preuzima dobra rješenja od *Mobile IP*, iskorištava nove mogućnosti adresiranja, poboljšava sigurnost procedura otkrivanja agenta i registracije te optimizacijom puta između čvora sugovornika i pokretnog čvora rješava trokutasto usmjeravanje.

2.2.1 Adrese i funkcijски entiteti

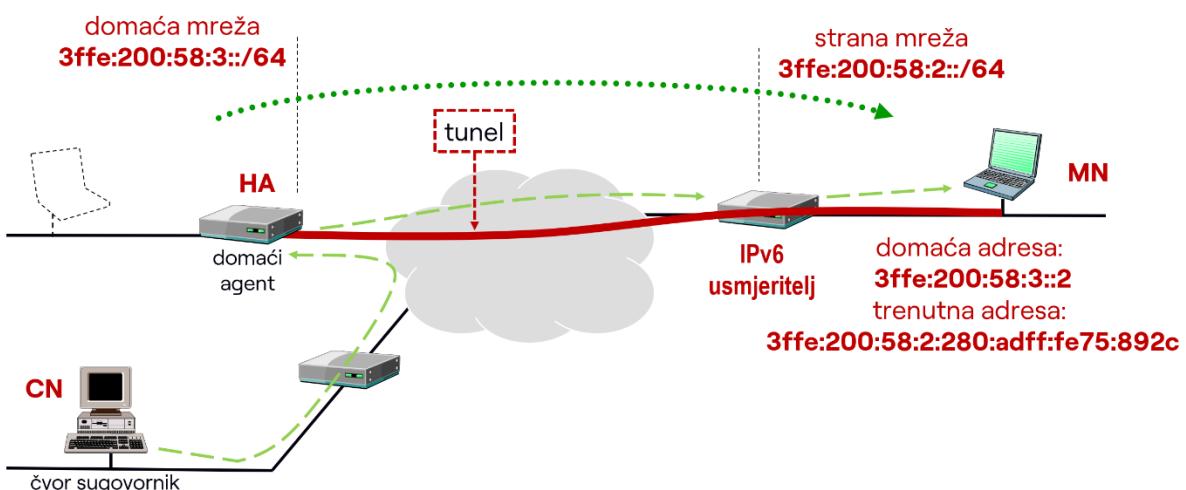
U odnosu na *Mobile IP*, pojmovi domaće i trenutne adrese ostaju isti, ali postoji samo jedna vrsta trenutne adrese, a to je mjesna trenutna adresa.

Osnovni funkcijski entiteti, pokretni čvor, MN i domaći agent odgovaraju onima iz *Mobile IP*. Čvor sugovornik specificiran je kao novi funkcijski entitet (engl. Correspondent Node, CN). Funkcionalnost stranog agenta integrirana je u IPv6-usmjeritelja, tako da više nema tog funkcijskog entiteta (sl. 2.15).



Slika 2.15 – Funkcijski entiteti Mobile IPv6

Komunikacija s pokretnim čvorom predočena je na sl. 2.16.



Slika 2.16 – Komunikacija s pokretnim čvorom

⁴⁰ „Mobility Support in IPv6”, RFC 6275, IETF, srpanj 2011.

Pokretni čvor, MN, iz domaće mreže (3ffe:200:58:3::/64) s domaćom adresom 3ffe:200:58:3::2 prešao je u stranu mrežu (3ffe:200:58:2::/64) u kojoj je autokonfigurirao trenutnu adresu 3ffe:200:58:2:280:adff:fe75:892c i registrirao je kod domaćeg agenta, HA. Kad čvor sugovornik, CN, šalje datagrame pokretnom čvoru oni se usmjeravaju prema njegovoj domaćoj mreži u kojoj ih presreće domaći agent, HA, i preusmjerava tunelom prema stranoj mreži. Ako je i sugovornik IPv6-čvor, tako da ima potporu za pokretljivost, može se pokrenuti procedura optimizacije usmjeravanja i nakon toga pakete upućivati izravno na pokretni čvor, izbjegavajući trokutasto usmjeravanje.

Procedure za upravljanje pokretljivošću koje uključuju registraciju i optimizaciju usmjeravanja izvedene su posebnim dodatnim zaglavljem pokretljivosti (engl. *Mobility Header*) koje se postavlja nakon svih ostalih dodatnih zaglavlja, a prije zaglavila višeg sloja. Osim tog zaglavla, za upravljanje pokretljivošću se koriste još dva dodatna zaglavla:

- zaglavje namijenjeno odredištu, za dojavu domaće adrese pokretnog čvora, MN, čvoru sugovorniku, CN, kao odredištu te
- zaglavje usmjeravanja, za izravno usmjeravanje na relaciji CN – MN, tj. na trenutnu adresu pokretnog čvora,

a porukama ICMPv6 provodi se otkrivanje domaćeg agenta i dobivanje mrežnog prefiksa. Razmjena poruka između MN i HA zaštićena je pomoću IPsec^{41,42}.

2.2.2 Otkrivanje usmjeritelja i promjene poveznice

Otkrivanje usmjeritelja odvija se slično postupku otkrivanja agenta kod *Mobile IP*, ali se ne primjenjuju poruke oglašavanja i traženja agenta. *Mobile IPv6* koristi protokol otkrivanja susjeda, NDP, za rješavanje problema koji se odnose na interakciju čvorova priključenih na istu poveznicu. NDP uključuje sljedeće poruke ICMPv6:

- pobuđivanje usmjeritelja (engl. *Router Solicitation*);
- oglašavanje usmjeritelja (engl. *Router Advertisement*);
- pobuđivanje susjeda (engl. *Neighbor Solicitation*);
- oglašavanje susjeda (engl. *Neighbor Advertisement*);
- preusmjeravanje (engl. *Redirect*).

Utvrđivanje promjene poveznice provodi se ovako:

- na poveznicama koje omogućuju višeodredišno adresiranje, svaki usmjeritelj periodički razasilje poruku *Router Advertisement* kojom oglašava da je raspoloživ;
- pokretni čvor osluškuje poruke *Router Advertisement*;
- ako unutar određenog vremena ne primi poruku *Router Advertisement* od istog usmjeritelja, ili od drugog usmjeritelja na istoj poveznici, pokretni čvor prepostavlja da je promijenio poveznicu te prelazi na autokonfiguraciju trenutne adrese.

⁴¹ „Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”, RFC 3776, IETF, lipanj 2004.

⁴² „Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture”, RFC 4877, IETF, travanj 2007.

Razlozi za autokonfiguraciju nove trenutne adrese prema tome mogu biti premještanje s jedne poveznice na drugu ili promjena adrese (prefiksa) usmjeritelja na poveznici na koju je priključen. Prefiks trenutne adrese odgovara mrežnom prefiksu strane mreže.

2.2.3 Registracija i deregistracija pokretnog čvora

Da bi se komunikacija mogla ostvariti, barem domaći agent, a po mogućnosti i trenutni sugovornici moraju saznati tu trenutnu adresu, a to se postiže registracijom koja se ovdje naziva povezivanjem (engl. *Binding*). Procedura je suštinski ista kao kod *Mobile IP*, tj. pokretni čvor registrira novu adresu kao trenutnu adresu kod domaćeg agenta koji je potvrđuje pokretnom čvoru. Poruke za povezivanje prenose se koristeći dodatno IPv6-zaglavljje – zaglavlje pokretljivosti i to:

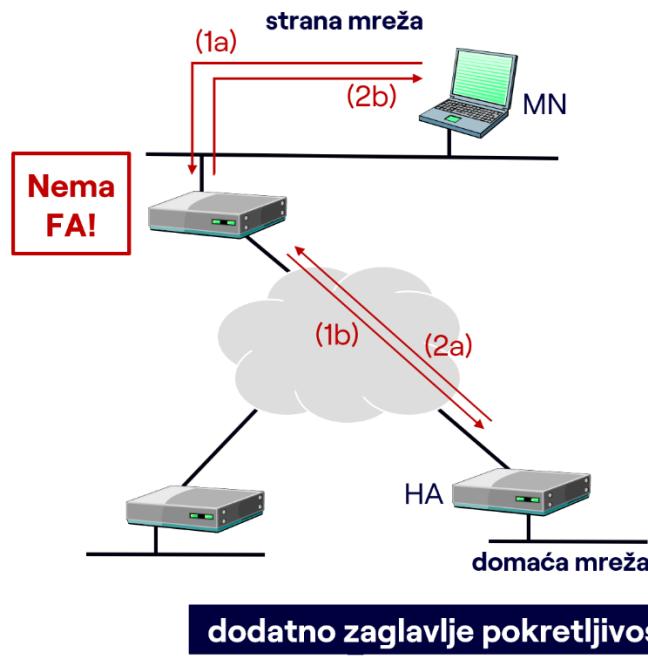
- ažuriranje povezivanja (engl. *Binding Update*): poruka kojom pokretni čvor obavješćuje domaćeg agenta o svojoj trenutnoj adresi;
- potvrda povezivanja (engl. *Binding Acknowledgement*): poruka kojom domaći agent potvrđuje primljenu poruku *Binding Update*;
- zahtjev za osvježavanjem povezivanja (engl. *Binding Refresh Request*): poruka sa zahtjevom čvora sugovornika da mu pokretni čvor pošalje poruku *Binding Update* za važeću trenutnu adresu;
- domaća adresa (engl. *Home Address*): poruka koju šalje pokretni čvor kao obavijest o svojoj domaćoj adresi.

Registracija pokretnog čvora prikazana na sl. 2.17 teče ovako:

- Pokretni čvor šalje poruku *Binding Update* do nadležnog usmjeritelja (1a) koji je iz strane mreže prosljeđuje dalje kroz mrežu (1b) do domaće mreže i domaćeg agenta;
- Domaći agent potvrđuje povezanost porukom *Binding Acknowledgement* iz domaće mreže (2a) koja se prosljeđuje dalje kroz mrežu (2b) do strane mreže i pokretnog čvora.

Uz izmijenjene procedure u odnosu na *Mobile IP*, učinkovitost upravljanja pokretljivošću popravljena je i uvođenjem posebnih struktura podataka koji omogućuju bržu obradu poruka. To su:

- spremnik pridruženih adresa (engl. *Binding Cache*) u domaćem agentu i čvorovima sugovornicima kojim se omogućuje provjera odredišne adrese svakog primljenog paketa i njegovo usmjeravanje na trenutnu adresu pokretnog čvora;
- popis poruka *Binding Update* u pokretnom čvoru (engl. *Binding Update List*) poslanih bilo domaćem agentu, bilo čvorovima sugovornicima, za koje nije isteklo vrijeme života registracije, *Lifetime*;
- popis domaćih agenata u pokretnom čvoru (engl. *Home Agents List*) sastavljen na temelju višeodredišno razaslanih poruka *Router Advertisements*.



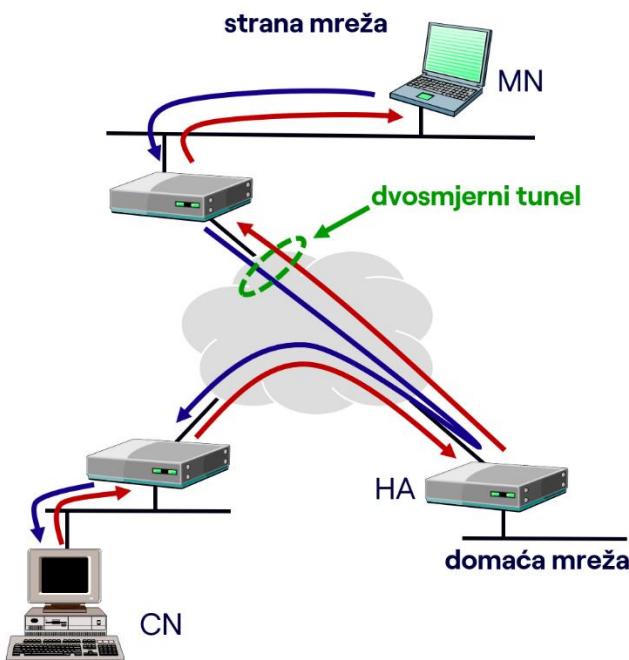
Slika 2.17 – Registracija pokretnog čvora

Deregistracija se provodi porukom *Binding Update* kojom se kao nova trenutna adresa postavlja domaća adresa pokretnog čvora.

2.2.4 Optimizacija usmjeravanja

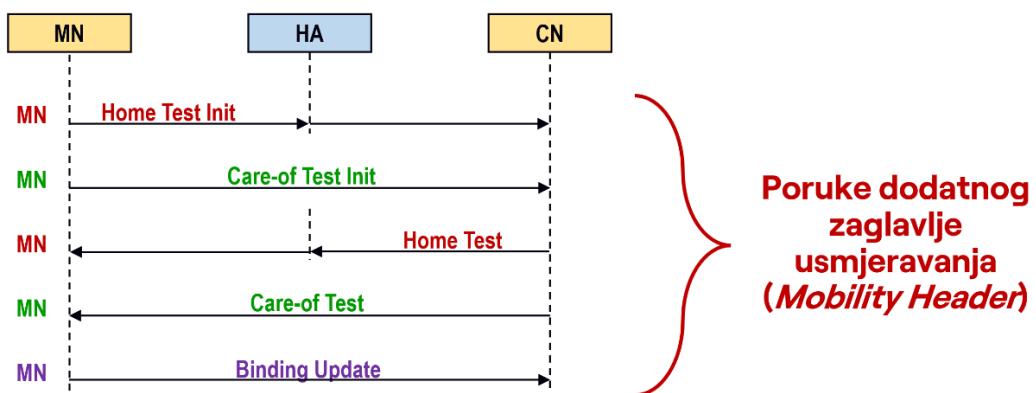
Usmjeravanje paketa između pokretnog čvora i čvora sugovornika bez optimizacije odvija se povratnim tunelom, kao što je prikazano na sl. 2.18.

Domaći agent razašilje poruku *Neighbor Advertisement* u ime pokretnog čvora na njegovoj domaćoj poveznici i time „privlači“ usmjeravanje prema pokretnom čvoru na tu poveznicu. Isto tako, domaći agent u ime pokretnog čvora odgovara na upit *Neighbor Solicitation* od usmjeritelja (*proxy Neighbor Discovery*). Domaći agent presreće pakete adresirane na pokretni čvor i tunelira ih prema trenutnoj adresi pokretnog čvora, a pokretni čvor šalje svoje pakete čvoru sugovorniku tunelirano preko domaćeg agenta. Ovo je primjer reverznog tuneliranja koje se primjenjuju za IPv6 kako bi se izbjegli sigurnosni problemi u mrežama koje se štite filtriranjem odlaznih paketa čije su adrese „sumnjive“, kao što to bi bila domaća adresa pokretnog čvora.



Slika 2.18 – Usmjeravanje paketa povratnim tunelom

Primjećujemo da se opet javlja problem neučinkovitog usmjeravanja. Kad bi čvor sugovornik, CN, imao informaciju o trenutnoj adresi, mogao bi izravno komunicirati s pokretnim čvorom, MN. Da bi to bilo moguće, registracija se mora obaviti ne samo s HA, nego i s CN, odnosno svim CN-ovima s kojima MN ima uspostavljene TCP-konekcije ili komunicira UDP-om. Procedura optimizacije usmjeravanja odvija se kao na sl. 2.19.



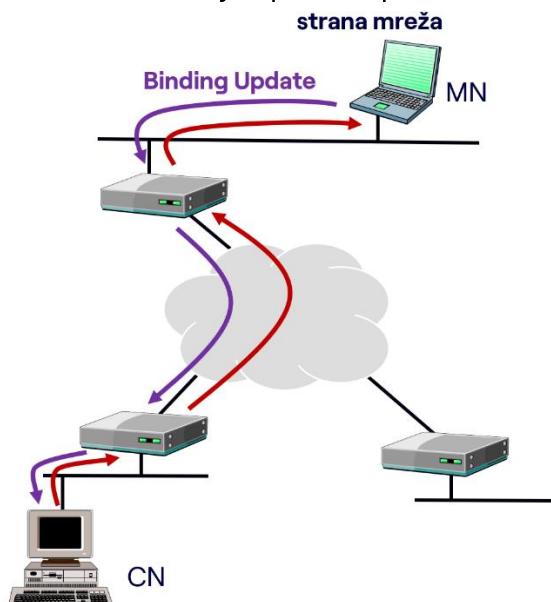
Slika 2.19 – Procedura optimizacije usmjeravanja paketa na pokretni čvor

Pokretni čvor šalje čvoru sugovorniku dvije poruke: najprije poruku *pokreni test domaće adresu* (*Home Test Init*, *HoTI*) putem domaćeg agenta, a zatim izravno poruku *pokreni test trenutne adresu* (*Care-off Test Init*, *CoTI*). Čvor sugovornik potvrđuje s porukom *test domaće adresu* (*Home Test Init*, *HoT*) putem domaćeg agenta i izravno porukom *test trenutne adresu* (*Care-off Test Init*, *CoT*).

Po uspješnoj razmjeni tih poruka, pokretni čvor šalje poruku *Binding Update* čvoru sugovorniku. IPv6-usmjeritelji pohranjuju tu informaciju u priručne spremnike važećih povezivanja. Za svaki poslani paket, usmjeritelji provjeravaju postoji li za odredišnu adresu

podatak u spremniku. Ako postoji, paket se izravno usmjerava prema pokretnom čvoru, koristeći dodatno zaglavje usmjeravanja, a ne više tuneliranje. U suprotnom, paket se usmjerava ubičajeno, tj. prema domaćoj poveznici.

U dodatnom zaglavju usmjeravanja definira se put kojom treba usmjeravati pakete prema pokretnom čvoru. Taj put ima dva "skoka". Prvi je trenutna adresa, a drugi i posljednji skok je povratna adresa unutar samog pokretnog čvora. Ishod usmjeravanja je da se paket šalje izravno pokretnom čvoru i to na njegovu trenutnu adresu. Komunikacija prema pokretnom čvoru sada može ići izravno, a ne više duljim putem, preko domaćeg agenta (sl. 2.20).



Slika 2.20 – Optimirano usmjeravanje paketa između čvora sugovornika i pokretnog čvora

Sigurnost podataka nužna je za sve poruke *Binding Update/Acknowledgement*, zbog istih prijetnji kojima je izložen i *Mobile IP*. Da bi se to postiglo, potrebno je ostvariti sigurnosno združivanje između entiteta koji razmjenjuju upravljačke poruke, MN i HA te MN i CN kako bi se postigla njihova autentičnost i integritet, kao i tajnost nekih podataka (trenutna adresa). Isto tako treba spriječiti sigurnosne napade koji koriste njihovo ponavljanje i promjenu redoslijeda.

Primjenjuje se arhitektura IPsec⁴³ integrirana u IPv6 kojom se jamči se autentičnost, integritet i tajnost podataka, a izvodi se dodatnim IPv6-zaglavljima^{44,45}. Ponavljanje i promjena redoslijeda može se onemogućiti posebnom numeracijom poruka.

Zaglavlje za provjeru autentičnosti (engl. *Authentication Header*, AH)⁴⁶ daje jamstvo da poruka stvarno dolazi s navedenog izvora i da nije mijenjana na putu. Zaglavlje za sigurnosno

⁴³ „Security Architecture for the Internet Protocol”, RFC 4301, IETF, prosinac 2005.

⁴⁴ „Using IPsec to Protect MIPv6 Signaling between Mobile Nodes and Home Agents”, RFC 3776, IETF, lipanj 2004.

⁴⁵ „Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)”, RFC 4835, IETF, travanj 2007.

⁴⁶ „IP Authentication Header”, RFC 4302, IETF, prosinac 2005.

ovijanje podataka (engl. *Encrypted Security Payload*, ESP)⁴⁷ jamči povjerljivost/tajnost podataka tj. da poruka nije na putu bila mogla biti pročitana.

Za ilustraciju, promotrimo sigurnu komunikaciju pokretnog čvora i domaćeg agenta. Datagram kojim se prenosi poruka *Binding Update* izgleda ovako:

1. Zaglavje IPv6 (izvorišna adresa: trenutna adresa MN, odredišna adresa: adresa HA).
2. Zaglavje s informacijama za odredište (opcija: domaća adresa).
3. Zaglavje za sigurnosno ovijanje, ESP, u transportnom načinu rada.
4. Zaglavje pokretljivosti (*Binding Update* s trenutnom adresom).

Datagram kojim se povratno prenosi poruka *Binding Acknowledgement* izgleda ovako:

1. Zaglavje IPv6 (izvorišna adresa: adresa HA, odredišna adresa: trenutna adresa MN).
2. Zaglavje usmjeravanja (domaća adresa).
3. Zaglavje za sigurnosno ovijanje, ESP, u transportnom načinu rada.
4. Zaglavje pokretljivosti (*Binding Acknowledgement*)

Slično se osiguravaju i druge upravljačke poruke za *Mobile IPv6*.

2.3 Ostali modeli pokretljivosti

Uz osnovne modele definirane protokolima *Mobile IP* i *Mobile IPv6*, istražuju se i razvijaju posebni modeli kojima se želi postići učinkovitije upravljanje pokretljivošću kad se pokretne čvor kreće između poveznica ili podmreža na istoj stranoj mreži, kad se kretanje odvija u ad-hoc mreži ili se cijela mreža kreće.

IP-mikropokretljivost (engl. *IP micro mobility*) dopunjava „makropokretljivost“ koju omogućuju *Mobile IP* i *Mobile IPv6*. Mikropokretljivost se odnosi na kretanje čvora unutar jedne domene, između poveznica ili podmreža u istoj stranoj mreži. U takvoj bi situaciji česte promjene priključne točke, a time i trenutne adrese, izazivale povećanu razmjenu upravljačke informacije između strane i domaće mreže, sa svim poteškoćama koje izaziva prebacivanje komunikacije (gubitak podataka, kašnjenje). Posebni protokoli to rješavaju na različite načine^{48,49,50}.

Ad-hoc mreža (engl. *Mobile Ad-Hoc Network*, MANET) je posebna vrsta mreže bežično povezanih čvorova koji se mogu kretati i pritom mijenjati povezanost s ostalim čvorovima⁵¹. Takva mreža nema (unaprijed) definiranu strukturu i topologiju – kako se čvorovi kreću i mijenjaju odnose u prostoru, tako se mijenja mreža i mogući način usmjeravanja paketa između čvorova, za što su potrebni posebni protokoli.

⁴⁷ „IP Encapsulating Security Payload (ESP)”, RFC 4303, IETF, prosinac 2005.

⁴⁸ „Hierarchical Mobile IPv6 (HMIPv6) Mobility Management”, RFC 5380, IETF, listopad 2008.

⁴⁹ „Mobile IPv6 Fast Handovers”, RFC 5568, IETF, srpanj 2009.

⁵⁰ „Proxy Mobile IPv6”, RFC 5213, IETF, kolovoz 2008.

⁵¹ „Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, RFC 2501, IETF, siječanj 1999.

Mrežna pokretljivost (engl. *Network Mobility*, NEMO) se odnosi na cijelu mrežu koja se kreće i mijenja priključak na Internet⁵²⁵³, primjerice takva bi bila mreža u vlaku.

2.4 Zadaci

1. Pobrojite i obrazložite zahtjeve na pokretljivost u IP-mreži.
2. Objasnite funkcije pokretnog čvora te domaćeg i stranog agenta specificirane protokolom *Mobile IP*.
3. Definirajte tri podmreže koje međusobno komuniciraju putem četvrte IPv4-mreže. Jedna od podmreža je domaća, a druga strana mreža pokretnog čvora, dok je u trećoj čvor sugovornik. Dodijelite IP-adrese čvorovima te prikažite kakve su izvođene i odredišne adrese datagrama koje razmjenjuju pokretni čvor u stranoj mreži i čvor sugovornik.
4. Kako je protokolom *Mobile IP* riješeno otkrivanje agenta i registracija pokretnog čvora?
5. Zašto polje TTL u ICMP-poruci pobuđivanja agenta (*Agent Solicitation*) treba biti postavljeno na vrijednost „1“?
6. Zašto se registracijske poruke prenose transportnim protokom UDP, a ne koristi se protokol TCP?
7. Čime se postiže sigurnost registracije pokretnog čvora za protokol *Mobile IP*? Što se onemogućuje primjenom sigurnosnih mehanizama?
8. U kojem je slučaju, s motrišta lokacije čvorova, problem trokutastog usmjerenja u IPv4-mreži najizraženiji? Odgovor popratite skicom mreža koja ilustrira problem!
9. Može li i kako pokretni čvor komunicirati u stranoj IPv4-mreži u kojoj nisu izvedene funkcije pokretljivosti?
10. Objasnite funkcije čvorova i agenata kojim se rješava pokretljivost za protokol IPv6.
11. Koja je uloga dodatnog zaglavlja pokretljivosti protokola IPv6? Koje mjesto u redoslijedu dodatnih zaglavlja zauzima zaglavje pokretljivosti?
12. Koja je uloga protokola NDP kod pokretljivosti u IPv6-mreži?
13. Istražite kako izgleda IPv6-datagram koji sadrži poruku *Binding Update*. Prikažite format osnovnog i svih korištenih dodatnih zaglavlja.
14. Istražite kako izgleda IPv6-datagram koji sadrži poruku *Binding Acknowledgement*. Prikažite format osnovnog i svih korištenih dodatnih zaglavlja.
15. Usporedite rješenja za pokretljivost u IP-sloju za protokole IPv4 i IPv6.

⁵² „Network Mobility Support Terminology”, RFC 4885, IETF, srpanj 2007.

⁵³ „Network Mobility Support Goals and Requirements”, RFC 4886, IETF, srpanj 2007.

3. Protokoli usmjeravanja u Internetu

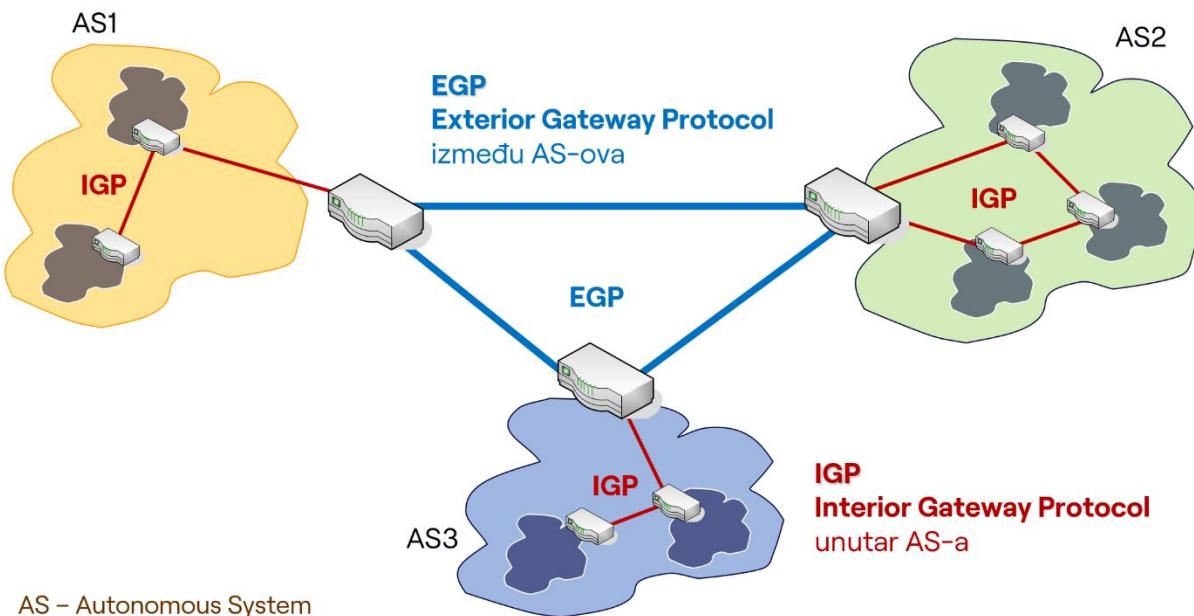
Jedna od osnovnih zadaća protokola IP je usmjeravanje. Internet je datagramska mreža i radi na načelu komutacije paketa.

Usmjeravanje je postupak pronalaženja puta i prosljeđivanja paketa od izvorišnog do odredišnog čvora u mreži. Svaki paket (IP-datatype) usmjerava se preko niza međusustava i podmreža na temelju odredišne adrese, neovisno o ostalim datagramima. Treba podsjetiti da na mrežnom sloju nema uspostavljanja veze s kraja na kraj – mrežni spoj pruža nespojnu uslugu!

Protokole usmjeravanja dijelimo s obzirom na područje djelovanja:

- unutar autonomnog sustava (*Interior Gateway Protocol*, skr. IGP),
- između autonomnih sustava (*Exterior Gateway Protocol*, skr. EGP).

Autonomni sustav (engl. *autonomous system*, AS) je skup mreža, podmreža i usmjeritelja temeljenih na istim načelima pod zajedničkom upravom i zajedničkom politikom usmjeravanja “prema van”, odnosno prema ostalim AS-ovima. Najčešće se nalazi pod administracijom i u vlasništvu jednog mrežnog operatora, davaljatelja internetskih usluga (engl. *Internet Service Provider*, skr. ISP) ili veće kompanije i koriste jedinstveni protokol IGP. Svaki AS ima jedinstveni broj (engl. *autonomous system number*, skr. ASN)⁵⁴. Primjer AS-a je Hrvatska akademска i istraživačka mreža CARNet s jedinstvenim brojem AS 2108. Na slici 3.1 prikazana je klasifikacija protokola usmjeravanja.



Slika 3.1 – Klasifikacija protokola usmjeravanja

⁵⁴ „Guidelines for creation, selection and registration of Autonomous System (AS)“, RFC 1930, IETF, travanj 1996.

Protokoli usmjeravanja koriste dinamički (adaptivni) algoritam usmjeravanja. Kod procesa usmjeravanja moraju biti zadovoljeni zahtjevi kao što su jednostavnost, zauzimanje što manje mrežnih resursa, mogućnost samostalnog izlaza iz neregularnih stanja, itd. Kada usmjeritelj dobije paket, mora ga proslijediti sljedećem usmjeritelju. Dakle, mora imati informacije o ostalim usmjeriteljima i računalima u Internetu koje su zapisane u tablicama usmjeravanja.

Tablicu usmjeravanja koju posjeduje svaki usmjeritelj potrebno je stalno ažurirati, budući da dolazi do promjena u topologiji mreže, zbog uvođenje novih čvorova ili povremenih ispada čvorova ili poveznica. Na osnovu podataka u tablicama usmjeravanja, za svaki datagram potrebno je odabrati optimalni put i proslijediti ga po odabranom putu prema sljedećem usmjeritelju. Optimalnost puta određuje se s obzirom na kašnjenje, udaljenost, cijenu i druge parametre.

Usmjeritelj mora biti u mogućnosti djelovati ako dođe do nekakve pogreške u mreži. U slučaju pogreške, šalje odgovarajuću poruku ICMP (*Internet Control Message Protocol*). Mogući slučajevi su: nepoznata odredišna mreža IP-paketa, zagušenje u mreži ili istek vremena života paketa (TTL = 0).

3.1. Besklasno usmjeravanje

Besklasno usmjeravanje (engl. *Classless Inter-Domain Routing*, skr. CIDR) je usmjeravanje kod kojeg se odredišna IP-adresa određuje na temelju mrežnog prefiksa⁵⁵. Putovi usmjeravanja ne agregiraju se prema klasama adresa, već prema mrežnom prefiksnu. Duljina mrežnog dijela (*Net ID*) se označava prefiksom iza adrese, npr. 195.24.0.0/13, a prvih 13 bitova određuju adresu podmreže. Veličina mrežnog dijela adrese može biti proizvoljna, a dopušteno je i agregiranje – združivanje (engl. *route aggregation* ili *supernetting*) prefiksa kod usmjeravanja, s tim da združeni prefiksi ne smiju sadržavati adrese mreža koje im ne pripadaju. Primjer združivanja će biti pokazan kasnije.

Prednosti besklasnog usmjeravanja su u učinkovitijem iskorištenju adresnog prostora te unapređenju upravljanja tablicom usmjeravanja jer su tablice usmjeravanja manje, odnosno sadrže manji broj zapisa u usporedbi s tablicom usmjeravanja usmjeritelja koji ne podržavaju besklasno usmjeravanje. Osnovni nedostatak je što je sam proces usmjeravanja složeniji.

3.2. Protokol RIP

Protokol RIP (*Routing Information Protocol*) je protokol usmjeravanja unutar autonomnog sustava, a u uporabi je inačica je RIPv2⁵⁶. Podržava besklasno usmjeravanje, maske podmreža, rutu sljedećeg skoka (engl. *next hop route*), autentifikaciju te skupno razšiljanje (engl. *multicast*). Osnovna značajka protokola RIP je da se kriterij odabira puta (metrika) temelji na (dinamičkom) algoritmu vektora udaljenosti (engl. *vector distance*), odnosno broju skokova, a za komunikaciju koristi transportni protokol UDP.

Osnovne operacije protokola RIP su:

⁵⁵ „Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan”, RFC 4632, IETF, kolovoz 2006.

⁵⁶ „Routing Information Protocol Version 2”, RFC 2453, IETF, studeni 1998.

- prilikom uvođenja i pokretanja usmjeritelj traži od susjednih usmjeritelja kopije njihovih tablica usmjeravanja,
- u aktivnom načinu rada usmjeritelj šalje tablice usmjeravanja svim susjednim usmjeriteljima, periodički, svakih 30 sekundi (jedan ciklus),
- svaka promjena topologije mreže (metrike) šalje se ostalim usmjeriteljima skupnim razasiljanjem,
- usmjeritelj prihvata tablice usmjeravanja od svojih susjeda, uspoređuje ih sa svojom te ažurira ako je potrebno,
- ako usmjeritelj ne dobije tablicu usmjeravanja od susjeda unutar 6 ciklusa (180 s), ruta se postavlja na „beskonačnu metriku“ (16) što označava prekid veze, a nakon 60 s ruta se briše iz tablice usmjeravanja.

3.2.1. Format zaglavljia

Slika 3.2. prikazuje zaglavljje paketa RIP. Polje *tip RIP datagrama* označava radi li se o zahtjevu za informacijom (vrijednost 1) ili odgovoru na zahtjev (vrijednost 2). Polje *inačica* označava inačicu protokola koja se koristi. Polje *identifikacija protokola* najčešće ima vrijednost 2 što označava da se radi o 32-bitnim IP-adresama. U nastavku je polje koje opisuje vezu s ostalim usmjeravajućim protokolima IGP i EGP (obično je vrijednost 0). Nakon toga slijede informacije o rutama koje se šalju, odnosno vrijednosti tablice usmjeravanja s parametrima za svaku rutu (engl. *route table entry*, skr. RTE): IP adresa, maska podmreže, sljedeći skok te metrika. U jednom paketu može biti najviše 25 zapisa o rutama.

0	8	16	24	31			
Tip RIP datagrama	inačica	ne koristi se					
Identifikacija protokola (2 za IPv4)	Veza s ostalim protokolima (route tag)						
IP adresa (rute koja se šalje)							
maska podmreže							
sljedeći skok							
metrika							

Slika 3.2 – Format zaglavljia RIP

3.2.2. Nedostaci protokola

Osnovni nedostatak protokola RIP je metrika koja se temelji na udaljenosti, odnosno broju skokova: najbolja je ruta s najmanjim brojem skokova. Problem posebno dolazi do izražaja kada je na nekoj dionici odabrane rute zagušenje, jer bi u tom slučaju bilo bolje usmjeravati na rutu s boljom propusnosti poveznica, iako ta ruta uključuje veći broj skokova. Ograničenost na 15 skokova što predstavlja maksimalni broj skokova ili „beskonačnu metriku“ ne dozvoljava primjenu u većim mrežama.

Sljedeći nedostatak protokola RIP je spora konvergencija algoritma, a što je opisano u udžbeniku *Komunikacijske mreže* (poglavlje 4.4.3). Riječ je o tome da se algoritam bolje ponaša kod oglašavanja „dobrih vijesti“ (npr. dodavanje novog usmjeritelja ili nove rute), nego kod „loših vijesti“ (npr. ispad usmjeritelja ili prekid veze). Nadalje, potrebno je 180 sekundi (6 ciklusa) kako bi se „shvatilo“ da je došlo do prekida ili ispada.

Zbog prirode algoritma vektora udaljenosti koji ne sprječava petlje u usmjeravanju može se javiti tzv. „brojanje u beskonačnost“ (engl. *count to infinity*). Problem je u sljedećem: usmjeritelj koji prima rutu od drugog, susjednog usmjeritelja, ne zna je li on sam dio te rute. Ako jeste, višestruki prolaz istim usmjeriteljem/usmjeriteljima – petlja, pri određivanju najkraćeg puta, tj. najbolje rute, utječe na stvaranje rute „beskonačne“ duljine (vidi primjer: Knjiga „Komunikacijske mreže“, Slika 4.10 – Primjer: reakcija algoritma vektora udaljenosti na ispad čvora u topologiji).

3.2.3. Poboljšanja protokola

Za problem „brojanja u beskonačnost“ u praksi je predloženo više rješenja, jedno od njih je poboljšanje algoritma vektora udaljenosti razdvajanjem horizonta (engl. *split horizon*). Riječ je o tome da svaki usmjeritelj zanemaruje povratne informacije o ruti od usmjeritelja koji su naučili o toj ruti upravo od njega (tzv. petlje). Razdvajanjem horizonta usmjerava se na sve usmjeritelje prema naprijed, osim unatrag, prema usmjeritelju koji je posao poruku za ažuriranje tablice usmjeravanja.

Druga mogućnost je da se povratne informacije o ruti uvijek šalju s maksimalnom metrikom 16, tj. da se „otruje“ povratna informacija (engl. *split horizon with poisoned reverse*). U tom slučaju će se izbjegći krivi zaključak da je povratna informacija o ruti „bolja“ (s manjom metrikom) od izvorene.

Nadalje, budući da se „brojanje u beskonačnost“ u većini slučajeva javlja zbog kašnjenja informacije o promjeni, odnosno različitih vremena primitka informacije o prekidu prilikom razašiljanja, nakon detekcije prekida moguće je postaviti vremensku kontrolu (60 – 120 sekundi) tijekom koje se zanemaruju sve dobivene informacije o rutama. Ovaj postupak se naziva zadržavanje informacije o prekidu (engl. *hold-down*).

Kao dodatno rješenje za sporu konvergenciju primjenjuje se da se svaka informacija o promjeni šalje čim se ona dogodi (engl. *triggered update*) i u tom slučaju se ne čeka period od 30 sekundi za slanjem tablice usmjeravanja susjednim čvorovima.

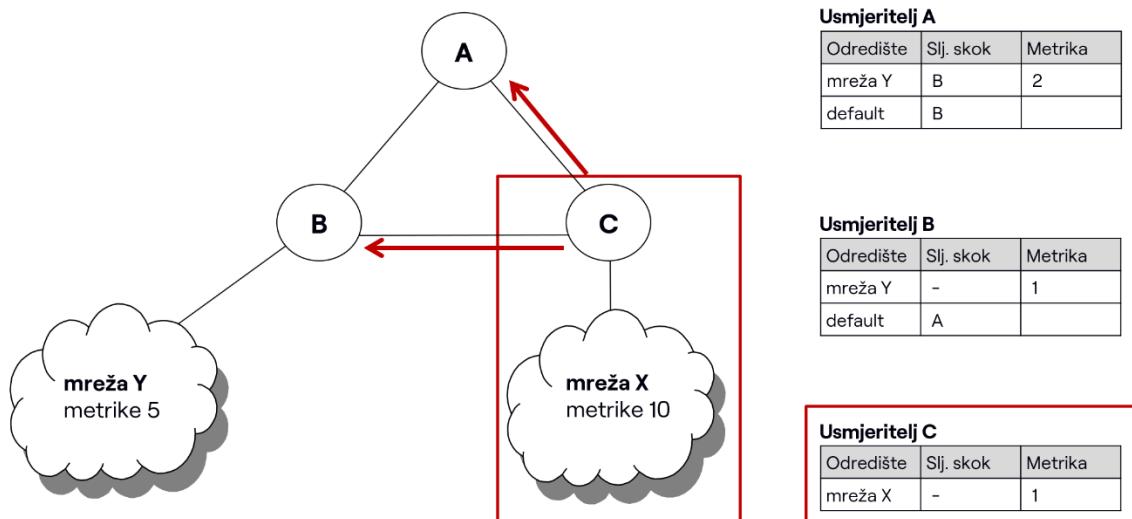
3.2.4. Primjeri rada protokola

U nastavku su dani primjeri koji ilustriraju rad protokola RIP prilikom punjenja tablica usmjeravanja, uvođenja novog usmjeritelja u mrežu i prekida veze te ukazuju na nedostatke protokola. U primjerima metrika 1 u tablicama usmjeravanja označava izravnu povezanost, metrika 2 da se na putu do odredišta nalazi jedan usmjeritelj (skok) na putu, itd.

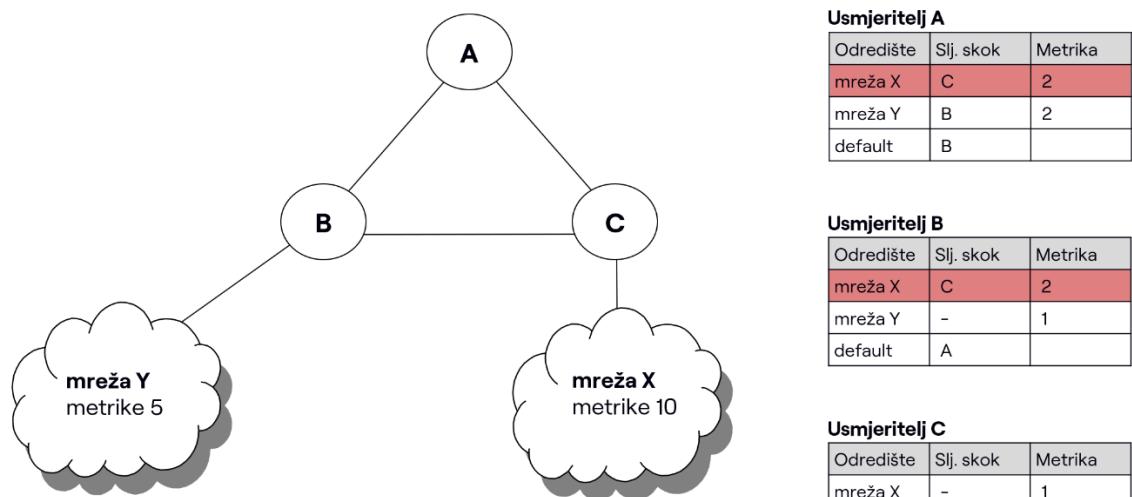
Primjer 1: početno punjenje tablice usmjeravanja

Pretpostavimo uvođenje novog usmjeritelja C u mrežu (slika 3.3). Usmjeritelj C povezuje mrežu X metrike 10 s ostatkom mreže. Mreža metrike 10 označava da se u toj mreži nalaze usmjeritelji koji su povezani tako da je paketu potrebno 10 skokova da „prođe“ mrežu s jednog kraja na drugi. U prvom trenutku tablica usmjeravanja je prazna, odnosno jedini zapis kojeg posjeduje jest veza s mrežom X metrike 1 (izravna povezanost). Usmjeritelj C u prvom koraku šalje svoju tablicu usmjeravanja susjednim usmjeriteljima.

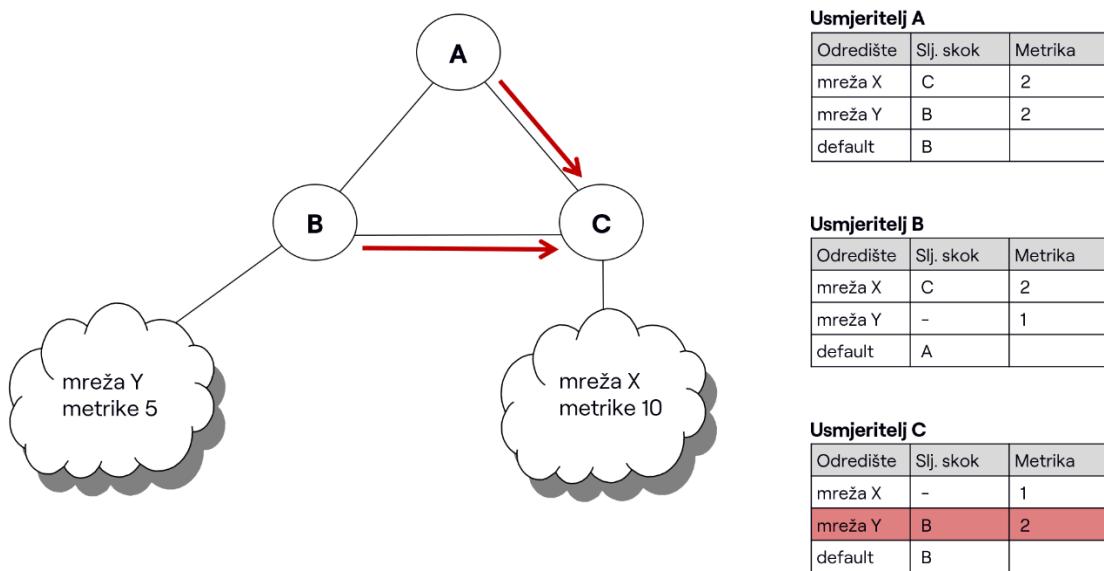
U drugom koraku, nakon što usmjeritelji A i B prihvate tablicu usmjeravanja od C, ažuriraju pristiglu informaciju u svojim tablicama usmjeravanja. Unose u svoju tablicu usmjeravanja podatak o novoj mreži X i njenoj ruti, odnosno dodaju zapis o novoj ruti prema mreži X koju dohvaćaju preko usmjeritelja C (metrike 2), što je predviđeno na slici 3.4.



Slika 3.3 – Slanje tablice usmjeravanja susjednim usmjeriteljima A i B (korak 1)



Slika 3.4 – Ažuriranje tablica usmjeravanja usmjeritelja A i B (korak 2)



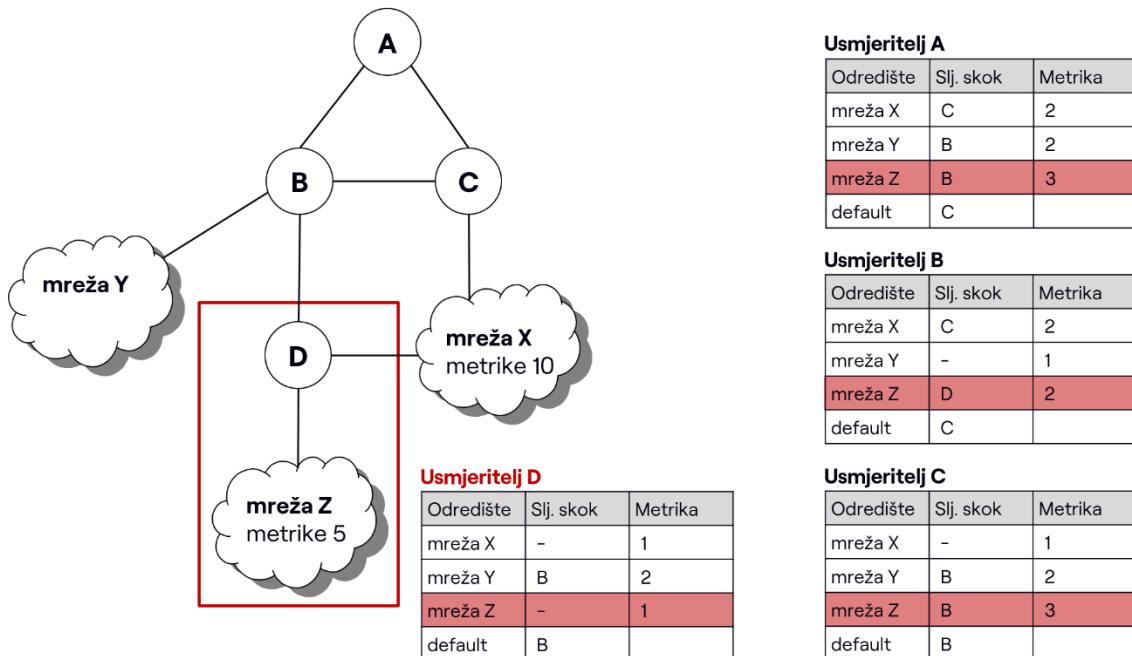
Slika 3.5 – Slanje ažuriranih tablica usmjerenja novo dodanom usmjeritelju C (korak 3)

U trećem koraku, usmjeritelji A i B šalju svoje ažurirane tablice usmjerenja susjednim usmjeriteljima: usmjeritelj A usmjeriteljima B i C, a usmjeritelj B usmjeriteljima A i C. Usmjeritelj C tako dobiva tablice usmjerenja od A i B te saznaće da je usmjeritelj B vezan izravno s mrežom Y, ažurira svoju tablicu usmjerenja i dodaje novu rutu (mreža Y, preko B, metrike 2). Od usmjeritelja A ne saznaće nikakvu novu informaciju ili bolju rutu te na temelju njegove tablice usmjerenja nema potrebe za ažuriranjem svoje tablice. U sljedećoj iteraciji usmjeritelj C šalje svoju novu tablicu usmjerenja susjedima A i B. Na taj je način proces uvođenja novog usmjeritelja i punjenja tablice usmjerenja završen. Mreža se nalazi u stabilnom stanju sve dok se dogodi neka nova promjena u mreži (slika 3.5).

Primjer 2: uvođenje novog usmjeritelja

Uvodi se usmjeritelj D koji mrežu Z povezuje s ostatkom mreže (slika 3.6). Usmjeritelj D izravno je povezan s mrežom Z i mrežom X te usmjeriteljem B. Usmjeritelj D se javlja susjednim usmjeriteljima (usmjeritelju B i izravno povezanim u mrežama X i Z) slanjem svoje tablice usmjerenja čime ih obavještava da je izravno povezan s mrežama X i Z (metrika 1).

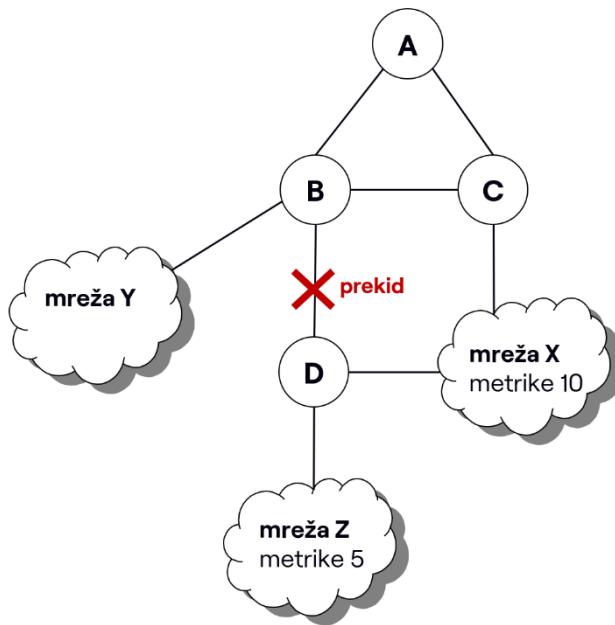
Usmjeritelj B, kada dobije informaciju od D, ažurira svoju tablicu usmjerenja i postavlja da mu je mreža Z dohvatljiva preko D s metrikom 2. U sljedećem ciklusu, B šalje svoju tablicu usmjerenja susjedima (usmjeriteljima A, C i D) te D tako dobiva informacije od B za ostatak mreže. Mreža Z je sada postala dostupna te sav promet prema njoj ide preko usmjeritelja D.



Slika 3.6 – Uvođenje novog usmjeritelja D

Primjer 3: prekid poveznice

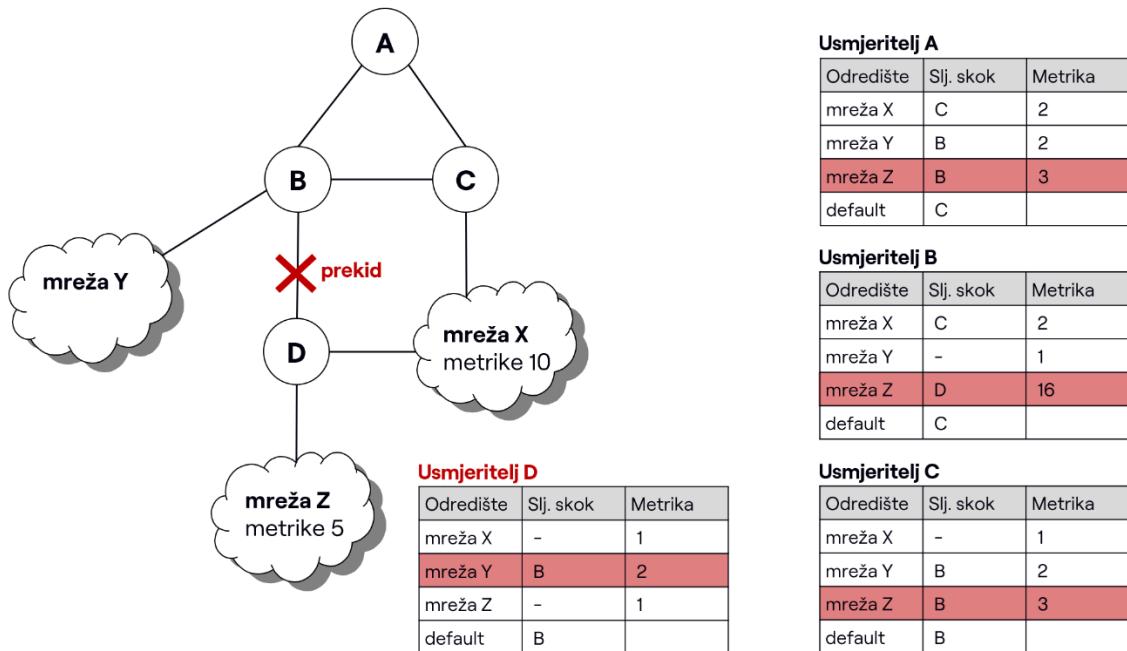
Pretpostavimo da je došlo do prekida poveznice između usmjeritelja B i D (slika 3.7a). U tom slučaju potrebno je „naučiti“ usmjeritelje da je mogući put do mreže Z preko mreže X, odnosno potrebno je usmjeriti promet preko usmjeritelja C.



Slika 3.7a – Mreža s prekidom poveznice između usmjeritelja B i D

Nakon 6 ciklusa (180 sekundi) usmjeritelj B neće dobiti tablicu usmjeravanja od D te će shvatiti da je došlo do prekida i postaviti metriku na 16 (slika 3.7b) te obavijestiti o tome susjedne usmjeritelje A i C. Kada C dobije informaciju iz mreže X da je do mreže Z metrika 11

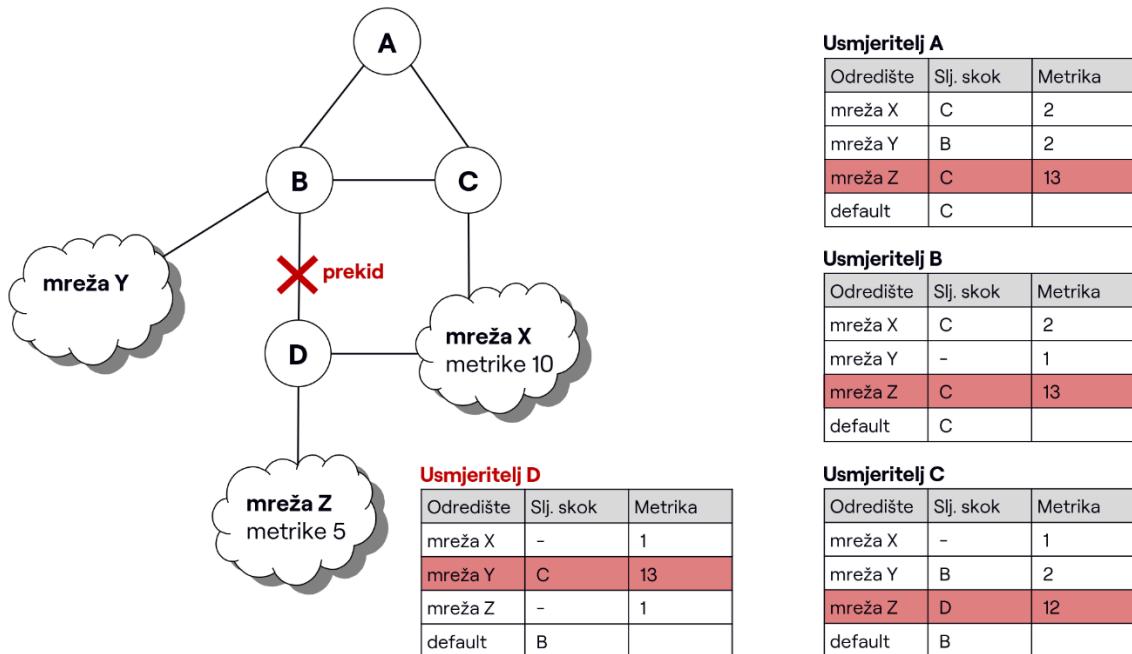
shvatit će da je to kraća ruta ($11 < 16$) i postavit će svoju metriku do mreže Z na 12, dakle preko usmjeritelja D (prvi označeni usmjeritelj), a ne više preko usmjeritelja B.



Slika 3.7b – Tablice usmjeravanja 6 ciklusa nakon prekida

Mogući problem nastaje ako usmjeritelj B prije nego što pošalje informaciju o prekidu usmjeritelju C, dobije od C informaciju da je metrika do mreže Z = 3. Postavit će rutu do mreže Z na 4 i poslati svoju tablicu usmjeritelju C. C zna da nije izravno povezan s mrežom Z i povećava metriku na 5, šalje tablicu usmjeravanja usmjeritelju B itd., sve dok C ne dobije informaciju s druge strane, od usmjeritelja mreže X (metrike 10) o kraćoj ruti. Budući da je taj put, od C do D, metrike 10, proći će 10 ciklusa da mreža „nauči“ da je to kraći put. Ovo svojstvo naziva se spora konvergencija protokola. Kad ne bi postojala alternativna ruta do mreže Z preko mreže X dogodio bi se opisani slučaj „brojanja u beskonačnost“, odnosno prošlo bi vrijeme od 16 ciklusa kako bi mreža shvatila da je stvarno došlo do prekida.

Na slici 3.8 je prikazano stanje kada se protokol stabilizira i prilagodio novonastaloj situaciji nakon prekida. Sav promet prema mreži Z sada ide preko usmjeritelja C i D, a ne više preko usmjeritelja B.



Slika 3.8 – Tablice usmjeravanja nakon prekida i konvergencije protokola

3.2.5. Proširenje protokola za rad u mreži IPv6

Većih razlika između protokola RIPv2 i nove generacije protokola RIP, RIPng⁵⁷, odnosno RIPv6, nema. Riječ je o protokolu koji koristi 128-bitne IP-adrese koji ne zahtijeva vlastite sigurnosne mehanizme već ih preuzima iz IPv6 (autentifikacija).

3.3. Protokol OSPF

Protokol OSPF (Open Shortest Path First) je protokol usmjeravanja unutar autonomnog sustava, a u uporabi je inačica OSPFv2⁵⁸. Podržava besklasno usmjeravanje, maske podmreža, rutu sljedećeg skoka, mehanizme autentifikacije, skupno razašiljanje, više paralelnih ruta (engl. *multipath routing*) te hijerarhijsko usmjeravanje koje se primjenjuje u velikim mrežama. Kod više paralelnih ruta moguće je izvoditi uravnoteženje opterećenja između ruta s jednakom težinom (metrikom).

Osnovna značajka protokola OSPF je da se kriterij odabira puta (metrika) temelji na algoritmu stanja poveznice (engl. *link-state*) kojim se za svaki usmjeritelj izračunava stablo najkraćih puteva (engl. *shortest path first tree*). Algoritam ne uzima u obzir samo topologiju mreže, nego i propusnost poveznica. Za komunikaciju usmjeritelja ne koristi se transportni protokol UDP kao kod protokola RIP, nego se OSPF-paket izravno ovija u IP-datagram. Svaki usmjeritelj održava raspodijeljenu bazu podataka sa stanjima poveznica LSDB (engl. *link state database*) iz koje gradi svoju tablicu usmjeravanja. LSDB sadrži stanja svih poveznica te zapis opisuje stanje poveznice između dvaju usmjeritelja. Svaki usmjeritelj raspolaže podacima o svim poveznicama, a ne samo onima na koje je izravno spojen.

⁵⁷ „Routing Information Protocol new generation (RIPng) for IPv6“, RFC 2080, IETF, siječanj 1997.

⁵⁸ „Open Shortest Path First Protocol Version 2“, RFC 2178, IETF, travanj 1998.

Kod usmjeravanja u velikim mrežama, mreža se unutar autonomnog sustava grupira u tzv. područja (engl. area). U skladu s tim postoji više vrsta usmjeritelja:

- usmjeritelj unutar područja usmjeravanja (engl. *internal router*, skr. IR) – nalazi se i usmjerava pakete unutar područja usmjeravanja;
- usmjeritelj na granici područja usmjeravanja (engl. *area border router*, skr. ABR) – nalazi se na granici područja usmjeravanja i usmjerava pakete između različitih područja usmjeravanja;
- usmjeritelj na granici autonomnog sustava (engl. *autonomous system boundary router*, skr. ASBR) – nalazi se na granici autonomnog sustava AS i usmjerava pakete između autonomnih sustava, tako da je riječ o usmjeritelju koji uz protokol OSPF ima implementiran i protokol za usmjeravanje između AS-ova;
- usmjeritelj na okosnici mreže (engl. *backbone router*, skr. BR) – nalazi se na granici područja usmjeravanja i više njih zajedno čine okosnicu OSPF-mreže. Obično je usmjeritelj ABR ujedno i BR jer svako područje usmjeravanja mora biti povezano na okosnicu mreže.

Osnovne operacije protokola OSPF su:

- otkrivanje susjednih usmjeritelja (engl. *neighbor discovery*),
- izbor nadležnog (engl. *designated*) usmjeritelja i pomoćnog nadležnog usmjeritelja (engl. *backup*) za svako područje usmjeravanja,
- sinkronizacija tablica usmjeravanja,
- kreiranje i održavanje tablica usmjeravanja,
- oglašavanje stanja poveznica (engl. *link state advertisement*, skr. LSA).

U komunikaciji usmjeritelja generira se mali promet budući da se poruke razmjenjuju po potrebi tj. samo pri promjeni u topologiji mreže, a ne periodički. Svi usmjeritelji unutar istog područja usmjeravanja imaju identične tablice usmjeravanja koje opisuju topologiju mreže. Pri komunikaciji usmjeritelja šalju se samo stanja pojedinih poveznica (LSA), a ne cijele tablice usmjeravanja, što opet rezultira manjim zauzimanjem mrežnih resursa. Informacije o stanju poveznica šalju se nadležnom (ili pomoćnom) usmjeritelju koji primljenu informaciju o stanju poveznica postupkom preplavljanja proslijeđuje ostalim usmjeriteljima unutar područja usmjeravanja.

Za komunikaciju sa susjednim usmjeriteljima koristi se protokol *hello* koji prigodom uvođenja novog usmjeritelja omogućuje otkrivanje susjednih usmjeritelja slanjem *hello* paketa svim susjedima. U stabilnom stanju paketi *hello* se šalju susjednim usmjeriteljima svakih 10 sekundi, tako da svaki usmjeritelj očekuje javljanje susjednih usmjeritelja što mu osigurava informaciju da je s poveznicama prema susjednim usmjeriteljima i sa samim usmjeriteljem sve u redu. Ako usmjeritelj ne primi paket *hello* unutar 40 sekundi, zaključuje da je došlo do prekida poveznice i prestaje oglašavati tu poveznicu te usmjerava novopridošle pakete drugom rutom. Ažuriranje tablica usmjeravanja vrši se postupcima sinkronizacije, odnosno oglašavanjem stanja poveznica kroz inicijalnu i kontinuiranu sinkronizaciju. Inicijalna sinkronizacija odvija se kod uvođenja novog usmjeritelja koji od svojih susjednih usmjeritelja oglašavanjem stanja poveznica dobiva informacije o stanjima poveznica u mreži. Nakon

inicijalne sinkronizacije prelazi se na kontinuiranu kod koje se oglašavaju stanja poveznica prilikom svake promjene postupkom preplavljanja kako je opisano.

3.3.1. Format zaglavlja

Slika 3.9. prikazuje zaglavje paketa OSPF. Nakon polja *verzija*, slijedi polje *tip paketa* koje označava o kojem tipu komunikacije (poruci) se radi: (1) – upoznavanje usmjeritelja (engl. *hello*), (2) – opis baze (engl. *database description*), (3) – zahtjev za stanjem poveznice (engl. *link state request*), (4) – ažuriranje stanja poveznice (engl. *link state update*), (5) – potvrda o primjeku stanja poveznice (engl. *link state acknowledgement*). U nastavku je polje u kojem je zapisana duljina paketa te zatim 32-bitna oznaka izvorišnog i odredišnog područja usmjeravanja. OSPF zaglavje podržava mehanizme sigurnosti: zaštitnu sumu i autentifikaciju (mogu se primjeniti različite sheme autentifikacije koje se zapisuju u polju *tip autentifikacije*).

0	8	16	24	31
verzija	tip paketa	Duljina paketa		
Oznaka (ID) izvornog OSPF usmjeritelja				
oznaka (ID) OSPF područja				
zaštitna suma	tip autentifikacije			
autentifikacija (64 bits)				

Slika 3.9 – Format zaglavja OSPF

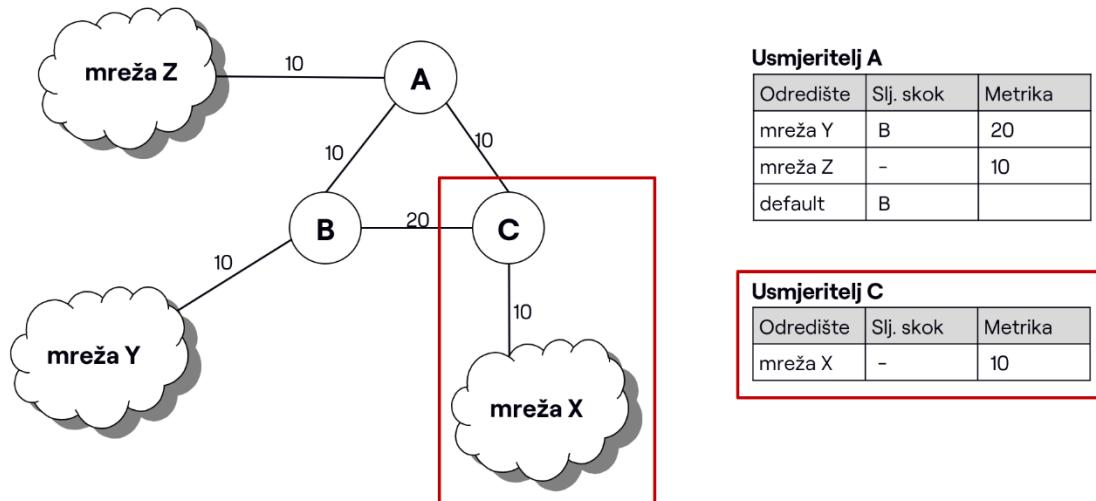
3.3.2. Primjeri rada protokola

U nastavku su dani primjeri koji ilustriraju rad protokola prilikom punjenja tablica usmjeravanja, uvođenja novog usmjeritelja te prekida veze.

Primjer 1: Uvođenje novog usmjeritelja

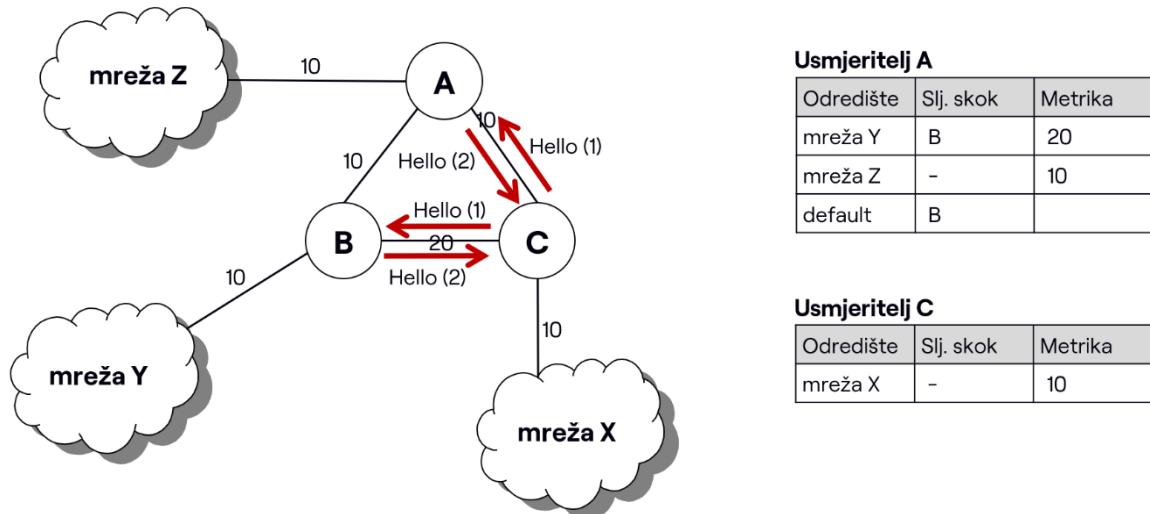
Zamislimo slučaj u kojem u mrežu uvodimo novi usmjeritelj C kako bismo mrežu X povezali s ostatkom mreže. Uvođenjem u mrežu, usmjeritelj C na početku ima praznu tablicu usmjeravanja, odnosno sadrži zapis samo o izravnoj vezi s mrežom X (slika 3.10). Metrika označava stanje poveznice dobiveno na temelju topologije (stablo najkraćih putova) i propusnosti, a manji iznos metrike predstavlja „bolju“ rutu.

Proces uvođenja novog usmjeritelja i punjenja tablice usmjeravanja je sljedeći. Usmjeritelj šalje poruku *hello* radi otkivanja susjednih usmjeritelja. Tako saznaće i adresu nadležnog usmjeritelja, koji je zadužen za njegovo područje usmjeravanja. Nakon definiranja susjeda, potrebno je napraviti sinkronizaciju tablica usmjeravanja, odnosno prikupiti podatke o rutama. Zatim se formira vlastita tablica usmjeravanja, karakteristična za dotični usmjeritelj. Na kraju se novoformirana tablica usmjeravanja oglašava kako bi se novonastalo stanje uskladilo s ostalim usmjeriteljima. Slijedi razrada opisanog procesa u nastavku.



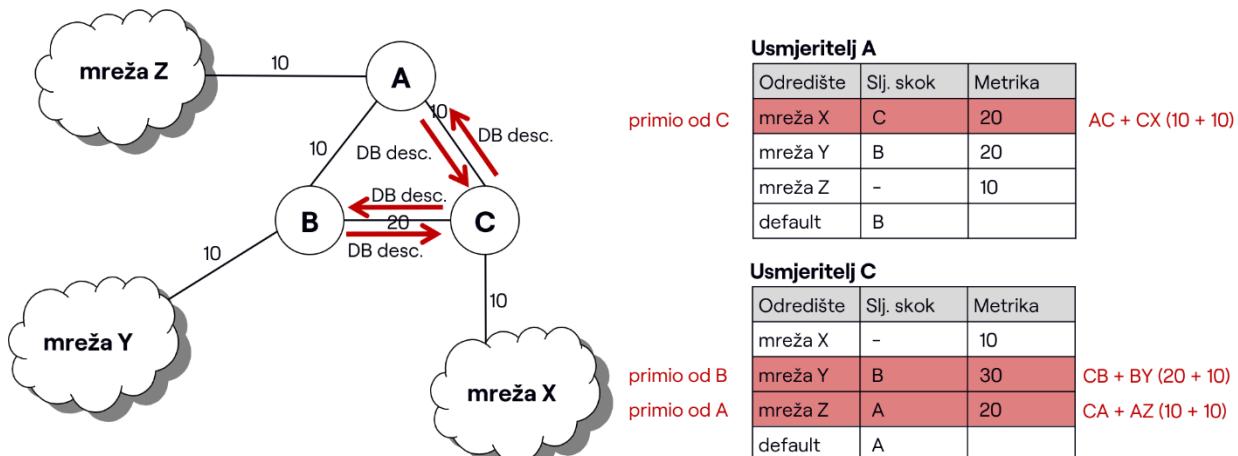
Slika 3.10 – Uvođenje usmjeritelja C u mrežu

U prvom koraku usmjeritelj C šalje pakete *Hello* susjedima (usmjeriteljima A i B). Usmjeritelji A i B primanjem paketa *Hello* od usmjeritelja C saznaju za njegovo uvođenje u mrežu. U drugom koraku usmjeritelji A i B šalju paket *Hello* svojim susjedima (prema tome i novom usmjeritelju C). Tako usmjeritelj C sazna za svoje susjedne usmjeritelje (A i B), slika 3.11.



Slika 3.11 – Upoznavanje susjednih usmjeritelja (koraci 1 i 2)

Nakon upoznavanja, treći korak podrazumijeva inicijalnu sinkronizaciju tablica usmjeravanja koja započinje razmjenom tablica usmjeravanja (između C i A te C i B). Parovi usmjeritelja (C i A te C i B) šalju zapise stanja poveznica (LSA-ove) iz svoje tablice usmjeravanja u sljedećem paketu tipa 2 (*database description*) tako da se sljedeći paket šalje tek kad je prijašnji potvrđen paketom tipa 5 (*link state acknowledgment*). Usmjeritelj A uvodi novi zapis o mreži X, a usmjeritelj C o rutama za mreže Y i Z (slika 3.12).



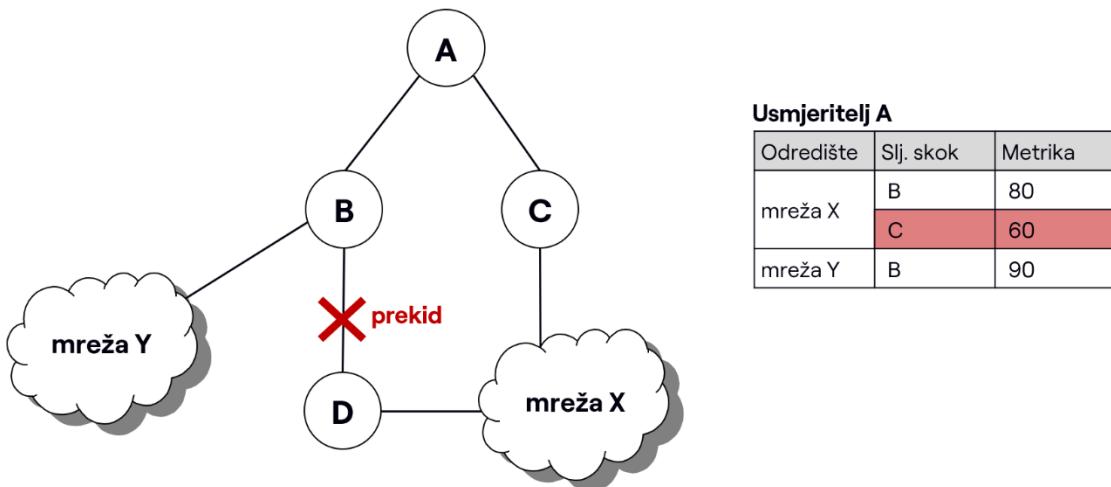
Slika 3.12 – Inicijalna sinkronizacija

U nastavku inicijalne sinkronizacije, svaki usmjeritelj šalje niz paketa *link state request* kojima zahtijeva LSA-ove koje nema ili one koje su noviji kod susjeda, a susjedni usmjeritelji odgovaraju preplavljanjem traženih LSA-ova u paketima *link state update*. Nakon što su razmijenjeni svi LSA-ovi s obje strane, inicijalna sinkronizacija je završena, a poveznica među usmjeriteljima je spremna za protok podataka.

U stabilnom stanju, izvodi se kontinuirana sinkronizacija tablica usmjeravanja preplavljanjem kada usmjeritelj želi osvježiti neki od svojih LSA-ova bilo zbog promjene nekog od lokalnih stanja (npr. prekid poveznice), bilo da želi izbrisati neki od LSA-ova. Kontinuirana sinkronizacija izvodi se slanjem LSA (jedan ili više) unutar paketa *link state update* preko svih svojih sučelja. Kad neki od susjeda primi navedeni paket, ispituje svaki LSA unutar paketa, šalje potvrdu natrag pošiljatelju, a navedeni LSA šalje u novom paketu *link state update* preko svih svojih sučelja osim onog po kojemu ga je primio. Ovo se nastavlja dok svi usmjeritelji u mreži ne dobije navedenu LSA.

Primjer 2: Prekid poveznice

Promet prema mreži X može ići preko usmjeritelja C ili usmjeritelja D, ovisno o metriци. Ako dođe do prekida veze između B i D, sav promet se do mreže X i Z usmjerava preko usmjeritelja C (slika 3.13).



Slika 3.13 – Prekid poveznice između usmjeritelja B i D

3.3.3. Proširenje protokola za rad u mreži IPv6

Nova inačica protokola OSPF za rad u mreži IPv6 je OSPFv3⁵⁹. Većina funkcionalnosti preuzeta je iz OSPFv2 tako da nema većih razlika. Svakom usmjeritelju dodjeljuje se identifikacijski broj koji zamjenjuje IPv6-adresu kako bi se izbjeglo prenošenje „dugačkih“ 128-bitnih adresa u paketima prilikom komunikacije usmjeritelja. Jedino paketi LSA sadrže IPv6-adrese. Najvažnija promjena je da su polja za autentifikaciju izbačena iz zaglavlja, jer se mehanizmi autentifikacije oslanjaju na zaglavlja AH i ESP.

3.4. Protokol BGP

Protokol BGP (*Border Gateway Protocol*) je protokol usmjeravanja između autonomnih sustava (AS), a u uporabi je inačica BGPv4⁶⁰. Osnovna mu je značajka da se temelji na algoritmu vektora staza (engl. *vector path*) koji je sličan algoritmu vektora udaljenosti, ali uzima u obzir „staze“ kao niz AS-ova na putu do odredišta. Podržava besklasno usmjeravanje i združivanje ruta (engl. *route aggregation*) kako bi se smanjila veličina tablica usmjeravanja. Za komunikaciju koristi transportni protokol TCP.

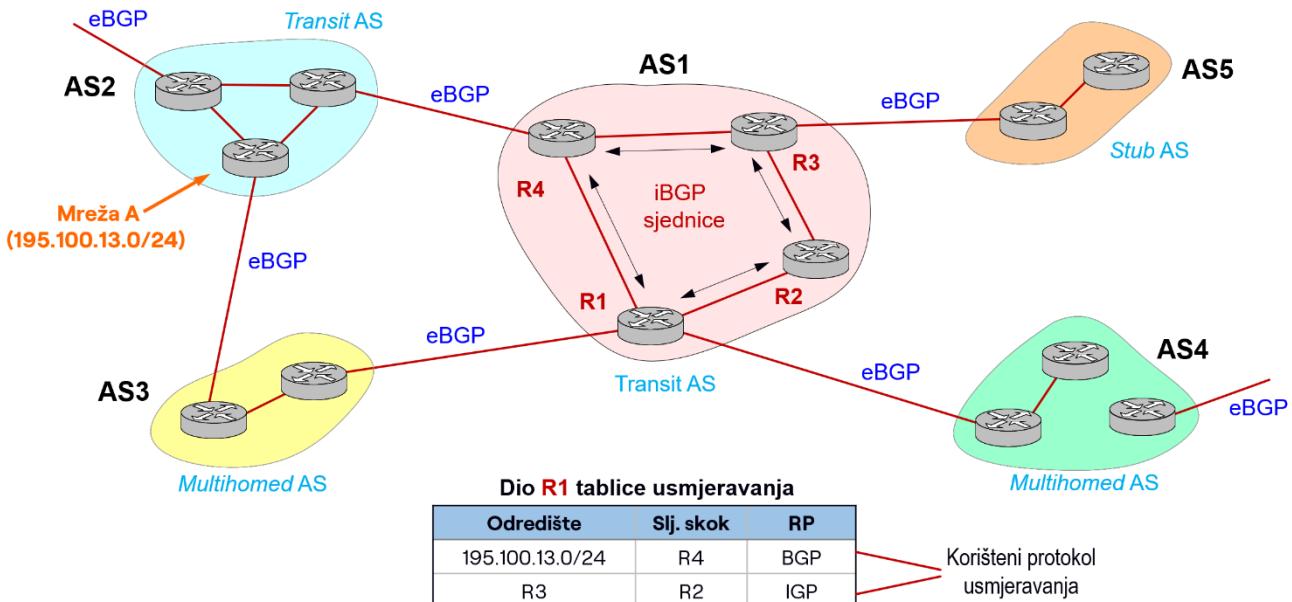
Protokol BGP može raditi kao unutarnji (engl. *internal/BGP*, skr. iBGP) i tada usmjerava pakete unutar istog AS-a ili kao vanjski (engl. *external*, skr. eBGP) koji usmjerava pakete između usmjeritelja smještenih u različitim AS-ovima. Usmjeritelji s protokolom BGP nalaze se „na rubu“ AS-a te se stoga nazivaju rubni ili vanjski (BGP) usmjeritelji. S motrišta usmjeravanja razlikuju se tri vrste AS-ova:

- *Stub AS* – AS s jednim izlazom, ima vezu sa samo jednim AS-om te prenosi samo lokalni promet;
- *Multihomed AS* – povezan je s više AS-ova, ali ne prenosi tranzitni promet;
- *Transit AS* – povezan je s više od jednog AS-a i u skladu s definiranim pravilima prenosi tranzitni i lokalni promet.

Na slici 3.14 prikazana je mreža s pet autonomnih sustava različitih vrsta. Usmjeritelji koji se nalaze u različitim AS-ovima komuniciraju protokolom eBGP, a oni koji se nalaze unutar istog AS-a komuniciraju putem protokola iBGP. Tablica usmjeravanja za usmjeritelj R1 na slici pokazuje da rubni usmjeritelj može koristiti različite protokole usmjeravanja (BGP, IGP), ovisno o odredištu. Treba napomenuti da protokol iBGP nije isto što i protokol IGP.

⁵⁹ „Open Shortest Path First Protocol for IPv6“, RFC 5340, IETF, srpanj 2008.

⁶⁰ „A Border Gateway Protocol 4“, RFC 4271, IETF, siječanj 2006.



Slika 3.14 – Usmjeritelji BGP u internetskoj mreži

Prilikom dodavanja novog usmjeritelja u mrežu, pronalazak susjednih usmjeritelja vrši se ručno od strane administratora mreže, nakon čega se uspostavlja TCP sjednica i pokreće razmjena cijelih tablica usmjeravanja, odnosno informacija o stazama (engl. *Network Layer Reachability Information*, skr. NLRI). Staza se sastoji od slijeda autonomnih sustava koje treba proći do odredišta. Za svako odredište mogu postojati višestruke staze, a dopušta se primjena različitih politika usmjeravanja za pojedina odredišta.

Svaku stazu obilježava skup parametara koji definiraju politiku usmjeravanja. Staza kojom se usmjerava paket odabire se na temelju parametara staze, dostupnosti staze, dodatnih pravila o prihvaćanju paketa (politika, sigurnost, ...), pravila o propuštanju paketa, ugovora između AS-ova te atributa o kojima će biti više riječi u nastavku.

Svaki usmjeritelj sadrži bazu staza (engl. *Routing Information Base*, skr. RIB) u kojoj se nalaze tri vrste popisa:

- popis staza koje su primljene od susjeda i uzimaju se u obzir kod procesa odlučivanja, a do tada predstavljaju tzv. neobrađene staze,
- popis staza s lokalnim informacijama o usmjeravanju do kojih se dolazi primjenom vlastitih pravila usmjeravanja i provođenjem procesa odlučivanja nad popisom tzv. neobrađenih staza primljenih od susjeda i
- popis staza koje se šalju susjednim usmjeriteljima.

3.4.1. Poruke

Komunikacija između usmjeritelja obavlja se izmjenom sljedećih poruka: *open*, *update*, *keepalive* i *notification*.

Poruka *open* šalje se kod uspostave sjednice između susjednih usmjeritelja i kod izmjene početnih postavki, kao što su identifikacija međusobnih mogućnosti i pregovaranje o

parametrima sjednice. Služi za upoznavanje usmjeritelja i poveznice između njih. Uz zaglavljje, poruka *open* sadrži sljedeća polja:

- *version* – inačica protokola BGP (BGPv4),
- *my autonomous system* – sadrži broj AS-a u kojem se nalazi pošiljatelj poruke,
- *hold time* – vremenska kontrola, definira vrijeme čekanja, dopušteno trajanje neaktivnosti nakon čega se prekida sjednica (brojač se ponovo pokreće kada dođe poruka *keepalive* ili *update*); predstavlja najveće vrijeme koje može proći između prijama dvaju uzastopnih poruka *keepalive* i/ili *update* od pošiljatelja (najmanje 3 sekunde),
- *BGP identifier* – identifikacija pošiljatelja (IP adresa usmjeritelja),
- *optional parameters length* – veličina polja *optional parameters*,
- *optional parameters* – sadrži popis izbornih parametara.

Poruka *update* omogućuje razmjenu informacija o stazama NLRI, tj. objavu novih i ukidanje zastarjelih. Oглаšavaju se staze iz baze RIB unutar popisa za slanje susjednim usmjeriteljima te se na temelju dobivenih staza ažuriraju staze i njihovi atributi. Parametri poruke su sljedeći:

- *path attributes* – sadrži popis atributa koji se ažuriraju za određene staze,
- *total path attributes length* – duljina polja *path attributes*,
- *network layer reachability information (NLRI)* – popis staza (njihovih IP-adresa) koje se najavljaju za ažuriranje,
- *withdrawn routes* – popis staza koje su najavljene, ali se neće ažurirati jer više nisu valjane,
- *total route length* – duljina polja *withdrawn routes*.

Porukom *update* može se objaviti najviše jedan skup atributa staza za više odredišta, ako ta odredišta imaju zajedničke attribute. Svi atributi staze koji se nalaze u poruci *update*, odnose se na sva odredišta koja su popisana u polju NLRI.

Poruka *keepalive* izmjenjuje se zbog održavanja sjednice između usmjeritelja, a šalje se i kao potvrda nakon poruke *open*. Uz održavanje sjednice služi za utvrđivanje dostupnosti usmjeritelja, a uobičajeno vrijeme između poruka *keepalive* je 60 sekundi, odnosno 1/3 vremena vremenske kontrole koja je obično postavljena na 180 sekundi. Nakon svakog primitka poruke *keepalive* ili *update*, ponovno se pokreće vremenska kontrola.

Poruka *notification* predstavlja obavijest o pogreškama i zatvaranju sjednice. Nakon slanja ove poruke sjednica se raskida, a razlozi mogu biti pogreške kao što su istek vremenske kontrole, primitak nepoznatog atributa, primitak pogrešnog AS broja ili neki drugi zapisan u polju *error code*.

3.4.2. Atributi

Atributi staza koji se razmjenjuju porukama *update* opisuju karakteristike staze i omogućavaju usmjeriteljima primjenu vlastite politike usmjeravanja. Dijelimo ih u četiri kategorije: (dobro poznati) obvezni (engl. *well-known mandatory*), (dobro poznati) neobvezni (engl. *well-known discretionary*), izborni tranzitni (engl. *optional transitive*) koji se

odnose na sve AS-ove (globalni) te izborni lokalni (engl. *optional non-transitive*) koji se odnose na AS koji ih prima. Svaka staza može imati jedan ili više izbornih atributa kao dodatak dobro poznatim atributima. Atributi su *origin*, *AS-path*, *next-hop*, *multi-exit discriminator* (MED), *local preference*, *atomic aggregate* i *aggregator*.

Atribut *origin* je obvezni atribut koji definira porijeklo staze. Postavlja ga usmjeritelj od kojeg staza potječe, a može imati oznaku da potječe iz istog ili različitog AS-a, ili da porijeklo staze nije poznato.

Atribut *AS-path* je obvezni atribut koji sadrži listu AS-ova koje treba proći do odredišta. Koristan je kod višestrukih staza (za isto odredište), a služi i za izbjegavanje petlji, preferiranje određene staze (kroz odabrane AS-ove) kao i za filtriranje, odnosno zabranu usmjeravanja paketa kroz određene AS-ove.

Atribut *next-hop* je također obvezni atribut koji definira adresu usmjeritelja na koji se prvo usmjerava paket prema odredištu (sljedeći skok).

Atribut *MED* je izborni lokalni višeizlazni diskriminirajući atribut koji služi za odabir jedne od više ponuđenih staza prema istom AS-u. Pomoću njega usmjeritelji savjetuju svoje susjede kojim putem poslati pakete prema njima, a preferira se put prema vlastitom AS-u.

Atribut *local preference* je neobvezni atribut koji se izmjenjuje između lokalnih usmjeritelja unutar AS-a. Određuje politiku usmjeravanja odlaznog prometa AS-a i ne utječe na ostale AS-ove.

Atribut *atomic aggregate* je također neobvezni atribut koji predstavlja združenu stazu do odredišta. Združivanje staza omogućava da više staza sa svojim karakteristikama može biti objavljeno kao jedna u svrhu reduciranja broja staza.

Atribut *aggregator* je izborni tranzitni atribut koji daje do znanja da je usmjeritelj združio stazu te zapisuje svoj AS-broj i IP-adresu. Združivati se mogu samo staze koje imaju iste attribute. U nastavku je dan primjer združivanja.

Primjer 1: združena staza

Potrebito je pronaći združenu stazu za sljedeće adrese (staze):

192.168.98.0	(11000000.10101000.01100010.00000000)
192.168.99.0	(11000000.10101000.01100011.00000000)
192.168.100.0	(11000000.10101000.01100100.00000000)
192.168.102.0	(11000000.10101000.01100110.00000000)
192.168.104.0	(11000000.10101000.01101000.00000000)
192.168.105.0	(11000000.10101000.01101001.00000000)
192.168.96.0	(11000000.10101000.01100000.00000000)

Do združene staze dolazi se tako da se odredi *najmanja* adresa koja obuhvaća sve navedene adrese (logičko „I“). Dobiva se adresa (združena staza) 192.168.96.0/20 s maskom podmreže 255.255.240.0. Kako navedeno rješenje sadrži i staze koje ne pripadaju združenoj stazi kao

što su 192.168.96.0, 192.168.97.0, 192.168.101.0 i 192.168.103.0, prve dvije se mogu isključiti jer ne pripadaju združenoj stazi, pa uzimamo prvu adresu koja joj pripada: 192.168.98.0/20.

3.4.3. Algoritam odabira staze

Algoritam odabira staze odlučuje o „najboljoj stazi“ za zadano odredište na temelju procesa odlučivanja. Nema definiranog pravila već se primjenjuje vlastita politika određena od strane administratora AS-a. Promatraju se neobrađene staze objavljene u bazi staza RIB, a u obzir se mogu uzimati svi ili samo neki atributi. U nastavku je dan primjer donošenja odluke o stazama.

- Odaber stazu s najvećom vrijednosti atributa *local preference*. Ako se put ne može odrediti na temelju ovog kriterija prijeđi na sljedeći korak;
- Odaber stazu koja je domaćeg porijekla (*origin*), dobivena iz vlastitog AS-a. Ako se staza ne može odrediti na temelju ovog kriterija prijeđi na sljedeći korak;
- Odaber stazu s najkraćim atributom *AS path*. Ako se staza ne može odrediti na temelju ovog kriterija prijeđi na sljedeći korak;
- Odaber stazu s manjom vrijednosti atributa *origin*. Ako se staza ne može odrediti na temelju ovog kriterija prijeđi na sljedeći korak;
- Odaber stazu s najmanjim atributom *MED*. Ako se staza ne može odrediti na temelju ovog kriterija prijeđi na sljedeći korak;
- Odaber stazu koja je definirana na temelju eBGP.

U nastavku je dan primjer odabira staze.

Primjer 2: odabir staze

Za primjer na slici 3.15 iz mreže B (usmjeritelj R5, AS3) do mreže A (AS5) može se doći različitim stazama. Uzmimo u obzir sljedeće tri staze:

- staza AS3 – AS2 – AS5,
- staza AS3 – AS1 – AS5,
- staza AS3 – AS4 – AS1 – AS5.

Kako bi se odabrala „najbolja“ staza potrebno je primijeniti algoritam odabira staze. Odabrana staza će se zapisati u tablicu usmjeravanja usmjeritelja R5 i po njoj će se usmjeravati paketi.

Prepostavimo da se proces donošenja odluke o (najboljoj) stazi temelji na algoritmu opisanom na početku ovog poglavlja te da su atributi staza sljedeći:

Atributi staze 1

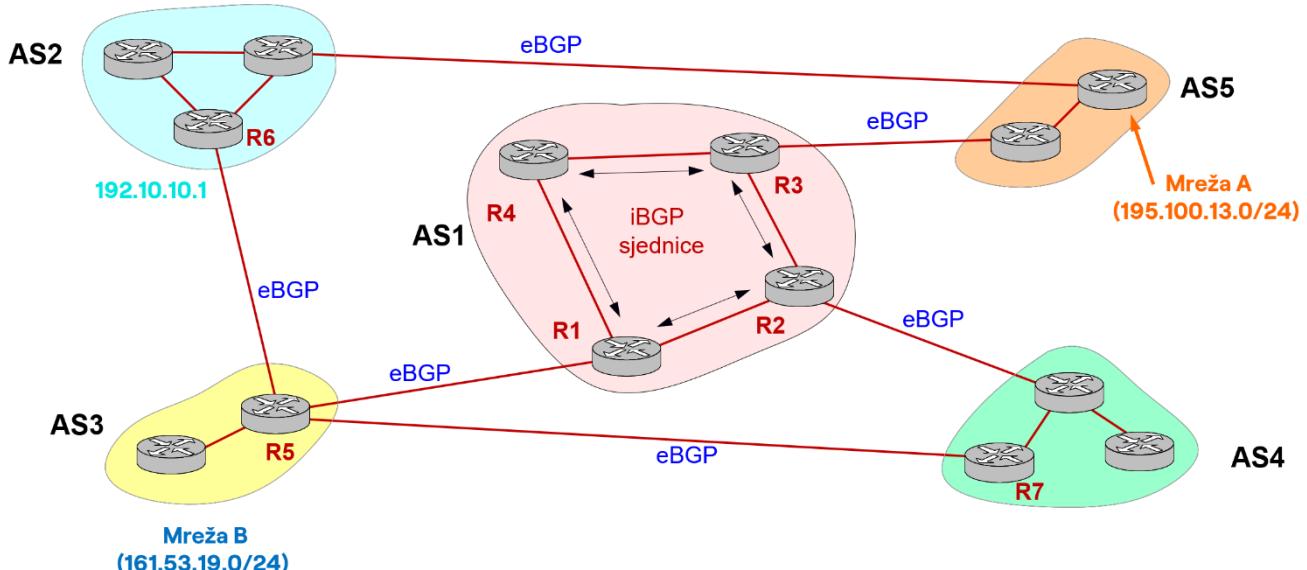
- *Origin*: IGP-0
- *AS path*: AS2 – AS5
- *Local preference*: 3
- MED: 1

Atributi staze 2

- *Origin*: IGP-0
- *AS path*: AS1 – AS5
- *Local preference*: 3
- MED: 2

Atributi staze 3

- *Origin*: IGP-0
- *AS path*: AS4 – AS1 – AS5
- *Local preference*: 3
- MED: 3

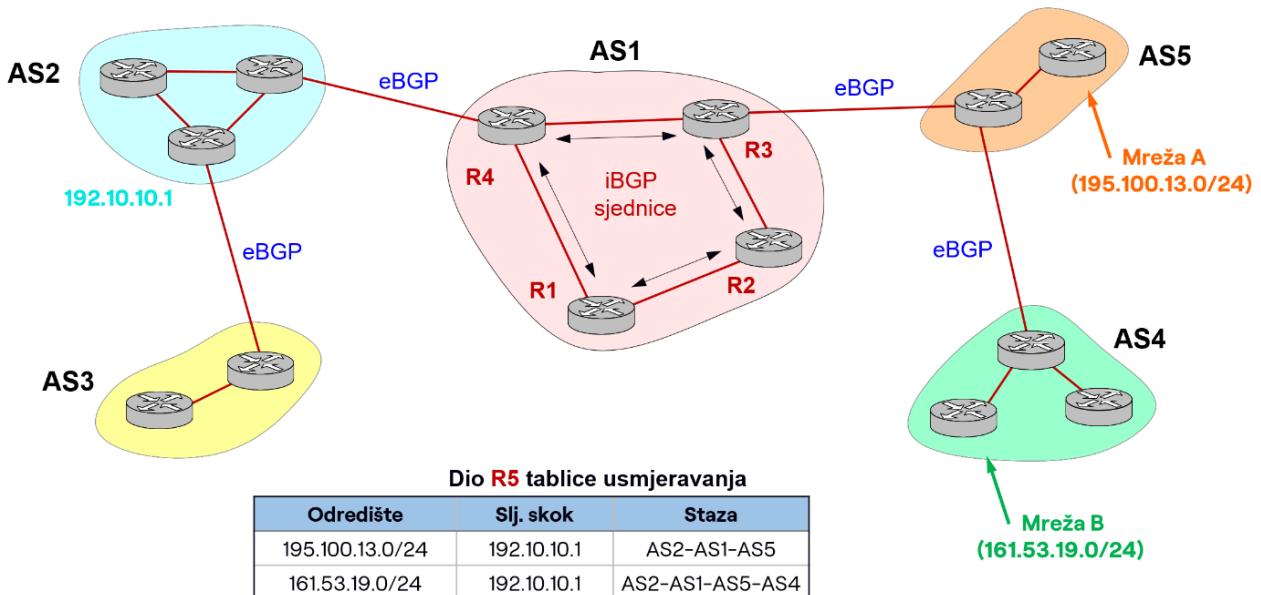


Slika 3.15 – Primjer mreže za odabir staze na temelju atributa

U tom slučaju, prema algoritmu, prvo se za sve tri staze gleda atribut *local preference*. Kako u ovom slučaju on ima istu vrijednost za sve tri staze, prelazi se na sljedeći kriterij, porijeklo puta, odnosno atribut *origin*. Kako su sve ponuđene staze domaćeg porijekla, prelazi se na sljedeći kriterij, duljinu staze (*AS path*). Ovim kriterijem otpada staza 3 jer je ona najduža. Iz preostale dvije staze gleda se vrijednost atributa *origin*, a kako se opet na temelju njegove vrijednosti ne može odrediti "bolji" put, promatra se atribut MED po kojem je odabrana staza 1, budući da ima manju vrijednost atributa MED. Dakle staza koja se upisuje u tablicu usmjeravanja usmjeritelja R5 za odredišni AS5 je *AS path* = AS2 – AS5 s atributom *next-hop* = R6.

Primjer 3: tablica usmjeravanja

Na slici 3.16 prikazana je mreža s pet autonomnih sustava te dio tablice usmjeravanja usmjeritelja R5 u kojoj se nalaze dva zapisa za dvije odredišne mreže. Uz svako odredište u tablici usmjeravanja nalazi se informacija o sljedećem skoku i stazi (nizu AS-ova na putu do odredišta).



Slika 3.16 – Tablica usmjeravanja protokolom BGP

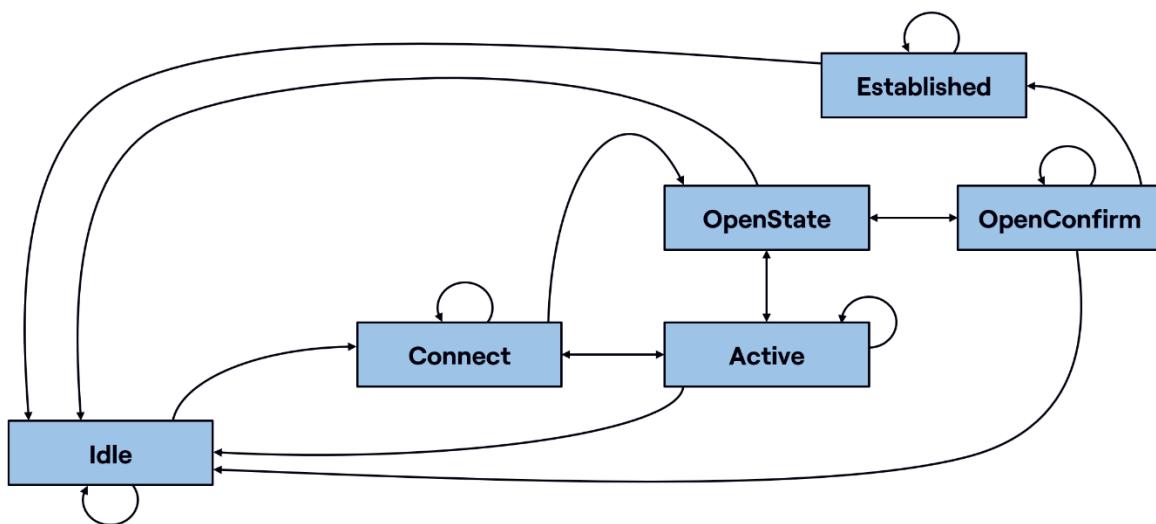
3.4.4. Komunikacija usmjeritelja

Komunikacija BGP-usmjeritelja u internetskoj mreži može se predočiti modelom konačnog automata (slika 3.17) sa šest stanja⁶¹: *Idle*, *Connect*, *Active*, *OpenSent*, *OpenConfirm* i *Established*.

Svaki BGP-usmjeritelj se inicijalno nalazi u stanju *Idle* u kojem inicijalizira resurse i pokreće uspostavu TCP-sjednica sa susjednim usmjeriteljima. Ako dođe do bilo kakve pogreške (pogrešna TCP-vrata, kriva konfiguracija adrese ili broja AS-a) usmjeritelj prekida sjednicu i vraća u stanje *Idle*.

U stanju *Connect* usmjeritelj se kratko nalazi dok se ne uspostavi TCP-sjednica sa susjednim usmjeriteljem i tada prelazi u stanje *OpenSent*. Ako se TCP-sjednica iz nekog razloga ne može uspostaviti, odlazi u stanje *Active* te nakon određenog vremena u stanje *Idle*. Ako se sjednica uspostavi, prelazi u stanje *OpenConfirm* gdje očekuje poruku *keepalive*, kao potvrdu usmjeritelja da je primio valjanu poruku *open*. U slučaju pogreške prima poruku *notification* i vraća se u početno stanje *Idle*. Ako je poruka *keepalive* primljena unutar predviđenog vremena (vremenska kontrola nije istekla) usmjeritelj konačno prelazi u stanje *Established*, a ako nije, šalje poruku *notification* te se vraća početno stanje *Idle*. U stanju *Established* izmjenjuju se poruke *update*, *notification* i *keepalive* s usmjeriteljem s kojim je uspostavljena veza kako je već objašnjeno. Nakon primitka poruke *notification* ili bilo kakve druge pogreške, vraća se u početno stanje *Idle*.

⁶¹ „BGP-4 Protocol Analysis“, RFC 4274, IETF, siječanj 2006.



Slika 3.17 – Model konačnog automata protokola BGP

3.4.5. Regionalni internetski register

Regionalni internetski registar (engl. *Regional Internet Registry*, skr. RIR) vrši raspodjelu brojeva AS-a i IP adresa dobivenih od IANA (*Internet Assigned Number Authority*). Aktivno je pet registara s područjem djelovanja: RIPE NCC (*RIPE Network Coordination Centre*), nadležan za Europu, Bliski Istok i središnja Aziju, ARIN (*American Registry for Registry Numbers*), nadležan za Sjevernu Ameriku i dijelove Kariba, APNIC (*Asia-Pacific Network Coordination Centre*), nadležan za Aziju i Tih ocean, LACNIC (*Latin American and Caribbean Internet Address Registry*), nadležan za Latinsku Ameriku i Karibe te AfriNIC (*African Network Information Centre*) nadležan za Afriku.

Čelna svjetska organizacija (IANA) koja raspolaže IP adresama sa sjedištem u Los Angelesu u SAD-u dijeli adrese RIR-ovima, a RIR-ovi dalje adrese dodjeljuju nacionalnim internetskim registrima (engl. *National Internet Registry*, NIR) ili izravno ISP-ovima ili lokalnim internetskim registrima (engl. *Local Internet Registry*, LIR). NIR postoji samo u APNIC-u.

CARNet kao i ostali davatelji internetskih usluga (ISP) u RH spadaju pod nadležnost RIPE NCC. CARNet je lokalni internetski registar (LIR) kao i ostali davatelji internetskih usluga koji dijeluju u Hrvatskoj.

CARNet upravlja s 164.092 IP-adrese.

- 82.132.0. 0 – 82.132.127.255 (/17), 32767 adresa
 - 161.53.0.0 – 161.53.255.255 (/16), 65535 adresa
 - 192.84.105.0 – 192.84.105.255 (/24), 255 adresa
 - 193.198.0.0 – 193.198.255.255 (/16), 65535 adresa

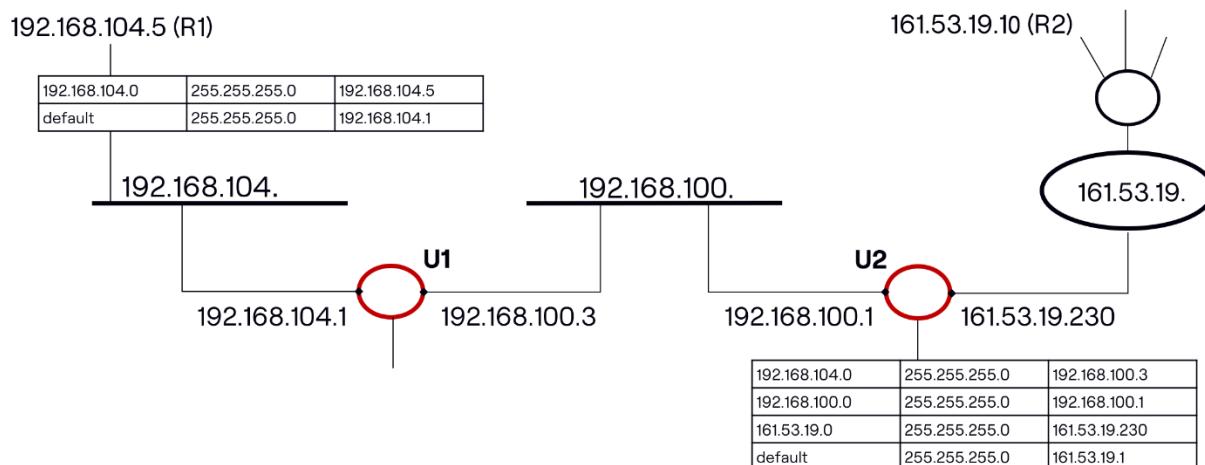
Unutar Hrvatske, CARNet povezuje sve veće hrvatske gradove, i to na nekoliko razina različitih tehnologija i pristupnih brzina. Okosnica mreže povezuje veće sveučilišne centre (Dubrovnik, Osijek, Pula, Rijeka, Split, Zadar, Zagreb) brzinama od 100 Mbit/s do 1 Gbit/s, dok

su za manje centre osigurane veze brzina od 2 Mb/s do 100 Mb/s. Mreža u Zagrebu i Splitu povezuje veće fakultete i znanstvene ustanove brzinama do 10 Gbit/s⁶².

CARNet ostvaruje vezu s Internetom preko pan-europske istraživačke mreže GÉANT brzinom 10 Gbit/s. Veza prema drugim ISP-ovima u Hrvatskoj ostvarena je kroz mjesto razmjene internetskog prometa u Hrvatskoj, *Croatian Internet eXchange (CIX)*⁶³. CIX je otvoren za sve ISP-ove u RH, kako za komercijalne tako i nekomercijalne, odnosno privatne mreže. Uspostavom izravnih komunikacijskih kanala među hrvatskim ISP-ovima postiže se velika ušteda u razmjeni podataka među hrvatskim internetskim korisnicima jer izravno međusobno povezivanje ISP-ova smanjuje nepotrebni promet kroz treće mreže. CIX članice dogovaraju međusobni način izmjene prometa (engl. *peering*).

3.5. Zadaci

1. Koja je uloga usmjeritelja u internetskoj mreži?
2. Koja su polja u IP-zaglavlju važna za usmjeravanje datagrama?
3. Koje su osnovne značajke protokola RIP?
4. Navedite nedostatke protokola RIP i kako se oni rješavaju?
5. Za mrežu na slici 3.18 računalo R1 s IP-adresom 192.168.104.5 želi poslati podatke računalu R2 s IP-adresom 161.53.19.10. Opišite postupak usmjeravanja!

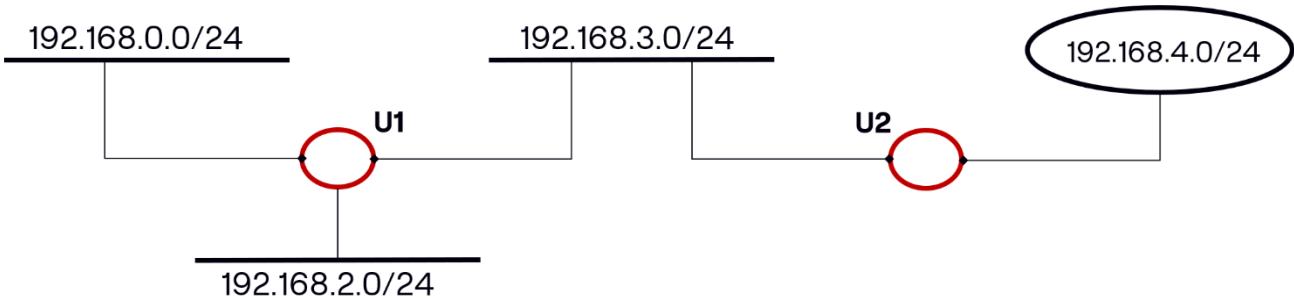


Slika 3.18 – Primjer mreže s usmjeriteljima i tablicama usmjeravanja

6. Izradite tablice usmjeravanja za usmjeritelje U1 i U2 za mrežu prema slici 3.19.

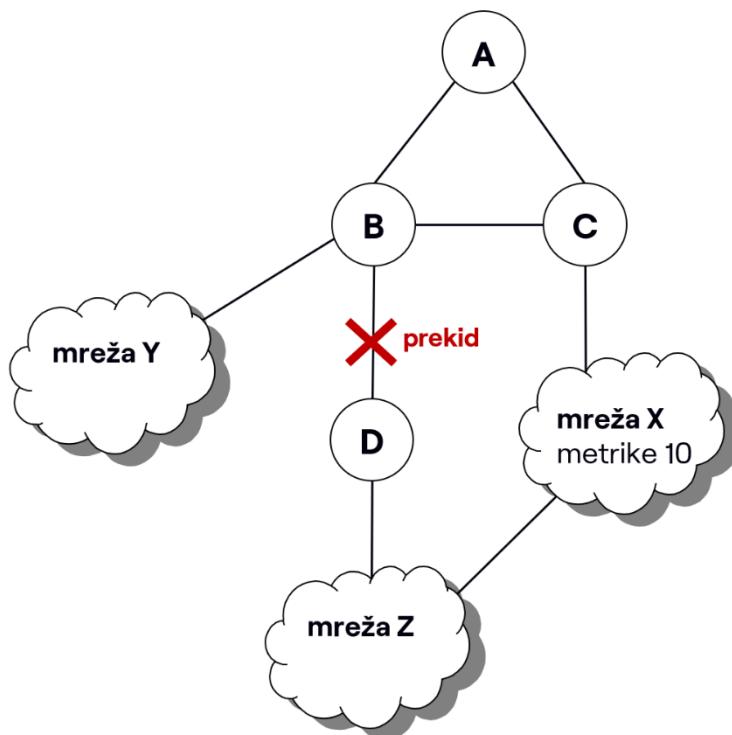
⁶² http://www.carnet.hr/o_carnetu/carnet_infrastruktura

⁶³ "Croatian Internet Exchange CIX", <http://www.cix.hr>



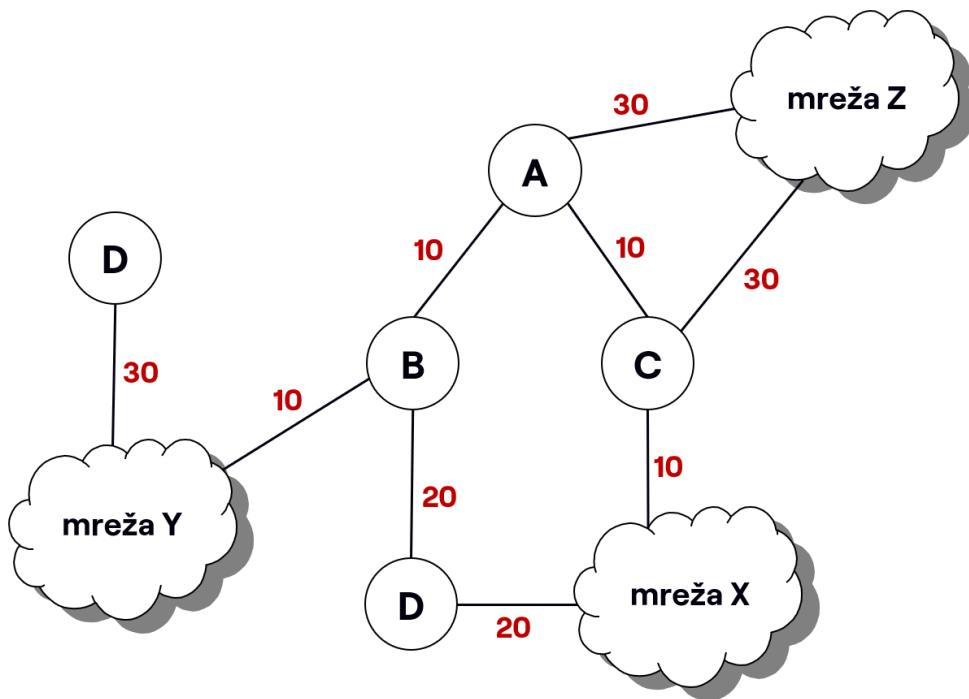
Slika 3.19 – Primjer mreže s praznim tablicama usmjeravanja

7. Na svom računalu spojenom na Internet (PC-u s operacijskim sustavom Windows) u komandnoj liniji (`cmd`) naredbom `route print` ili `netstat -r` ispišite i analizirajte tablicu usmjeravanja za protokole IPv4 i IPv6. Koje se naredbe koriste za promjenu, dodavanje i brisanje rute u tablici usmjeravanja na računalu?
8. Objasnite slučaj kada u mreži prema slici 3.20 dođe do prekida između usmjeritelja B i D te B dobije tablicu usmjeravanja od A prije nego što o novonastalom prekidu obavijesti usmjeritelja A! Što će se dogoditi?



Slika 3.20 – Primjer prekida u mreži

9. U čemu su slični, a u čemu različiti protokoli RIPv2 i RIPng?
10. Koje su osnovne značajke protokola OSPF?
11. Navedite operacije protokola OSPF.
12. Za primjer na slici 3.21 odredite bazu stanja poveznica LSDB za cijelu mrežu te tablice usmjeravanja usmjeritelja A, B, C, D i E koji koriste protokol OSPF!



Slika 3.21 – Primjer određivanja najkraćeg puta

13. U čemu su slični, a u čemu različiti protokoli OSPFv2 i OSPFv3?
14. Usporedite protokol OSPF s protokolom RIP.
15. Koje su osnovne značajke protokola BGP?
16. Koje se poruke izmjenjuju između usmjeritelja BGP?
17. Navedite atribute staza i objasnite njihovu ulogu.
18. Usmjeritelj ima zapisan združeni put $10.10.1.32/27$. Pripada li združenom putu adresa $10.10.1.44/27$? Pripada li združenom putu adresa $10.10.1.90/27$? Objasnite!
19. Kako se obavlja ažuriranje tablice usmjeravanja kod BGP-usmjeritelja?
20. Zašto se koriste različiti protokoli kod usmjeravanja unutar i između autonomnih sustava?

4. Signalizacijski protokoli u Internetu

Pružanje interaktivnih usluga, kao što su govorna komunikacija ili videokonferencija zahtijeva uspostavu sjednice između točaka na koje su priključeni korisnici i komunikaciju u stvarnom vremenu s određenom kvalitetom usluge. Protokol IP (IPv4 i IPv6) sam to ne omogućuje, već su potrebni posebni signalizacijski protokoli.

Uvođenjem signalizacijskih protokola u internetsku mrežu odvaja se podatkovni tok (npr. govor, video) od toka upravljačkih informacija kojim se uspostavlja sjednica te osigurava komunikacija u stvarnom vremenu i interaktivnost sudionika u komunikaciji. Primjeri usluga koje su tako riješene su prijenos govora Internetom (engl. *voice over IP*, VoIP) ili internetska telefonija (engl. *Internet telephony*), videokonferencija i slično. Prijenos podataka za takve usluge je „problematičan“ jer protokol IP dostavlja datagrame na odredište na načelu „najbolje moguće“ s obzirom na uvjete u mreži, tj. najbrže, s najmanjim mogućim kašnjenjem, ali bez ikakvih jamstava za kvalitetom usluge koju može narušiti preveliko kašnjenje, promjena kašnjenja i gubitak paketa koji prenose govor ili video.

Najznačajniji signalizacijski protokol za ostvarivanje stvarnovremenih interaktivnih usluga u IP-mreži je protokol SIP (*Session Initiation Protocol*)^{64,65}. Protokol SIP je protokol aplikacijskog sloja koji služi za pokretanje, održavanje, promjenu i raskid sjednice s jednim ili više sudionika. Primjenjuje se za govornu komunikaciju (VoIP)⁶⁶ i druge usluge. Za istu svrhu se još koriste i (stariji) protokoli kao što su H.323⁶⁷, MGCP (*Media Gateway Control Protocol*)⁶⁸ i TRIP (*Telephony Routing over IP*)⁶⁹.

Prijenos paketa s govorom i videom obično se ostvaruje protokolom RTP (*Real-time Transport Protocol*)⁷⁰ u aplikacijskom sloju koji je namijenjen strujanju medija, jer omogućuje kompenzaciju kolebanja kašnjenja i otkrivanje poremećaja slijeda podataka. Većina izvedbi RTP-a koristi UDP kao transportni protokol.

Uz navedene, postoje protokoli koji omogućavaju prijenos protokolom IP signalizacijskih protokola korištenih u kanalskim mrežama (PSTN, GSM). Najznačajniji je skup protokola SIGTRAN (*Signalling Transport*) za prijenos signalizacije SS7 (*Signalling System No. 7*) mrežom IP (SS7 over IP), a tu su još protokol BICC (*Bearer Independent Control Call*) za prijenos signalizacije SS7 ISUP (*ISDN User Part*) mrežom IP i drugi.

4.1. Protokol SIP

Protokol SIP je signalizacijski protokol aplikacijskog sloja koji služi za upravljanje sjednicom između dvaju ili više sudionika. Koristi protokole TCP i UDP na transportnom sloju (slika 4.1).

⁶⁴ „SIP: Session Initiation Protocol“, RFC 3261, IETF, lipanj 2002.

⁶⁵ „A Hitchhiker's Guide to the Session Initiation Protocol (SIP)“, RFC 5411, IETF, veljača 2009.

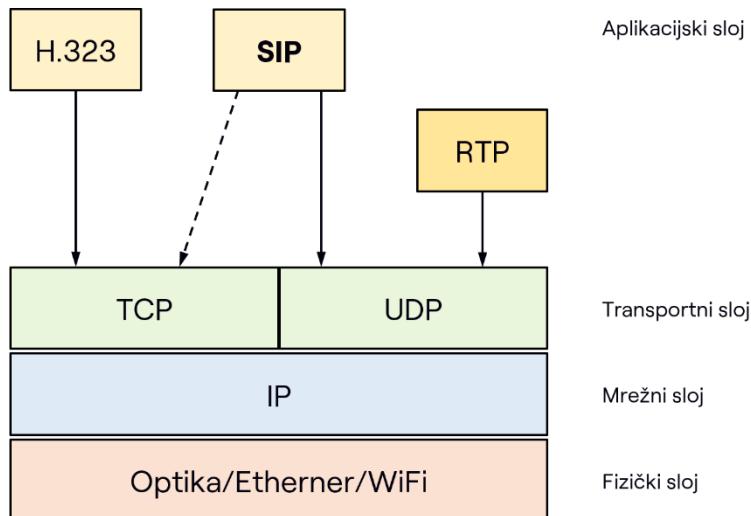
⁶⁶ „Voice over IP (VoIP) SIP Peering Use Cases“, RFC 6405, IETF, studeni 2011.

⁶⁷ „Packet-based multimedia communications systems“, ITU-T Recommendation H.323

⁶⁸ „Media Gateway Control Protocol (MGCP)“, RFC 3435, IETF, siječanj 2003.

⁶⁹ „Telephony Routing over IP (TRIP)“, RFC 3219, IETF, siječanj 2002.

⁷⁰ „RTP: A Transport Protocol for Real-time Applications“, RFC 3550, IETF, srpanj 2003.



Slika 4.1 – Protokol SIP u protokolnom stogu

Uspostava i upravljanje sjednicom provodi se posredstvom protokola TCP, dok se prijenos medija (podataka) obično provodi protokolom UDP, no to ovisi o samoj usluzi, njezinoj izvedbi i vrsti medija koji se prenosi. Ako je riječ o usluzi prijenosa govora (VoIP) koja zahtijeva komunikaciju u stvarnom vremenu, koristi se transportni protokol UDP. Razlog tomu je što protokol TCP kod izgubljenih paketa traži retransmisiju koja uvodi neprihvatljiva kašnjenja: za stvarnovremene usluge prihvatljivije izgubiti paket nego čekati na njegovu retransmisiju.

Protokol SIP koristi se u izvedbi različitih internetskih usluga kao što su usluga prisutnosti (engl. *presence*) i trenutno poručivanje (engl. *instant messaging*). Pruža podršku za pokretljivost na aplikacijskom sloju:

- pokretljivost uređaja/terminala (engl. *terminal mobility*) – uređaj mijenja položaj i/ili pristupnu točku u mreži;
- pokretljivost osobe (engl. *personal mobility*) – osoba koristi različite uređaje za pristup uslugama;
- pokretljivost usluge (engl. *service mobility*) – pristup uslugama neovisan o promjeni uređaja i/ili mreže;
- pokretljivost sjednice (engl. *session mobility*) – korisnik mijenja uređaje za vrijeme odvijanja komunikacije.

Osnovne značajke protokola SIP su:

- pronalaženje korisnika u mreži radi uključivanja u sjednicu,
- održavanje i razmjenjivanje podataka/parametara o sjednici (pregovaranje o sjednici),
- mijenjanje parametara sjednice,
- upravljanje sudionicima u sjednici – upućivanje poziva korisniku za sudjelovanje u sjednici te
- raskidanje sjednice s korisnikom.

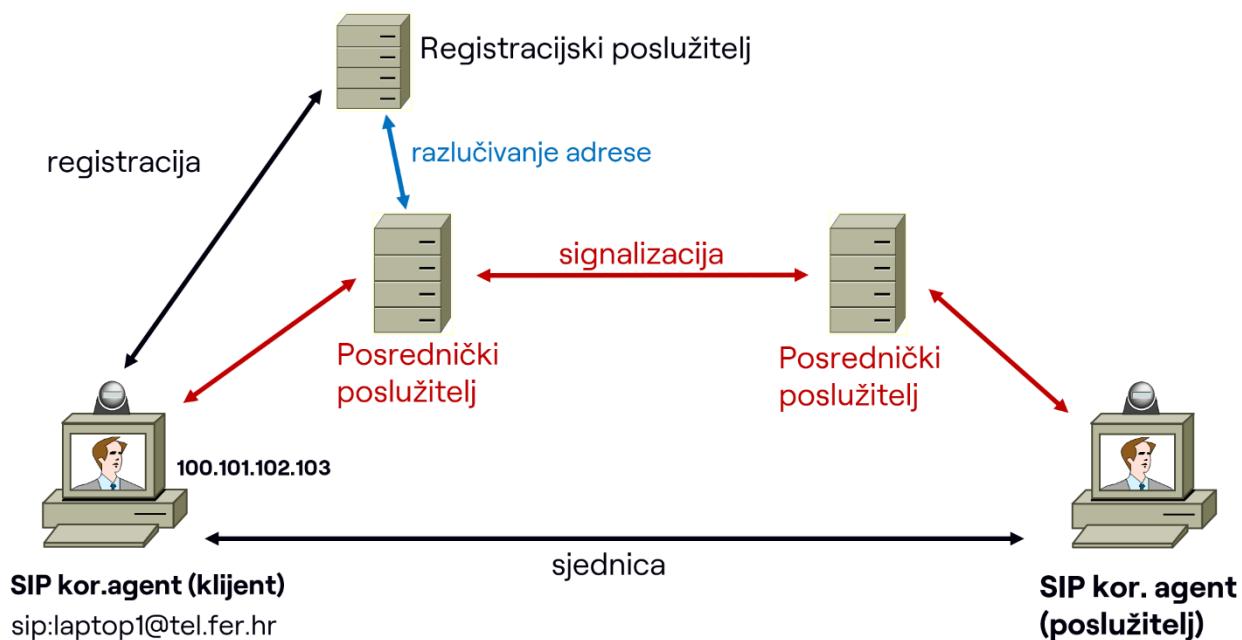
Osnovna svrha protokola je omogućiti osobnu pokretljivost korisnika i raspozнати korisnika u mreži putem jedinstvene adrese, neovisne o trenutnom položaju.

Mrežna arhitektura izgrađena je od dvije osnovne komponente: korisničkog agenta (engl. user agent, UA) i mrežnog poslužitelja i uključuje sljedeće mrežne entitete:

- korisnički agenti s klijentske (engl. *user agent client*, UAC) i poslužiteljske (engl. *user agent server*, UAS) strane koji se nazivaju SIP-klijenti. UAC je odgovoran za generiranje zahtjeva, a UAS za odgovore na zahtjeve. Nalaze se na klijentskim uređajima, uglavnom u obliku aplikacija;
- posrednički poslužitelji (engl. *proxy server*) koji primaju i prosleđuju SIP-poruke od korisničkog agenta ili drugog posredničkog poslužitelja prema odredištu. Posrednički poslužitelj može generirati zahtjeve drugim poslužiteljima ili klijentima;
- registracijski poslužitelj (engl. *registrar server*) koji registrira korisnike unutar domene, prihvata zahtjeve za registraciju i održava podatke o korisnicima i njihovim trenutnim lokacijama (njihove trenutne IP adrese) unutar domene s ciljem ispravnog usmjeravanja zahtjeva. Najčešće se postavlja zajedno s poslužiteljem za preusmjeravanje ili posredničkim poslužiteljem;
- poslužitelja za preusmjeravanje (engl. *redirect server*) koji prihvata zahtjeve za uspostavom sjednice i vraća popis svih mogućih adresa korisnika na temelju podataka iz registra. Ne može poslati zahtjev, niti kao UA uspostaviti vezu.

Poslužitelji nisu neophodni za uspostavu sjednice između dva korisnika, međutim oni nude dodatne funkcionalnosti i zbog toga se uvijek koriste. Za otkrivanje lokacije korisnika u mreži koriste se lokacijski poslužitelji (engl. *location server*) koji sadrže informacije o trenutnoj lokaciji korisnika.

Slika 4.2 prikazuje mrežnu arhitekturu protokola SIP, međudjelovanje mrežnih elemenata te uspostavu sjednice između klijenta i poslužitelja. U komunikaciji sudjeluju posrednički poslužitelji tako da se sva komunikacija odvija preko njih.



Slika 4.2 – Mrežna arhitektura protokola SIP

Za adresiranje i identifikaciju elemenata koristi se URI (*Uniform Resource Indicator*) u uobičajenom formatu *ime@domena* ili točnije:

[sip:]<user>@(<host>|<domain>).

Primjer SIP-adrese je *sip:racunalo@tel.fer.hr*. Korisnički dio adrese je ime korisnika ili telefonski broj. *Host* je naziv domene ili numerička adresa računala na kojem se korisnik nalazi. U većini slučajeva korisnički dio adrese može se prepostaviti iz e-mail adrese ili imena korisnika.

Pronalaženje posredničkog poslužitelja može se provesti na dva načina: pokušajem izravne uspostave veze na temelju *host* dijela adrese ili proslijđivanjem zahtjeva na prvi registrirani posrednički poslužitelj.

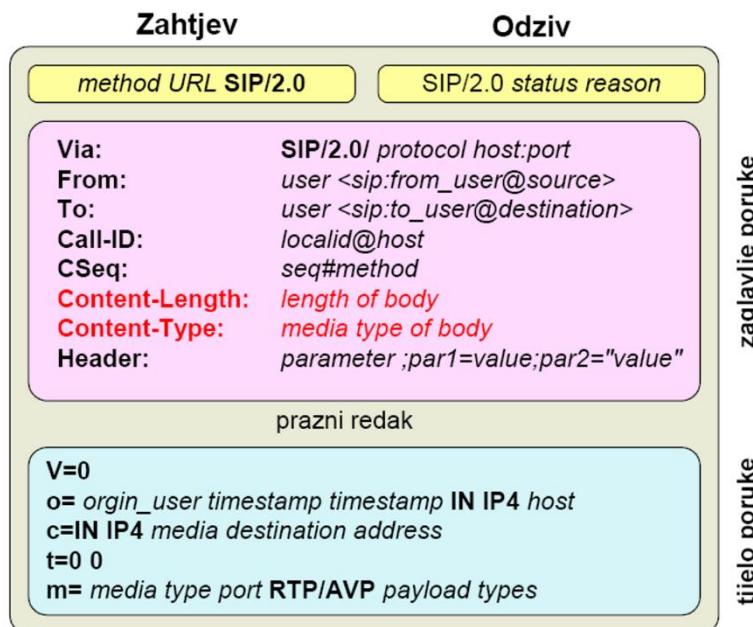
4.1.1. Poruke

Poruke protokola SIP su tekstnog formata i kao i poruke protokola HTTP, a komunikacija se odvija na načelu klijent-poslužitelj. Osnovna podjela poruka je na zahtjeve (metode) koji se šalju od klijenta prema poslužitelju i odgovore ili odzive (statusne kodove) koji se šalju od poslužitelja prema klijentu. Zahtjevi i odgovori koriste generički oblik poruke:

- početni redak, sadrži zahtjev ili statusni kod odgovora,
- jedno ili više zaglavlja,
- prazni redak za odvajanje zaglavljia poruke i opcionalnog tijela poruke,
- tijelo poruke (neobvezno) – npr. opis sjednice protokolom SDP (*Service Description Protocol*).

Opis sjednice nužan je za prijenos podataka u stvarnom vremenu. Neki od parametra koji opisuju sjednicu su: vrata (engl. *port*), vrsta protokola za prijenos u stvarnom vremenu, vrsta kodiranja medija, naziv sjednice, verzija protokola, itd. Kod pokretanja sjednice prenosi se prijedlog parametara koji druga strana može prihvati ili odbaciti. Treba paziti da UDP-segmenti, zajedno sa svim zaglavljima, ne prijeđu maksimalnu transmisijsku jedinicu (engl. *Maximum Transmission Unit*, MTU) jer će to dovesti do fragmentacije IP-paketa. Poruke se izmjenjuju s kraja na kraj ili od točke do točke i u tom slučaju mogu biti poslane od strane korisničkih agenata na klijentu i poslužitelju te od strane posredničkih poslužitelja.

Na slici 4.3 prikazan je format poruka, zahtjeva i odziva (odgovora).



Slika 4.3 – Format poruka

Parametri se prenose u zaglavljima poruka i sadrže informaciju o pozivajućoj i pozivanoj strani, duljinu i tip tijela poruke, itd. Neka od zaglavja koriste se u svim tipovima poruka, a neka samo u određenima. Prijamna strana može ignorirati zaglavja čije značenje ne razumije. Njihov redoslijed pojavljivanja nije bitan osim u slučaju zaglavja *via*, čiji redoslijed ne smiju mijenjati niti prijamna strana niti poslužitelji.

4.1.2. Zahtjevi

Zahtjevi su sljedeći:

- INVITE: pokretanje sjednice (poziv u sjednicu),
- Re-INVITE: promjenu stanja/parametara sjednice,
- ACK: potvrda uspostave sjednice, koristi se u paru s INVITE,
- BYE: završetak sjednice,
- CANCEL: prekid sjednice,
- REGISTER: prijava trenutnog položaja korisnika,
- OPTIONS: provjera mogućnosti primatelja.

Budući da je moguće da oba terminala ne podržavaju iste načine kodiranja medija, nužno je prilikom uspostave sjednice izvršiti razmjenu mogućnosti. Terminal koji poziva u tijelu svog zahtjeva INVITE prezentira svoje mogućnosti posredstvom protokola SDP (*Session Description Protocol*). Pozvani terminal nakon prijema zahtjeva INVITE analizira tijelo poruke te u odzivu šalje svoje mogućnosti. Nakon toga terminali mogu započeti sa slanjem podataka prema utvrđenom dogovoru.

Poruka ACK predstavlja potvrdu, odnosno konačni odgovor poruci INVITE, riječ je o zahtjevu od točke do točke. Slanjem poruke ACK, CSeq se ne smanjuje. Poslužiteljska strana uspoređuje Cseq broj u ACK poruci s odgovarajućim Cseq brojem u poruci INVITE.

Porukom BYE pokreće se raskid sjednice (zahtjev s kraja na kraj) i može ga inicirati samo jedan od korisničkih agenata koji sudjeluju u sjednici, a ne posrednički poslužitelj ili neki treći korisnički agent.

Porukom CANCEL pokreće se prekid sjednice, a može ga inicirati od korisničkih agenata ili posrednički poslužitelj. Riječ je o zahtjev od točke do točke koji se proslijeđuje istim putem kao i zahtjev INVITE.

Porukom REGISTER korisnik prijavljuje svoju lokaciju, odnosno na kojoj se trenutnoj IP-adresi nalazi. Registracija je obvezna za dolazne pozive, dok za odlazne nije. Zahtjev se šalje i proslijeđuje sve dok ne dođe do nadležnog poslužitelja za registraciju u domeni. CSeq se smanjuje svakim slanjem zahtjeva REGISTER i može sadržavati tijelo poruke, ali i ne mora.

Polja u zaglavlju mogu biti općenita ili vezana uz poruku zahtjeva, poruku odgovora ili vezana uz neki element u mreži. Polja koja se nalaze u zahtjevima i odgovorima su sljedeća:

- *call-ID* – obvezno polje, jedinstveni broj korisničkog agenta koji sudjeluje u komunikaciji,
- *contact* – adresa na koju se šalju zahtjevi i odgovori prilikom komunikacije, popunjava poslužitelj za preusmjeravanje,
- *CSeq* – nalazi se u svakom zahtjevu, predstavlja broj zahtjeva koji je poslan i povećava se sa svakim slanjem zahtjeva unutar iste komunikacije,
- *date* – datum slanja,
- *from* – adresa entiteta koji kreira/inicira poruku,
- *to* – adresa entiteta koji treba primiti poruku,
- *via* – zapis o ruti poruke, kako bi komunikacija išla istom rutom u drugom smjeru,
- *allow-events* – način komunikacije, npr. dijalog.

Polje *via* u zaglavlju definira put/rutu kojom se zahtjev usmjerava. Inicijator zahtjeva stavlja adresu u polje *via*, a poslužitelji provjeravaju polje *via*, dodaju vlastitu adresu i proslijeđuju zahtjeve. Svaki posrednički poslužitelj dodaje polje *via* sa svojom adresom kako bi se osiguralo da će odgovor ići istom rutom i kako bi se izbjegle petlje ili neuobičajene situacije kod usmjeravanja.

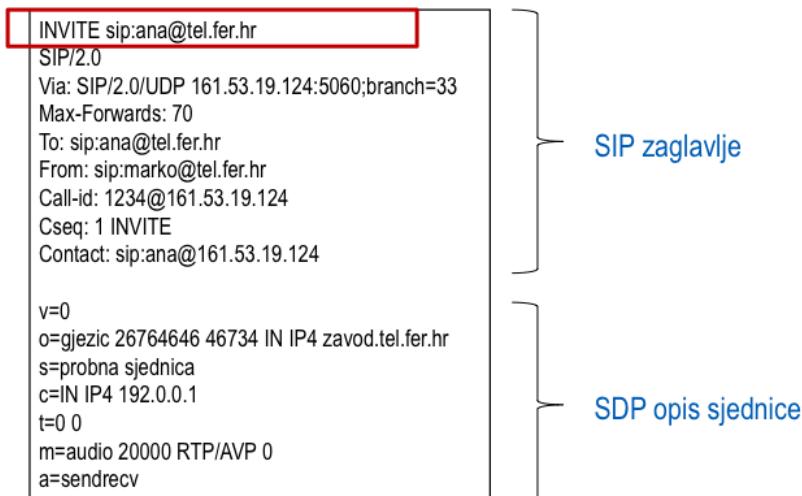
Polja vezana samo za zahtjev su sljedeća:

- *accept* – prihvatljiva vrsta medija,
- *accept-contact* – adresa posredničkog poslužitelja preko kojeg se šalje zahtjev,
- *accept-encoding* – prihvatljiva shema kodiranja,
- *accept-language* – prihvatljiv jezik komunikacije,
- *authorization* – informacija o autorizaciji poruke,
- *reason* – razlog prekida sjednice (kod poruka BYE i CANCEL),
- *reply-to* – adresa na koju se šalje odgovor,
- *route* – informacija o usmjeravanju zahtjeva,
- *session-expires* – vrijeme isteka sjednice.

Na slici 4.4 prikazan je primjer zahtjeva INVITE. Uspostavlja se sjednica pomoću zahtjeva s metodom INVITE upućen od strane *marko@tel.fer.hr* prema *ana@tel.fer.hr*. Prilikom

uspostave poziva postavljaju se polja *from*, *to* i *call-ID*, koja se ne mijenjaju tijekom poziva. Dakle, sve sljedeće poruke unutar tog dijaloga zadržavaju vrijednosti postavljene na početku. Polje *CSeq* služi za numeriranje zahtjeva unutar dijaloga. Polje *CSeq* u poruci odgovora označava na koji se zahtjev odgovor odnosi. Razlog za numeriranje je praćenje redoslijeda poruka. Već je spomenuto da SIP može koristiti UDP kao transportni protokol, a kod UDP-a se može dogoditi da se redoslijed poruka „pokvari“ na putu od izvorišta do odredišta. Ovako se zahtjev i odgovarajući odgovor mogu upariti pomoću polja *CSeq*. Vrijednost polja *CSeq* povećava se za jedan za svaki novi zahtjev, osim za zahtjeve ACK i CANCEL, koji uvijek sadrže *CSeq* onog zahtjeva na koji se odnose (ACK u smislu potvrde, a CANCEL u smislu opoziva prethodnog zahtjeva).

Definicija tipa tijela poruke istaknuta je poljem zaglavljima *Content-Type*, koje govori da je riječ od SDP opisu sjednice. SDP opis sjednice u SIP-zahtjevu (poruka INVITE) pokazuje da marko želi primati RTP-tok na vratima 20000 s (*audio*) podacima kodiranim određenim kodekom (*sendrecv stream*).



Slika 4.4 – Primjer zahtjeva INVITE

4.1.3. Odgovori

Postoji šest vrsta odgovora:

- 1xy – informativni, o statusu poziva, zahtjev primljen, nastavlja se procesiranje zahtjeva (npr. *180 ringing*),
- 2xy – potvrđni, uspješno izvršenje zahtjeva, akcija uspješno primljena, razumljiva i prihvaćena (npr. *200 OK*),
- 3xy – preusmjeravanje – daljnje akcije preusmjerenе s ciljem izvršenja zahtjeva (npr. *301 moved temporarily*),
- 4xy – pogreška na klijentu – zahtjev sadrži sintaksnu pogrešku ili ne može biti izvršen na tom poslužitelju (npr. *404 not found*),
- 5xy – pogreška na poslužitelju – nemogućnost valjanog izvršenja zahtjeva (npr. *500 internal server error*),
- 6xy – globalna pogreška – zahtjev nije valjan niti za jedan poslužitelj (npr. *decline*).

Informativni odgovori informiraju o napretku uspostave sjednice i razmjenjuju se s kraja na kraj. Izuzetak je poruka *100 trying* koja se šalje od točke do točke i ne sadrži tijelo poruke, te se nikad ne prosljeđuje. Ostali informativni odgovori su:

- *180 ringing* – informira da je INVITE primljen, ne šalje se ako pozvani korisnik odgovori dovoljno brzo,
- *181 call is being forwarded* – poziv je preusmjeren na drugu krajnju točku,
- *182 call queued* – zahtjev INVITE je primljen i stavljen u rep čekanja za obradu,
- *183 session progress* – informira da je INVITE primljen i uspostava sjednice je u postupku (slična je poruci *100 trying*, ali se šalje s kraja na kraj).

Potvrdni odgovori upućuju da je zahtjev uspješno primljen i prihvaćen:

- *200 OK* – (1) odgovor na poziv u sjednicu, prihvaca poziv i u tijelu poruke šalje parametre pozvanog korisnika, (2) odgovor na zahtjev, uspješan primitak ili obrada zahtjeva ili odgovor na INVITE, REGISTER i OPTIONS,
- *202 accepted* – zahtjev je primljen, ali ne može biti obrađen od primljene strane.

Poruke preusmjeravanja šalju se od strane posredničkog usmjeritelja ili usmjeritelja za preusmjeravanje kao odgovor na zahtjev za uspostavom sjednice. Primanjem odgovora klijent može potvrditi i primitak (ACK) i tada šalje novi zahtjev INVITE na dobivenu adresu poslužitelja:

- *300 multiple choices* – odgovor koji indicira da je zahtjev poslan na više mogućih lokacija,
- *301 moved permanently* – odgovor sadrži novu adresu pozvanog korisnika (polje zaglavka *Contact*),
- *302 moved temporarily* – odgovor sadrži novu adresu koja trenutno vrijedi za pozvanu stranu (adresu u polju *Contact* ne treba spremati, vrijedi određeno vrijeme definirano u polju *expires*),
- *305 use proxy* – odgovor koji daje adresu posredničkog poslužitelja koji je nadležan za poslani zahtjev te pozivajuća strana mora poslati novi zahtjev na novu adresu,
- *380 alternative service* – odgovor vraća adresu poslužitelja koji poslužuje željenu uslugu.

Pogreške mogu nastati na klijentu, poslužitelju ili općenito u komunikaciji. Pogreške na klijentu događaju se kad zahtjev ne može biti ispunjen te poslužitelj daje odgovor klijentu kako zahtjev mora biti preformuliran i ponovo poslan (4xx, npr. *400 bad request* – nedostaje neko polje). Pogreške na poslužitelju imaju oznaku 5xx (*500 server internal error*). Općenite pogreške predstavljaju odgovori koji upućuju da će se pogreška za poslani zahtjev uvijek dogoditi bez obzira na mjesto gdje se zahtjev pošalje te da ga ne treba nigdje i nikada u ovom obliku ponovo poslati, (6xx, npr. *600 busy everywhere*).

Slika 4.5 prikazuje primjer odgovora.

SIP/2.0 200 OK
Via: SIP/2.0/UDP 161.53.19.124
branch=33
Max-Forwards: 70
To: sip:marko@tel.fer.hr
From: sip:ana@tel.fer.hr
Call-ID: 1234@ 161.53.19.124
CSeq: 1 200 OK
Contact: sip:TN@ 161.53.19.124
 v=0 o=gjezic 26764646 46734 IN IP4 zavod.tel.fer.hr s= probna sjednica c=IN IP4 192.0.0.1 t=0 0 m=audio 20000 RTP/AVP 0 a=sendrecv

Slika 4.5 – Primjer odgovora

U ovom primjeru, poruka *200 OK* potvrđuje zahtjev INVITE. Na primjeru na slici, odgovor *200 OK* potvrđuje prethodni zahtjev INVITE i sadrži isti CSeq. Opis SDP sjednice u SIP-odgovoru (*200 OK*) pokazuje da *ana* prihvata kodek (*sendrecv stream*) te da želi primati RTP-tok na vratima 20000.

4.1.4. Međudjelovanje mrežnih elemenata

Slijed operacija prilikom uspostave sjednice je sljedeći:

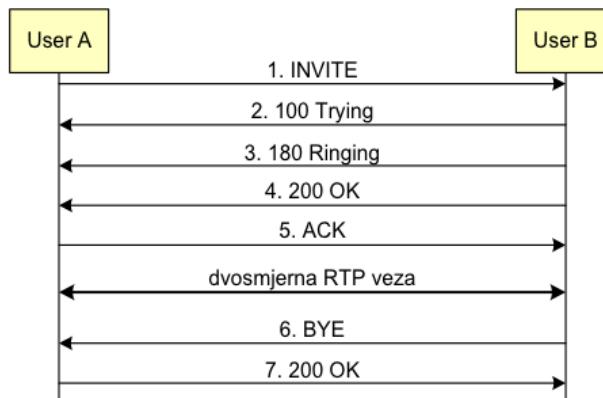
- klijent šalje inicijalni INVITE zahtjev;
- poslužitelj vraća odgovor;
- klijent prima odgovor na inicijalni zahtjev;
- klijent ili poslužitelj generiraju daljnje zahtjeve;
- primanje dalnjih zahtjeva;
- BYE – kraj sjednice;
- CANCEL – može se dogoditi tijekom sjednice.

Sjednica se može uspostaviti izravno ili preko jednog ili više posredničkih poslužitelja. Na sljedećoj slici prikazana je uspostava izravnog poziva. Tijek uspostave sjednice oponaša model telefonskog poziva. Na slici 4.6 prikazan je primjer izravnog poziva.

Za pokretanje sjednice koristi se zahtjev INVITE kao poziv na sudjelovanje u sjednici. Korisnički agent *User A* inicijalizira zahtjev INVITE tako da na početku sjednice postavi vrijednosti zaglavlja *To*, *From* i *Call-ID*. Ove vrijednosti se koriste tijekom cijelog vremena trajanja sjednice za njenu identifikaciju. S obzirom na to da se sjednica identificira preko ovih zaglavlja, ona se nikad ne mijenjaju.

Uspostava sjednice provodi se kroz tri poruke i to INVITE/200 OK/ACK. Sve druge poruke tipa *100 trying* i *180 ringing* nisu obvezne. Ovo se može zaključiti iz kodova poruka koji pripadaju skupini informacijski neobveznih poruka. Razmjenom poruka za uspostavu sjednice uspostavlja se odnos sudionika u komunikaciji (korisničkog agenta na strani A i njegovog para na strani B), koji se naziva dijalog. Dijalog je identificiran upravo gore

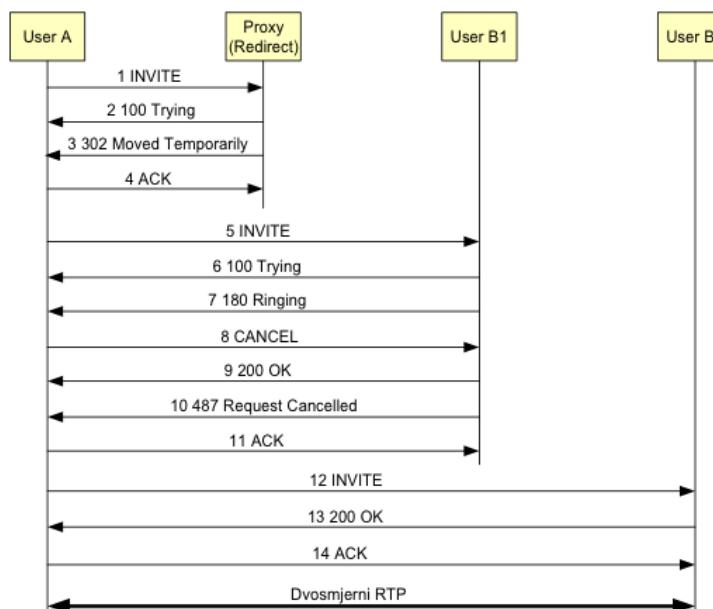
spomenutim vrijednostima *to*, *from* i *call-ID*. Raskid veze može inicirati bilo koja strana slanjem poruke BYE na koju druga strana odgovara s *OK*.



Slika 4.6 – Primjer izravnog poziva

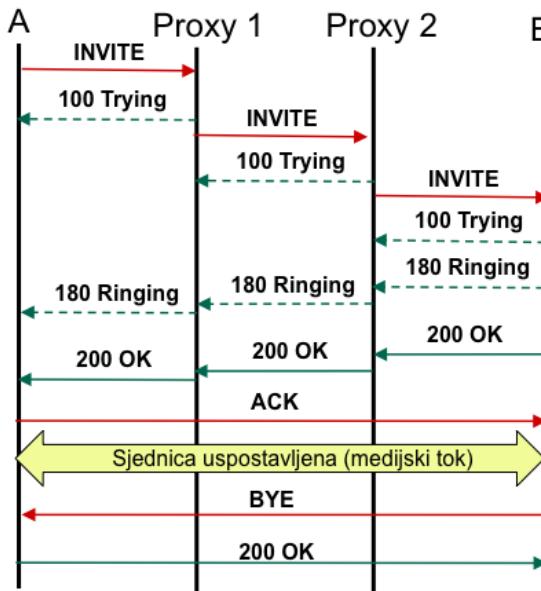
Sljedeći primjer prikazuje slučaj kada nema odziva i potrebno je saznati adresu korisnika. Komunikacija ide preko poslužitelja za preusmjeravanje koji dohvaća lokaciju korisnika preko lokacijskog poslužitelja i vraća ju posredničkom poslužitelju (porukom *302 moved temporarily*) koji zatim usmjerava poziv (zahtjev za sjednicom) na novu adresu (slika 4.7).

U ovom primjeru korisnik A kontaktira poslužitelja za preusmjeravanje (*redirect*) s upitom za korisnika B1. *Redirect* poslužitelj vraća poruku *302 moved temporarily* koja sadrži dva zaglavila *contact*, jedno s adresom B1 i drugo s adresom B2. Nakon toga, korisnički agent A pokušava uspostaviti vezu koristeći se adresom danom u prvom zaglavju *contact*. Nakon isteka vremenskog broja korisnik A prekida uspostavu veze *CANCEL* zahtjevom te šalje novi *INVITE* zahtjev na adresu iz drugog zaglavja *contact*. Komunikacija se odvija transportnim protokolom RTP (*Real-time Transport Protocol*) koji pruža uslugu prijenosa podataka sa stvarnovremenim svojstvima (npr. audio, video) s kraja na kraj koristeći pojedinačno (engl. *unicast*) ili višeodredišno (engl. *multicast*) slanje na mrežnom sloju.



Slika 4.7 – Uspostava sjednice preko usmjeritelja za preusmjeravanje

Slika 4.8 prikazuje uspostavu sjednice preko posredničkog poslužitelja. Klijent A šalje zahtjev INVITE koji se usmjerava preko dva poslužitelja (proxy1 i proxy2) do odredišta B. Nakon vraćanja informativnih poruka 100 trying i 180 ringing, vraća se odgovor OK klijentu A te je nakon dobivene potvrde ACK sjednica između klijenata A i B uspostavljena. Slijedi izmjena podataka i raskid sjednice (BYE, 200 OK) nakon obavljene komunikacije.



Slika 4.8 – Uspostava sjednice preko posredničkih poslužitelja

4.2 Zadaci

1. Kako se ostvaruje signalizacija u mreži s komutacijom paketa i zašto?
2. Može li se ostvariti kvalitetan telefonski poziv Internetom? Objasnite.
3. Koje su glavne značajke protokola SIP?
4. Pobrojite i obrazložite funkcije mrežnih elemenata u arhitekturi SIP.
5. Objasnite način adresiranja u arhitekturi SIP.
6. Koja je razlika između SIP-registra i domaćeg agenta u Mobile IP?
7. Na koji se način ostvaruje lociranje poslužitelja u mreži SIP?
8. Kako protokolom SIP otkrivamo lokaciju korisnika u mreži?
9. Kada se u komunikaciji SIP koristi transportni protokol TCP, a kada UDP?
10. Usporedite izravni i neizravni SIP-poziv. Koje se poruke pritom izmjenjuju?
11. Objasnite ulogu *vía* polja u zaglavlju SIP.
12. Čemu služe informativni odgovori?
13. Skicirajte uspostavu i raskid sjednice kada nema odziva korisnika.
14. Skicirajte primjer uspostave poziva SIP s tri sudionika.

15. Definirajte dvije domene SIP u kojima se nalaze SIP-klijenti koji žele uspostaviti govornu komunikaciju (VoIP) putem internetske mreže. Dodijelite adrese čvorovima te prikažite slijed poruka koje se izmjenjuju prilikom uspostave i raskida komunikacije.
16. Što se događa u slučaju pogreške u komunikaciji protokolom SIP?
17. Istražite proširenja protokola SIP i usluge koje se na njima temelje.
18. Istražite koji se sve protokoli koriste za signalizaciju u internetskoj mreži.
19. Istražite protokole transportnog sloja koji omogućavaju prijenos podataka sa stvarnovremenim svojstvima.
20. Istražite kako bi se protokol SIP primijenio u mreži IPv6.

Literatura

Knjige

- V. Matković, V. Sinković, „Teorija informacije“, Školska knjiga, Zagreb, 1984.
- V. Sinković, „Informacijske mreže“, Školska knjiga, Zagreb, 1994.
- I. Lovrek, „Modeli telekomunikacijskih procesa – Teorija i primjena Petrijevih mreža“, Školska knjiga, Zagreb, 1997.
- A. Bažant, G. Gledec, Ž. Ilić, G. Ježić, M. Kos, M. Kunštić, I. Lovrek, M. Matijašević, B. Mikac, V. Sinković, „Osnovne arhitekture mreža“, 2. izdanje, Element, 2007.
- A. Bažant, Ž. Car, G. Gledec, D. Jevtić, G. Ježić, M. Kunštić, I. Lovrek, M. Matijašević, B. Mikac, Z. Skočir, „Telekomunikacije – tehnologija i tržiste“, Element, Zagreb, 2007.
- I. Pandžić, A. Bažant, Ž. Ilić, Z. Vrdoljak, M. Kos, V. Sinković, „Uvod u teoriju informacije i kodiranje“, 2. izdanje, Element, Zagreb, 2009.
- A.S. Tanenbaum, D.J. Wetherall, „Computer Networks“, Fifth Edition, Pearson Education Inc., 2011.
- F. Halsall, „Computer Networking and the Internet“, 5th Edition, Addison Wesley, 2005.
- J.F. Kurose, K.W. Ross, „Computer Networking: A Top-Down Approach“, 6th Edition, Addison Wesley, 2012.
- J.L. Peterson, B.S. Davie, „Computer Networks: A Systems Approach“, 5th Edition, Elsevier – Morgan Kaufmann, 2011.
- P. Loshin, „IPv6: Theory, Protocol, and Practice“, Second Edition, Elsevier – Morgan Kaufmann, 2004.
- A. Farrel, „The Internet and its Protocols“, Elsevier – Morgan Kaufmann, 2004.

Pregledni članci

- W. Stallings, „IPv6: the New Internet Protocol“, *IEEE Communications Magazine*, Vol. 34, No. 7, pp. 96–108. July 1996.
- D. G. Waddington, F. Chang, „Realizing the Transition to IPv6“, *IEEE Communications Magazine*, Vol. 6, No. 3, pp. 138–148, 2002.
- C. E. Perkins, “Mobile IP”, *IEEE Communications Magazine*, Vol. 35, No. 5, pp. 84 –99, 1997.
- A.T: Campbell, J. Gomez-Castellanos, „IP Micro-Mobility Protocols“, *Mobile Computing and Communications Review*, Vol. 4, No. 4, pp. 45–53, 2000.
- S. Iren, P.D. Amer, P.T. Conrad, „The Transport Layer: Tutorial and Survey“, *ACM Computing Surveys*, Vol. 31, No. 4, pp. 360–405, 1999.
- H. Shulzrinne, J. Rosenberg, „The Session Initiation Protocol: Internet-Centric Signaling“, *IEEE Communications Magazine*, October 2000.

„BGP protokol“, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Centar informacijske sigurnosti, 2011.

[<http://www.cis.hr/files/dokumenti/CIS-DOC-2011-03-006.pdf>]

S. A. Baset, H. Schulzrinne, „An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol“, Columbia University, 2006.

[http://www.cs.columbia.edu/~salman/publications/skype1_4.pdf]