



UNIVERZITET SINGIDUNUM

**DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I
MEĐUNARODNU SARADNJU**

Studijski program: Savremene informacione tehnologije

MASTER RAD

**Internet Protokol verzije 6 i
Mobilnost kao njegov napredni servis**

Mentor:

Prof. dr Mladen Veinović

Student:

Vladimir Jakovljević 410262/2014

Београд, 2015. године

S A D R Ž A J

Pregled slika u radu.....	3
Pregled tabela u radu.....	3
Primeri komandi u tekstu	3
Uvod.....	5
1. Uvod u IPv6 protokol	6
1.1 Ograničenja IPv4 adresiranja	6
1.2 Karakteristike IPv6 protokola	7
1.3 Zaglavlje IPv6 paketa	8
13.12.1 Osnovno zaglavlje IPv6 paketa	9
13.12.2 Zaglavlja proširenja IPv6 paketa	10
1.4 Predstavljane IPv6 adresa	12
1.5 IPv6 unicast adrese	13
1.5.1 Adrese lokalne veze	14
1.5.2 Globalne unicast adrese	15
1.5.3 Jedinstvene lokalne unicast adrese	15
1.5.4 Specijalne IPv6 adrese	16
1.5.5 Kompatibilne IPv6 adrese	16
1.6 IPv6 multicast adrese	17
1.7 IPv6 Anycast adrese.....	18
13.12.1 Format anycast adrese.....	19
1.8 IP mobilnost	19
2. IPv6 mobilnost.....	20
2.1 Entiteti i osnovni pojmovi MIP arhitekture	20
2.1.1 Mobilni čvor.....	20
2.1.2 Domicilna adresa	20
2.1.3 CoA adresa	20
2.1.4 Domicilna i strana mreža	21
2.1.5 Domicilni agent	21
2.1.6 Strani agent.....	21
2.1.7 Korespondentni čvor.....	21
2.2 Osnovni principi Mobilnog IP-a.....	21
13.12.1 Funkcija otkrivanja agenta	22
13.12.2 Funkcija registracije agenta.....	22

13.12.3	Tunelovanje.....	23
2.3	MIPv4 i njegova slabosti i ograničenja.....	24
2.5.1	Suština Mobilnog IP-a za IPv4.....	24
2.5.2	Slabosti i ograničenja Mobilnog IP-a za IPv4.....	24
2.4	Osnove IPv6 Mobilnosti	25
2.5	Operacije IPv6 mobilnosti.....	26
2.6	Zaglavlje za IPv6 mobilnost.....	27
2.7	Poruke MIPv6.....	28
2.8	ICMP za IPv6 u funkciji MIPv6 i dinamičko otkrivanje adrese domicilnog agenta	31
2.9	Optimizacija putanje	33
2.10	Zaštita Mobilnog IPv6	34
2.11	IPv6 NEMO i mobilnost mreže	34
2.12	Praktična upotreba MIPv6 protokola.....	36
3.	Implementacija MIPv6	37
3.1	Omogućavanje IPv6 Mobilnosti na ruteru	37
3.2	Podešavanje informacija vezivanja.....	38
3.3	Omogućavanje i konfigurisanje NEMO na IPv6 mobilnom ruteru.....	38
3.4	Omogućavanje NEMO domicilnog agenta na mobilnom ruteru.....	40
3.5	Omogućavanje rominga (“lutanja”) na interfejsu mobilnog ruteru.....	40
3.6	Filtriranje zaglavlja proširenja Mobilnog IPv6 protokola.....	40
3.7	Kontrolisanje ICMP poruka za nedostupno odredište	41
3.8	Verifikacija prirodnog (native) IPv6 tunelovanja za Mobilni IPv6.....	42
3.9	Konfiguracija i verifikacija grupe hostova mobilnih čvorova na domicilnom agentu	42
3.10	Modifikacija Mobilnog IPv6 na interfejsu.....	44
3.11	Praćenje i održavanje Mobilnog IPv6 na ruteru.....	44
3.12	Mobilna domicilna mreže	45
13.12.1	Konfiguracija mobilne domicilna mreže	46
	Zaključak.....	49
	Literatura	51

Pregled slika u radu

Slika 1: Uporedni pregled formata IPv4 i IPv6 zaglavlja	9
Slika 2: Izgled IPv6 paketa.....	11
Slika 3: Kreiranja ID interfejsa po Modifikovanom EUI-64 formatu	14
Slika 4: Opšti format globalne unicast adrese	15
Slika 5: Format jedinstvene lokalne unicast adrese.....	16
Slika 6: Format multicast adrese	17
Slika 7: Format IPv6 anycast adrese.....	19
Slika 8: Algoritam registracije agenta kada se koristi FA.....	23
Slika 9: Problem tripartitnog rutiranja kroz princip funkcionisanja MIPv4	25
Slika 10: Proces registracije MN kod MIPv6.....	27
Slika 11: Opšti format zaglavlja IPv6 mobilnosti	28
Slika 12: Zaglavlje opcija destinacija koje sadži.....	29
Slika 13: Zaglavlje opcija destinacija koje sadži.....	29
Slika 14: Zaglavlje opcija destinacija koje sadži.....	30
Slika 15: Opšti format ICMPv6 poruke	32
Slika 16: DHAAD mehanizam	33
Slika 17: NEMO operacije	35
Slika 18: Kretanja paketa od korespondentnog čvora do mobilnog čvora mobilne domicilne mreže.....	45
Slika 19: Mobilna domicilna mreža transportne kompanije.....	46

Pregled tabela u radu

Tabela 1: Moguće vrednosti polja <i>Next Header</i>	12
Tabela 2: Definisane vrednosti polja <i>Scope</i> multicast adrese	18
Tabela 3: ICMPv6 poruke uključene u MIPv6	32

Primeri komandi u tekstu

Komanda 1: Opšti primer koda koji omogućava IPv6 Mobilnost na ruteru	37
Komanda 2: Opšti primer koda za podešavanje informacija vezivanja.....	38
Komanda 3: Opšti primer koda za omogućavanje i konfigurisanje NEMO na IPv6 mobilnom ruteru	39
Komanda 4: Opšti primer koda za omogućavanje NEMO domicilnog agenta na IPv6 mobilnom ruteru	40

Komanda 5: Opšti primer koda za omogućavanje rominga (“lutanja”) na interfejsu mobilnog ruteru	40
Komanda 6: Opšti primer koda za postavljanje liste dozvole	41
Komanda 7: Opšti primer koda za postavljanje liste zabrane	41
Komanda 8: Opšti primer koda za postavljanje liste zabrane	42
Komanda 9: Opšti primer koda za verifikaciju tunelovanja	42
Komanda 10: Opšti primer koda za konfiguraciju i verifikaciju grupe hostova	43
Komanda 11: Opšti primer koda za modifikaciju Mobilnog IPv6 na interfejsu	44
Komanda 12: Opšti primer koda za praćenje i održavanje Mobilog IPv6 na ruteru	45
Komanda 13: Konfiguracija glavnog domicilnog agenta u centrali transportne kompanije	47
Komanda 14: Konfiguracija domicilnog agenta u podcentrali kompanije	47
Komanda 15: Konfiguracija rutera u jednom prevoznom sredstvu	47

Uvod

Mobilnost predstavlja svakodnevnost savremenog čoveka, a potreba za upotrebom Interneta i servisa koje on pruža neophodnost. Ovo posebno važi za poslovnog čoveka, čije potrebe se ne završavaju samo sa pružanjem servisa, već i sa njihovom konstantnošću. Mobilnost u Internet svetu znači da se sa promenom lokacije i sa vezivanjem mobilnog uređaja za drugu tačku pristupa ne dolazi do prekida pojedinih servisa.

U trenutku pisanja ovog rada pojavila se informacija Američkog Sekretarijata za Internet Brojeve – ARIN (eng. *American Registry for Internet Numbers*), neprofitne organizacije koja upravlja distribucijom Internet resursa za region Severne Amerike, po kojoj je navedeni region ostao bez IPv4 adresa. Iako je ova informacija zvučala poznato, iz razloga što se godinama neplanski i neorganizovano troše IPv4, ovo je konačno zvanična informacija da su adrese potrošene. Međutim, stručna Internet zajednica je predvidela kraj IPv4 protokola i razvila IP protokol verzije 6 kao odgovor na kraj, ali i na slabosti prethodnika.

Kako se približava dan kada će IPv4 protokol i formalno postati prošlost, a IPv6 i njegove funkcije i protokoli proširenja predstavljati budućnost, a verovatno već i sadašnjost Interneta i računarskih mreža, u ovom radu je biće predstavljen Mobilni IPv6 protokol.

Konceptualno rad je podeljen na tri dela, koja se nalaze između uvodnog dela i zaključka:

U **prvom delu rada** objašnjeni su razlozi razvoja IPv6 protokola, njegove osnovne karakteristike, razlike i prednosti u odnosu na IPv4 protokol.

Drugi deo rada govori o konceptu Mobilnog IPv6 protokola (MIP) i njegovim principima, kroz objašnjavanje osnovnih entiteta i funkcija. U prvim odeljcima drugog dela najpre se objašnjava IPv4 mobilnost, kako bi se uočile prednosti MIPv6 u odnosu na njega.

Ideja je da **treći deo rada** bude neka vrsta uputstva za konfigurisanje Mobilnog IPv6 protokola, kroz objašnjavanje osnovnih koraka kod CISCO opreme, kao i prikaz istih kroz primere.

1. Uvod u IPv6 protokol

Značajnije izmene na četvrtoj verziji IP protokola (eng. *Internet Protocol*), odnosno na IPv4, izvršene su 1981. godine i date su u okviru RFC norme pod rednim brojem 791. IPv4 obezbeđuje 32 fiksna bita za adresiranje hostova. Teorijski, sa tim kapacitetom, omogućeno je 2^{32} , odnosno približno oko četiri milijarde adresa. Izgledalo da je adresiranje, kao osnovni problem svakog komunikacionog procesa, rešeno za duži niz godina, čak i vekova. Pored toga IPv4 se pokazala kao zrela i za implementiranje jednostavna tehnologija. Prilikom kreiranja i definisanja ove verzije Internet protokola nije se mogao predvideti eksponencijalni rast Internet prostora, koji je doveo do potrošnje gotovo celokupnog adresnog prostora. IPv4 je pokazao i neke druge nedostatke i ograničenja.

1.1 Ograničenja IPv4 adresiranja

Trošenje adresnog prostora, odnosno ograničeni broj adresa je jedan od glavnih nedostataka IPv4. Osnovni razlog za pojavu ovog nedostatka jeste eksponencijalni rast globalne računarske mreže, ali i ne baš dobra dodela adresa po klasama. Neretko su entiteti potraživali adresu Klase B, čiji je kapacitet 65000 adresa, iako je za njihove potrebe bilo dovoljno tek nešto preko kapaciteta Klase C, odnosno 255 adresa. Takođe, od entiteta se nije tražilo da opravdaju svoje zahteve za adresnim prostorom. Tako se došlo do pozicije da se samo mali procenat podeljenog adresnog prostora koristi i da postoje kompanije (Apple, Microsoft, General Electric i druge), odnosno entiteti koji drže „zarobljeni“ adresni prostor.

Sa porastom broja hostova i potrošnjom adresnog prostora, rastao je i broj mreža, a samim tim su rasle tabele rutiranja i javljao se problem sa ruterima da održavaju velike tabele. Mehanizmi koji su trebali da omoguće prevazilaženje problema ogromnog uvećanja tabele rutiranja su VLSM (eng. *Variable-Length Mask*) i CIDR (eng. *Classless Inter-Domain Routing*).

Kao posledica rasta hostova definisana su javna i privatna adresiranja, a kao način za uštedu adresa počeo je da se koristi NAT (eng. *Network Address Translation*). Koliko god bio elegantno rešenje, NAT je pokazao i svoje negativne strane, a deo stručne javnosti smatra da je NAT uzrok svega najboljeg i najgoreg u IP postavkama. [1]

Konfigurisanje IP adresa na hostovima predstavlja još jedan nedostatak. Naime, IPv4 zahteva ručno postavljanje adresa ili upotrebu dodatnog protokola, kao što je DHCP protokol (eng. *Dynamic Host Configuration Protocol*). Sa povećanjem broja uređaja koji pristupaju Internetu, javila se potreba za jednostavnijom dodelom adresa.

Sledeće ograničenje je nedostatak sigurnosnih usluga na nivou samog IP protokola. IPSec pruža sigurnosne usluge privatnosti, integriteta, autentifikacije i neporecivosti, ali kod IPv4 on je zapravo proširenje samog protokola, odnosno opcion je i nije dovoljno prihvaćen. Zato je bilo potrebno da IPSec postane standardan integralni deo IP skupa protokola.

Poput IPSec-a i mobilnost nije standardno dostupna u IPv4 verziji.

“Vrsta usluge” (eng. Type of Service) je polje u zaglavlju IPv4 paketa, kojim se ostvaruje dostava paketa u realnom vremenu, odnosno kvalitet usluge (eng. *Quality of Service*). Međutim, u slučajevima kada je sadržaj paketa nemoguće odrediti, a to se najčešće dešava kod korišćenja enkripcije, ovo se pokazalo kao nedovoljno kvalitetno rešenje. Zbog ovog, ali i drugih funkcionalnih nedostataka, bilo je potrebno razviti novi IP protokol sa poboljšanim kvalitetom usluge.

Mehanizmi, koji su naknadno pravljani za IPv4 (NAT, VLSM, CIDR, IPSec, QoS), imali su ulogu da se prevaziđu nedostaci, ali i da se produži vek upotrebe IPv4. Međutim, navedeni mehanizmi imaju i svoje slabosti i ograničenja. Kao odgovor na navedena, ali i neka druga, ograničenja i nedostake IPv4, međunarodna operativna grupa IETF (eng. *Internet Engineering Task Force*), razvila je i promovisala skup protokola i normi (RFC 1752, 1883, 1886, 1971, 1993). Navedeni protokoli i norme označeni su kao šesta iteracija IP protokola, odnosno IPv6.

1.2 Karakteristike IPv6 protokola

IPv6 je logična i evolucionarna faza razvoja IP mreža, ali može biti nesmotreno reći da je i konačna faza razvoja. Kada je razvijana IPv4 tehnologija nije se moglo ni pretpostaviti, da oko 4,3 milijarde adresa jednog dana neće biti dovoljne za adresiranje svih uređaja na globalnoj mreži.

IPv6 jeste izrađen na osnovama i iskustvima stečenim u radu sa IPv4 mrežama, ali takođe IPv6 ima sopstvene implementacije jedinstvenih funkcionalnosti. Poboljšanja koje je donela nova verzija IP protokola su sledeća:

Veći adresni prostor. Postoji nekoliko prednosti koje donose IPv6 adrese sa 128 bita (naspram 32 bita kod IPv4). Pored poboljšane globalne dostupnosti i fleksibilnosti, ovaj povećani adresni prostor dovodi do eliminisanja NAT-a, odnosno javnog i privatnog adresiranja kakvo postoji kod IPv4.

Eliminacija univerzalne (eng. *Broadcast*) adrese. IPv6 definiše tri osnovna načina adresiranja:

- Jednoodredišno (eng. *Unicast*) adresiranje prepoznaje jedan čvor kao odredište (1:1).
- Višeodredišno (eng. *Multicast*) adresiranje prepoznaje više čvorova kao odredište (1:N).
- Adresiranje najbliže adrese (eng. *Anycast*) adresiranje prepoznaje više čvorova, ali se kao odredište određuje najbliži čvor (1: najbliži od N).

Svi tipovi adresiranja su postojali i kod IPv4, ali je pored njih IPv4 imao i univerzalno adresiranje koje se pokazalo kao zahtevno po pitanju resursa, pa je izostavljeno kod IPv6.

Pojednostavljeno zaglavlje IPv6 paketa za poboljšanu efikasnost rutera. Jednostavnijim oblikovanjem IPv6 zaglavlja nastojalo se da višak informacija smesti u

ekstenziju paketa, čime se postigla efikasnija obrada paketa na ruterima, posebno u slučajevima posrednih rutera čiji je isključivi zadatak da paket samo proslede.

Podrška za zaštitu i mobilnost. IPv6, za razliku od svog prethodnika, podrazumeva podršku za IPsec i IP mobilnost.

Automatska konfiguracija adresa. IPv6 protokol obezbeđuje automatsku konfiguraciju IP adrese, prevođenjem adrese sloja veze (eng. *Data Link Layer Address*), primenom određenih algoritama, u IPv6 adresu, čime se obezbeđuje „plug-and-play“ funkcionalnost.

Prefiksi IPv6 adresa. Prefiks IPv6 adrese je deo adrese koji sadrži bitove čija je vrednost fiksna i predstavlja mrežni deo IPv6 adrese. Oznake za prefiks IPv6 mreže su analogne besklasnom tj. CIRD (eng. *Classless Inter-Domain Routing*) zapisu IPv4 protokola, odnosno pišu se u formatu *adresa/dužina prefiksa* (*dužina prefiksa* može imati najviše tri decimalne oznake – *xxx* i važi: $0 \leq xxx \leq 128$).

Više adresa po interfejsu. IPv6 interfejsima može se dodeliti više adresa, različitih tipova, koje se mogu istovremeno koristiti.

Adresa lokalne veze. IPv6 uređaji automatski kreiraju adresu za lokalno povezivanje na svakom interfejsu (eng. *Link-local addresses*). *Link-lokal* adresa, zapravo predstavlja tip *unicat* adrese namenjene isključivo za lokalno korišćenje. Ovde se može povući paralela sa privatnim IP adresama kod IPv4, jer se ove adrese ne koriste na Internetu već isključivo za *single* linkove ili segmente LAN-a.

Provajder-zavisno i provajder-nezavisno adresiranje. Usled velikog broja dostupnih adresa, preduzeća mogu koristiti adrese preko ISP-a (eng. *Internet Service Provider*), odnosno provajder-zavisno adresiranje (eng. *Provider-dependent addressing*) ili da koriste sopstveni provajder-nezavisni adresni prostor (eng. *Provider-independent addressing*).

U daljem tekstu biće detaljnije obrađene pojedine osobenosti IPv6 protokola, a kao preduslov za potpuniju obradu teme rada koja se odnosi na mobilnost kao napredni servis IPv6 protokola.

1.3 Zaglavlje IPv6 paketa

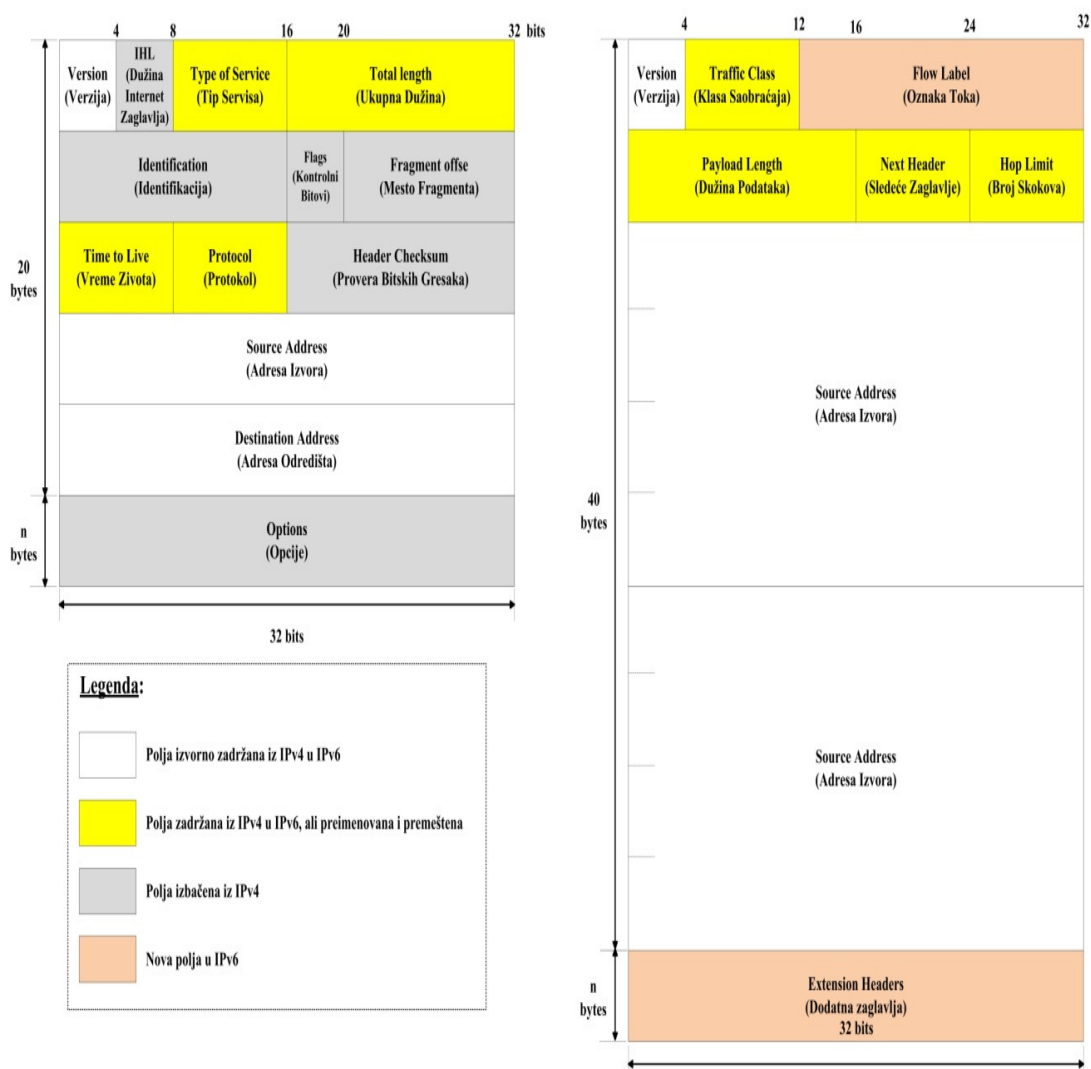
Kao što je već rečeno, jedna od osnovnih, ili bar prva uočljiva, razlika između IPv4 i IPv6 protokola je u zaglavlju paketa (eng. *Packet Header*). IPv6 zaglavlje je jednostavnije od IPv4 zaglavlja, a ta jednostavnost se postigla izbacivanjem retko korišćenih i nepotrebnih polja. Međutim uvedena su dodatna zaglavlja, tako da je za obradu osnovnog zaglavlja potrebno manje vremena, ali konačna brzina obrade zavisi od dodatnih zaglavlja. Dakle, IPv6 paket se sastoji iz tri dela:

- osnovnog zaglavlja,
- dodatnih zaglavlja (zaglavlja proširenja), kojih može biti najviše sedam, i
- podataka.

13.12.1 Osnovno zaglavlje IPv6 paketa

Neka polja iz IPv6 su zadržana izvorno u IPv6, odnosno nije menjana njihova funkcija, ime i mesto, dok su neka polja zadržana, ali su preimenovana i pomerena. Takođe, postoje i nova polja koja su dodata u IPv6. Na Slici 1 prikazan je uporedni pregled formata IPv4 i IPv6 zaglavlja. Osnovno zaglavlje IPv6 paketa sastoji se iz sledećih polja:

Verzija (eng. *Version*). Ovo polje ima isto mesto, naziv i funkciju kao i kod IPv4. Polje Verzija nosi podatak o kojoj se verzija protokola radi, njegova dužina je 4 bita, a vrednost 6 (kod IPv4 vrednost polja je 4).



Slika 1: Uporedni pregled formata IPv4 i IPv6 zaglavlja

Klasa Saobraćaja (eng. *Traffic Class*). Polje od 8 bita koje ima istu funkcionalnost kao i polje Tip Servisa (eng. *Type of Service*) kod IPv4. Uloga ovog polja je razvrstavanje

saobraćaja u klase i određivanje prioriteta paketima. Određivanje prioriteta paketima je korisno za kontrolu zagušenja saobraćaja.

Oznaka Toka (eng. *Flow Label*). Polje koje je uvedeno kao novo u IPv6, nije ga bilo u prethodnoj verziji protokola. Ovo polje je zaslužno što IPv6 može da ostvari potreban nivo kvaliteta usluge u mreži (QoS). Naime, ovo polje se koristi da se označe paketi koji imaju potrebu za posebnim tretmanom od strane IPv6 rutera. Pre svega se misli na saobraćaj koje koriste aplikacije koje se izvršavaju u realnom vremenu (govor, video signal i slično). Mehanizam je takav da se kreiraju tokovi podataka koji sadrže pakete sa istom labelom, gde je svaki tok jedinstveno određen sa izvorišnom i odredišnom adresom, i oznakom toka. Na ovaj način se može postići poseban tretman paketa kroz "rutiranje na isti način kako bi se garantovao dolazak u ispravnom redosledu. [2]

Dužina Podataka (eng. *Payload length*). Ovo polje je slično polju Ukupna Dužina (eng. *Total Length*) kod IPv4 i predstavlja ukupnu dužinu paketa, izraženu u bajtovima, umanjenu za 40, odnosno dužinu podataka. Dužina samog polja je 16 bita, pa maksimalna dužina podataka (sa 40 bajtova zaglavlja) može biti 2^{16} , odnosno 65.536 bajtova. Za pakete veće od ove veličine, koji se nazivaju *jumbograms* paketi, polje dužina podataka ima vrednost 0, ali se u dodatnom zaglavlju koristi opcija *Jumbo Payload*.

Sledeće Zaglavlje (eng. *Next Header*). Vrednost ovog polja, dužine 8 bitova, određuje tip informacija koje slede osnovno IPv6 zaglavlje. Informacije koje slede mogu biti podaci transportnog sloja, kao što su Transmission Control Protocol (TCP) ili User Datagram Protocol (UDP), ili to može biti dodatno zaglavlje. Ovo polje je slično polju Protokol (eng. *Protocol*) kod IPv4.

Broj Skokova (eng. *Hop Limit*). Polje je slično polju "Vreme Života" (eng. *Time to Live*) kod IPv4 i ima za svrhu sprečavanja pojave zagušenja odbacivanjem paketa koji su pogrešno rutirani. Predstavlja maksimalni broj rutera kroz koje paket može da prođe. Dužina polja je 8 bita, pa njegova maksimalna vrednost može biti 255 rutera. Nakon prolaska kroz ruter vrednost ovog polja se dekrementira za jedan. Ukoliko se vrednost polja izjednači sa nulom, paket se odbacuje, a izvoru se šalje ICMPv6 (eng. *Internet Control Messageing Protocol*) o grešci: *Time Exceeded* (ICMP tip 3).

Adresa Izvora (eng. *Source Address*). Adresa izvora paketa, dužine 128 bita, četiri puta duže polje od identičnog polja kod IPv4 (IPv4 adresa izvora je duga 32 bita).

Adresa Odredišta (eng. *Destination Address*). Adresa odredišta paketa, dužine 128 bita, četiri puta duže polje od identičnog polja kod IPv4 (IPv4 adresa odredišta je duga 32 bita). [3]

13.12.2 Zaglavlja proširenja IPv6 paketa

Većina dodatnih opcija kod IPv6 se nalaze u dodatnim zaglavljlama, odnosno zaglavljlama proširenja, pa se u paketu šalju samo nophodna dodatna zaglavlja (zaglavlja proširenja), što omogućava veću efikasnost u obradi i prenosu paketa. Ne postoji fiksni broj zaglavlja u paketu. Zaglavlja proširenja čine niz, a u polju sledeće zaglavlje (*Next Header*) svakog zaglavlja definisano je koje je sledeće zaglavlje u nizu. Poslednje

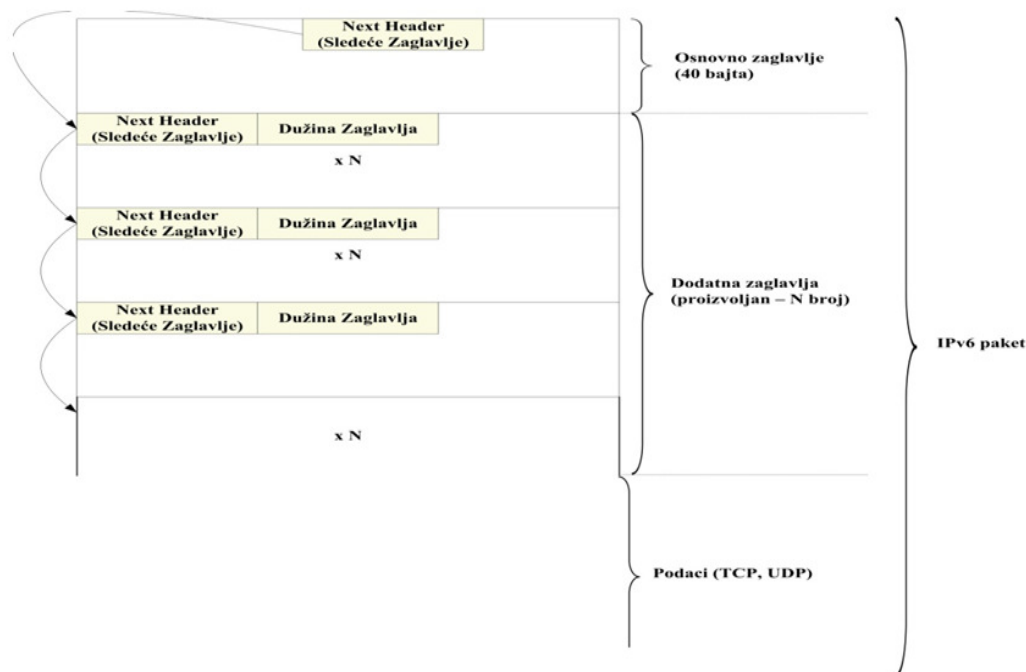
zaglavlje u nizu je vrednost podatka transportnog sloja. Na Slici 2 dat je detaljni prikaz IPv6 paketa.

Dodatna zaglavlja, po preporučenom redosledu, mogu biti:

Zaglavlje pojedinačnih skokova (eng. *Hop-by-Hop Options*): Kada se u IPv6 paketu koristi ovo zaglavlje, paket je potrebno obraditi u svakom ruteru (čvoru) na putanji paketa, izuzev njegovog odredišta. Jedan od slučajeva kada se primenjuje ovo zaglavlje je kada svaki ruter treba da “obezbedi” određeni propusni opseg za paket. Drugi slučaj je kada se radi o *velikom paketu*, tj. o paketu većem od 64 KB (*Jumbo Payload opcija*).

Zaglavlje odredišta (eng. *Destination Options*): Ovo zaglavlje prati svako *Hop-by-Hop Options* zaglavlje, i obrađuje se na odredištu ili na svakom ruteru naznačenom u dodatnom zaglavlju rutiranja. Alternativno, ovo zaglavlje može da prati i bezbednosno zaglavlje, ali u tom slučaju ono se procesuirá samo na odredištu.

Zaglavlje rutiranja (eng. *Routing Header*): U ovom zaglavlju se navode 128-bitne adrese rutera preko kojih paket mora da prođe do svog odredišta. Odrese rutera definiše izvorni uređaj i oni se, najverovatnij, razlikuju od putanje proračunate protokolom rutiranja na mreži.



Slika 2: Izgled IPv6 paketa

Zaglavlje fragmentacije (eng. *Fragment Header*): Ovo zaglavlje se koristi kada izvorni uređaj mora podeliti paket koji je veći od maksimalne prenosne jedinice, odnosno veći od MTU (eng. *Maximum Transmission Unit*) za put između sebe i odredišnog uređaja. Zaglavlje fragmentacije se koristi u svakom fragmentiranom paketu i ne može se koristiti u kombinaciji sa *Hop-by-Hop zaglavljem*.

Zaglavlje autentifikacije (eng. *Authentication Header*) i **Bezbednosno zaglavlje** (eng. *Encapsulating Security Payload - ESP*): Ova zaglavlja se koriste u IPSec bezbednosnim protokolom, kako bi obezbedili autentikaciju, integritet i poverljivost paketu. Zaglavlje autentifikacije i Bezbednosno zaglavlje su identični i za IPv4 i IPv6.

Zaglavlje mobilnosti (eng. *Mobility Header*): Ovo zaglavlje ima funkciji u komunikaciji između mobilnih čvorova, a njegova uloga će biti detaljno objašnjenja u središnjem delu ovog rada.

Kao što je već rečeno, u polju *Next Header* svakog zaglavlja, navedena je vrednost koja definiše šta sledi određeno zaglavlje. U Tabeli 1 date su moguće vrednosti *Next Header* polja. [3]

Vrednosti polja Next Header	
Next Header	Zaglavlje
0	Zaglavlje pojedinačnih skokova (eng. <i>Hop-by-Hop Options</i>)
6	TCP
17	UDP
41	Enkapsulirano IPv6 zaglavlje
43	Zaglavlje rutiranja (eng. <i>Routing Header</i>)
44	Zaglavlje fragmentacije (eng. <i>Fragment Header</i>)
46	Resource ReSerVation Protocol
50	Encapsulating Security Payload
51	Zaglavlje autentifikacije (eng. <i>Authentication Header</i>)
58	ICMPv6
59	Ne postoji sledeće zaglavlje
60	Zaglavlje odredišta (eng. <i>Destination Options</i>)
135	Zaglavlje mobilnosti (eng. <i>Mobility Header</i>)

Tabela 1: Moguće vrednosti polja *Next Header*

1.4 Predstavljane IPv6 adresa

Sa 128 bita za adresiranje hostova rešen je osnovni, može se reći i problem koji je podstakao na razvoj IPv6 protokola, a to je nedostatak adresnog prostora. Čak i da nije bilo neplanske dodale IP adresa, sa porastom ljudske populacije i porastom broja uređaja na Internetu, iscrpljivanje adresnog prostora predstavlja neminovnost. Postoji i mišljenje da je 2^{128} previše adresa. Kao argument protiv ovolikog broja bita za adresu korištena je činjenica da su za obradu izvorne i odredišne adrese, kroz CPU, magistralu ili memorijsku jedinicu od 64 bita, potrebna četiri prolaza, što u mnogome utiče na performanse sistema. Ipak, prevagnula je težnja da se problem adresnog prostora reši jednom za uvek, bez eventualnih novih iznenađenja, kao što je bio slučaj sa IPv4.

Za predstavljanje IPv6 adresa koristi se heksadecimalan prikaz, čime se 128 bitova pretvara u 32 karaktera. Zbog lakšeg pamćenja i kako bi bila prihvatljivija, IPv6 adresa sastavljena od 32 heksidecimalna karaktera se uređuje korišćenjem sledećih pravila:

- Heksidecimalni zapis se deli na 8 grupa, od po 4 karaktera, odnosno 16 bitova. Grupe karaktara se dele dvodačkom (:). Kod IPv6 se ne koristi deciman zapis adrese, kao što je to slučaj kod IPv4. Primer IPv6 adrese je: *3002:0000:0000:00B3:0000:0000:0000:1A2E*.
- Vodeće nule u svakoj grupi karaktera se mogu opciono izostaviti. Tako bi adresa data u prethodnom primeru, opciono mogla da se predstavi kao: *3002:0:0:B3:0:0:0:1A2E*.
- Izbacivanje grupa gde su sva četiri karaktera nule, odnosno njihova zamena navođenjem dve spojene dvotačke. Kako bi se omogućilo jedinstveno predstavljanje jedne adrese, ovo pravilo može da se upotrebi samo jednom tako da bi neispravno bilo adresu iz sledećeg primera zapisati kao: *3002::B3::1A2E*

, jer u ovom primeru se ne zna koliko je nula tačno izostavljeno, ali je zato pravilno napisati:

3002:0:0:B3::1A2E.

1.5 IPv6 unicast adrese

Unicast adresa identifikuje jednoznačno svaki čvor u mreži, tako da saobraćaj sa naznačenom unicast odredišnom adresom biva isporučen tom čvoru. Na ovaj način se svaki čvor čini dostupan ostalim uređajima sa kojima je on povezan, pa unicast adrese imaju kritičnu ulogu na svim mrežama. [1]

Kako bi se rutiranje učinilo jednostavnijim vrši se grupisanje IPv6 adresa, odnosno njihova agregacija. Adrese se grupišu tako što mogu da pripadaju istoj mreži ili pomoću prefiksa. Preduslov za grupisanje adresa je podela njihove strukture na dva dela:

- Identifikator mreže i
- Identifikator interfejsa.

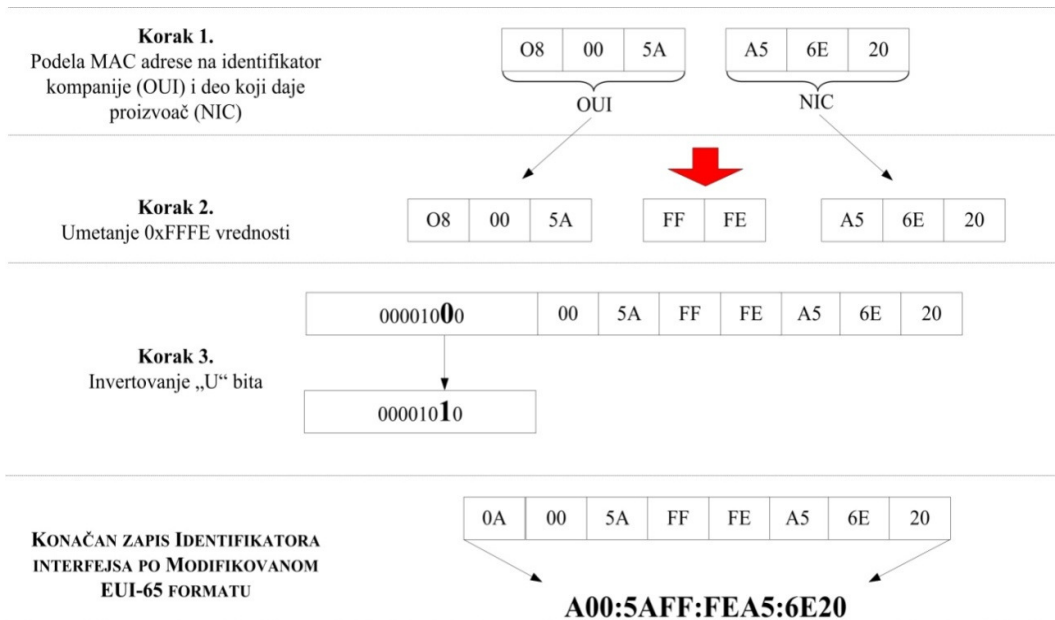
Sve unicast adrese, sem onih koje počinju sa tri nule (000), moraju da sadrže 64 bita za identifikator interfejsa. Identifikator interfejsa može biti konstruisani od 48-bitne adrese drugog sloja, odnosno MAC adrese (eng. *Media Access Control Address*), odnosno po Modifikovanom EUI-64 formatu. Glavna prednost EUI-64 formata (eng. *Extended Unique Identifier*) je eliminisanje potrebe za ručnom ili konfiguracijom IPv6 pomoću DHCP-a (DHCPv6) kao kod IPv4.

Mehanizam za kreiranje identifikatora interfejsa po Modifikovanom EUI-64 formatu je jednostavan. Najpre se MAC adresa deli na dva 24-bitna dela, tj. na deo koji označava firmu proizvođača mrežnog interfejsa – OUI (eng. *Organizationally Unique Identifier*) i jedinstvenog dela koji mrežnom interfejsu koji dodeljuje proizvođač – NIC (eng. *Network Interface Card*). Između ova dva dela umeće se vrednost 0xFFFE.

Sledeći korak je da se sedmi bit prvog bajta, odnosno univerzalni/lokalni („U“ ili U/L) bit (U/L – eng. *Universal/Local*) invertuje. "U" bit se postavlja na jedan (1) da definiše univerzalni (globalno jedinstveni) opseg, odnosno da označi lokalni opseg kad je podešen na nulu (0). Objašnjeni mehanizam je prikazan na Slici 3. [4]

Tipovi unicast adresa koje će ovde biti pojašnjene su:

- Adrese lokalne veze (eng. *Link-local Unicast Address*),
- Globalne unicast adrese (eng. *Global Local Unicast Address*),
- Jedinstvene lokalne unicast adrese (eng. *Unique Local Unicast Address*),
- Specijalne IPv6 adrese,
- Kompatibilne IPv6 adrese.



Slika 3: Kreiranje ID interfejsa po Modifikovanom EUI-64 formatu

1.5.1 Adrese lokalne veze

Prilikom priključenja uređaja (sa IPv6 podrškom) na mrežu na njegovim interfejsima se automatski konfiguriše IP adresa, odnosno adresa trećeg sloja. Ova adresa se naziva adresom lokalne veze, jer je pretežno namenjena za povezivanje uređaja na lokalnom linku, tako da uređaji ne moraju da se obraćaju ruteru prilikom komunikacije. Adrese lokalne veze koriste se i za protokol otkrivanja suseda (eng. *Neighbor Discovery*).

Adresa lokalne veze zamišljena je tako da bude nezavisna od adresne šeme koja se koristi na mreži i nije validna van svog opsega.

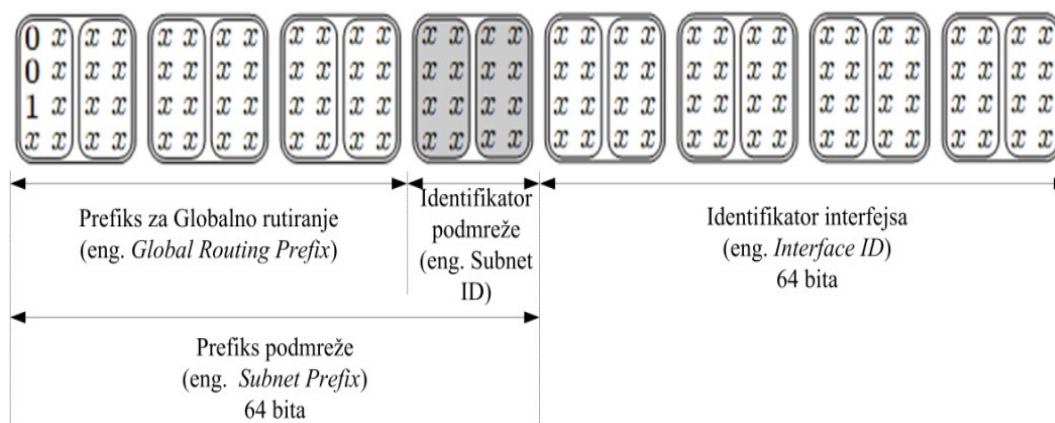
Identifikator mreže, kod adrese lokalnog linka, ima fiksni format FE80::/64, odnosno prvih deset bitova imaju vrednost *1111 1110 10*, a ostala 54 bita su nule (0). Prema tome, adresa lokalne veze interfejsa iz primera sa Slike 6 je:

FE80::A00:5AFF:FEA5:6E20.

1.5.2 Globalne unicast adrese

Globalne unicast adrese kod IPv6 su konvencionalne, javno dostupne, globalno rutabilne i jedinstvene adrese koje se mogu koristiti na Internetu ili bilo kom javnom domenu za adresiranje jednog interfejsa. Opšti format globalne unicast adrese dat je na Slici 4 [5].

Kod globalne unicast adrese identifikator mreže, odnosno prefix podmreže (eng. *Subnet Prefix*), sastoji se iz dva dela: prefiksa za globalno rutiranje i identifikatora podmreže (eng. *Subnet ID*). **Identifikator interfejsa** se i kod globalne unicast adrese koristi za identifikaciju čvorova na linku, odnosno na drugom sloju. Identifikator interfejsa može biti konstruisan po modifikovanom EUI-64 formatu.



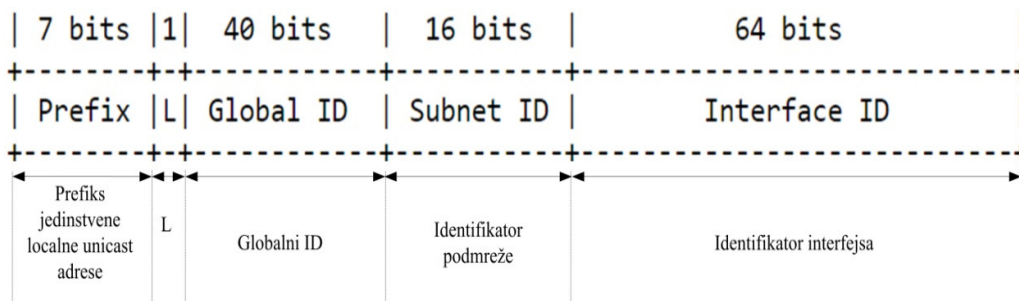
Slika 4: Opšti format globalne unicast adrese

Prefiks za globalno rutiranje (eng. *Global Routing Prefix*) se delom delegira provajderu sistema preko IANA (eng. *Internet Assigned Numbers Authority*), a preostali deo određuju provajderi sistema svojim korisnicima (organizacijama). Uobičajna dužina prefiksa za globalno rutiranje je 48 bita, a može bit i kraći. Kroz hijerarhijski struktuirani prefix za globalno rutiranje vrši se optimizacija procesa rutiranja, koji je sa porastom dužine adrese i tabela rutiranja, postao zahtevniji. Globalne unicast adrese, koje se trenutno delegiraju od strane IANA imaju opsg 2000::/3, odnosno počinju počinju binarnom vrednošću 001.

Identifikator podmreže (eng. *Subnet ID*) koristi korisnik (organizacija) za kreiranje organizacione strukture svoje mreže. [6]

1.5.3 Jedinstvene lokalne unicast adrese

Jedinstvene lokalne unicast adrese su slične privatnim adresama kod IPv4. Na Slici 5 prikazan je format jedinstvene lokalne unicast adrese.



Slika 5: Format jedinstvene lokalne unicast adrese

Jedinstvenu lokalno adresu, takođe možemo podeliti na dva dela, odnosno identifikator mreže i identifikator interfejsa. Identifikator interfejsa ima istu namenu kao i kod ostalih unicast adresa, dužine je 64 bita i može se konstruisati po modifikovanom EUI-64 formatu. Identifikator mreže, sastoji se iz sledećih delova:

- **Prefiksa lokalne jedinstvene adrese** (eng. *Prefix Unique Local Unicast Address*) koji ima vrednost FC00::/7, odnosno binarnu vrednost 1111 110 i kojim se identifikuje da je reč o lokalnoj jedinstvenoj adresi.
- **L bita** koji trenutno ima vrednost jedan (1) i zajedno sa prefiksom lokalne jedinstvene adrese identifikuje lokalno dodeljenu adresu (FD00::/8). Vrednost L bita nula (0) je ostavljena za buduće potrebe.
- **Identifikatora pod mreže** koji omogućava definisanje hijerarhijskog adresnog prostora unutar lokalnog domena. [7]

1.5.4 Specijalne IPv6 adrese

Postoje dva osnovna tipa specijalnih IPv6 adresa, **nespecifirana** (eng. *Unspecified*) i **povratna** (eng. *Loopback*) adresa.

Nespecifirana adresa kod IPv6 ekvivalentna je sa nespecifiranom IPv4 adresom (0.0.0.0). Upotrebljava se kada interfejs nema svoju IPv6 adresu. Najčešći takav slučaj je kada interfejs pokušava da odredi jedinstvenost svoje adrese, pa se nespecifirana adresa koristi kao izvorishna adresa u paketim. Ne dodeljuje nekom interfejsu, niti se koristi kao odredišna adresa. Vrednost nespecifirane adresa je 0:0:0:0:0:0:0:0 ("::"). [4]

Povratna adresa kod IPv6 je, po nameni, ekvivalentna sa IPv4 adresom 127.0.0.1. Njena vrednost je 0:0:0:0:0:0:0:1 (::1). Interfejsi je koriste radi referenciranja na samog sebe, odnosno omogućava interfejs da šalje pakete samom sebi. [4]

1.5.5 Kompatibilne IPv6 adrese

Kompatibilne adrese predstavljaju neku vrstu specijalnih adresa, privremenog karaktera, namenjenih za istovremeno koršćenje IPv4 i IPv6 protokola. Sa definitivnim i neminovnim prelaskom sa IPv4 na IPv6 protokol nestaće i potreba za postojanjem ovih adresa. Postoji nekoliko različitih definisanih vrsta ovih adresa, a najbitnije su **IPv4 kompatibilna adresa** (eng. *IPv4-Compatible IPv6 Address*) i **IPv4 mapirana adresa** (eng. *IPv4-mapped IPv6 address*).

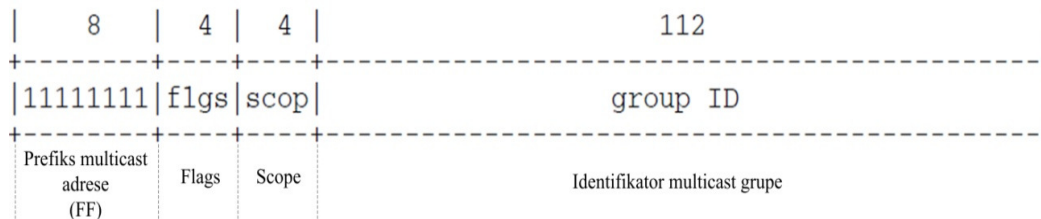
IPv4 kompatibilnu adresu koriste interfejsi koji funkcionišu i sa IPv4 i IPv6 adresama, odnosno u duplom režimu rada (eng. *dual-stack*). Kod kompatibilnih adresa IP adresa je u formatu IPv6 prezentacije, sa tim što je IPv4 adresa predstavljena sa poslednja 32 bita adresa, dok su vodećih 96 bita nule (0). Opšti format ove adrese se može predstaviti kao $0:0:0:0:0:0:A.B.C.D$, odnosno $::A.B.C.D$, gde je $A.B.C.D$ IPv4 adresa (npr. 192.168.10.2).

IPv4 mapirana adresa se koristi kada se IPv4 interfejs proglašava svoju adresu IPv6 interfejsa. Tada se njegova IPv4 adresa se “mapira” u IPv6 format i to, kao i kod kompatibilnih adresa u poslednja 32 bita. Vodećih 96 bitova imaju vrednost $0:0:0:0:0:FFFF$, tako da se IPv4 mapirana adresa može predstaviti u opštem formatu $0:0:0:0:0:FFFF:A.B.C.D$, odnosno $::FFFF:A.B.C.D$. Kada interfejs koji radi u duplom režimu rada predstavlja IPv4 adresu on to radi tako što šalje IPv4 paket (proglašava IPv4 adresu). [4]

1.6 IPv6 multicast adrese

Multicast saobraćaj kod IPv6 prepoznaje grupu interfejsa kao odredište saobraćaja. Princip je isti kao i kod IPv4, ali veći adresni prostor pruža više jedinstvenih multicast opsega na globalnom nivou.

Multicast adrese se prepoznaju po vodećih 8 jedinica (1), tako da imaju prefix $FF00::/8$. Nakon osam jedinica, sledeća četiri bita multicast adrese čine polje **Flag**, zatim slede četiri bita koja čine **Scope** polje. Ostatak adrese od 112 bita, čini **Identifikator grupe** (eng. *Group ID*) grupe. Format multicast adrese prikazan je na Slici 6. [8]



Slika 6: Format multicast adrese

Polje Flag trenutno ima funkciju za svoja poslednja tri bita, dok je vodeći bit polja trenutne vrednost nula (0) i ostavljen je kao rezerva za buduće potrebe. Poslednji bit ovog polja se obeležava sa **T** (eng. *Transient*) i označava da je multicast adresa permanentno dodeljena od strane IANA ($T=0$) ili da je nepermanentna, odnosno privremena ($T=1$). Treći bit ovog polja se obeležava sa **P** (eng. *Prefix*) i označava da li je multicast adresa formirana od unicast adrese ($P=1$) ili nije ($P=0$). Drugi bit ovog polja obeležava se sa **R** i označava da grupna multicast adresa u sebi sadrži unicast adresu **RP** (eng. *Rendezvous Point*) uređaja koji opslužuje multicast grupu ($R=1$).

Scope polje označava opseg, odnosno domen IPv6 multicast adrese. Definisane vrednosti Scope polja su date u Tabeli 2.

Binarana vrednost <i>Scope</i> polja	Heksadecimalna vrednost <i>Scope</i> polja	Domen multicast adrese
1	0001	Lokalni domen interfejsa (eng. <i>Interface-local Scope</i>)
2	0010	Lokalni domen linka (eng. <i>Link-local Scope</i>)
3	0011	Lokalni domen pod mreže (eng. <i>Link-local Scope</i>)
4	0100	Lokalni domen administrator (eng. <i>Administrator-local Scope</i>)
5	0101	Lokalni domen sajta (eng. <i>Site-local Scope</i>)
8	1000	Lokalni domen organizacije (eng. <i>Organization-local scope</i>)
E	1110	Globalni domen (eng. <i>Global scope</i>)

Tabela 2: Definisanje vrednosti polja *Scope* multicast adrese

1.7 IPv6 Anycast adrese

Anycast ili zajednička adresa je adresa kojom se adresira više od jednog interfejsa, koji obično pripadaju različitim čvorovima. Pošto anycast adresa ima istu strukturu kao i unicast adresa, uređaj se konfiguriše na taj način da “prepozna” da je adresa dodeljena njegovom interfejsu anycast. Paket sa anycast adresom kao odredišnom, rutira se ka najbližem interfejsu koji ima definisanu navedenu anycast adresu.

Anycast adrese se dodeljuju iz unicast adresnog prostora, koristeći neki od definisanih unicast formata, pa se zato i anycast adrese sintaksički ne razlikuju od unicast adresa. Kada je jedna unicast adresa dodeljena više od jednom interfejsu (najčešće čvoru), ona se pretvara u anycast adresu, a čvoru kome je dodeljena, kao što je već rečeno, mora eksplicitno da se naznači da je u pitanju anycast adresa.

Za svaku dodeljenu anycast adresu, postoji najduži prefiks P te adrese koji identifikuje topološki region u kome su svi interfejsi koji pripadaju tom anycast adresnom okviru. U regionu koji se identifikuje sa P, anycast adresa se mora održavati kao poseban ulaz u sistem usmeravanja (“host route”).

U najgorem slučaju, prefiks P od jednog anycast seta može biti prefiks nula, odnosno članovi skupa nemaju nikakav topološki lokalitet. U tom slučaju, anycast adresa mora biti održavana kao poseban ulaz rutiranja celog Interneta, što predstavlja ozbiljna ograničenja skaliranja koliko takvih "global" anycast setovi može biti podržano. Zato se očekuje da podrška za globalne anycast setove može biti nedostupna ili vrlo ograničena.

Jedna očekivana upotreba anycast adresa je da identifikuju set rutera koji pripadaju nekoj organizaciji koja pruža Internet usluge. Takođe, anycast adrese se mogu koristiti kako bi se identifikovali set ruteri prikazani na neku pod mrežu ili set rutera koji predstavlja ulaz u neki izdvojeni domen.

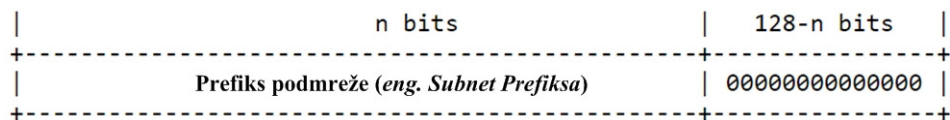
Postoji malo iskustva u korišćenju IPv6 anycast adresa, pa se zato javljaju sledeća ograničenja u upotrebi adresa:

- adresa ne sme da se koristi kao izvorna adresa IPv6 paketa,

- anycast adresa ne sme biti dodeljena IPv6 hostu, odnosno može se dodeliti samo IPv6 ruteru.

13.12.1 Format anycast adrese

Format IPv6 anycast adrese je prikazan na Slici 8.



Slika 7: Format IPv6 anycast adrese

Prvi deo anycast adrese čini „prefiks podmreže” i njegova uloga je da identifikuje specifičnu vezu (link). Anycast adresa je sintaksički ista kao unicast adresa za interfejs na link sa identifikatorom interfejsa postavljenim na nulu. [9]

Paketi poslati na neku anycast adresu bivaju isporučeni interfejsu jednog rutera, dok su svi ostali ruteri koji imaju interfejs u toj podmreži dužni da pordže tu anycast adresu i oni prime paket, ukoliko je apsolutna distanca do njih najkraća. Primer korišćenja anycast adrese je kada neki čvor mora da komunicira sa bilo kojim od seta nekih rutera.

1.8 IP mobilnost

Velika potreba za Internetom i njegova sveopšta primena doveli su do toga da savremeni informacioni uređaji (lap-topovi, mobilni telefoni, konzole, tablet i drugi uređaji) nemaju punu primenu bez globalne mreže. Brzina života savremenog čoveka i njegova pokretljivost stvaraju potrebu i da njegovi sve mobilniji uređaji mogu na bilo kom mestu i u bilo koje vreme da uspostave Internet konekciju, korišćenjem utičnice u zidu ili bežične mreže. Na ovaj način uspostavlja se određen vid mobilnosti po pitanju dostupnosti korisničkog uređaja. Međutim, na ovaj način komunikacioni uređaj konektovanjem na mrežu, mehanizmom dinamičkog adresiranja pomoću DHCP-a, dobija novi IP adresu, čima bivaju prekinute sve ranije kreirane sesije. Usled potrebe da uređaj zadrži ranije kreirane sesije IETF je razvio poseban vid mobilnosti, odnosno Mobilni Internet Protokol (MIP). Mobilni IP omogućava da komunikativni mobilni uređaji sa IP podrškom sa promenom lokacije čuvaju svoju adresu mrežnog sloja, i na taj način zadržavaju ranije kreirane sesije viših slojeva.

U sledećem poglavlju biće objašnjeni osnovni pojmovi i mehanizmi Mobilnog IP-a, za IPv6 protokol (MIPv6), sa osvrtom na funkcionisanje MIP-a kod IPv4 protokola (MIPv4).

2. IPv6 mobilnost

Mobilni IP, odnosno skraćeno MIP, je Internet Engineering Task Force standardni komunikacioni protokol koji je dizajniran da omogući prelazak mobilnih korisničkih uređaja sa jedne mreže u drugu tako da zadržavaju adresu trećeg sloja. Mobilni IP omogućava da IP adrese mobilnih čvorova ostanu iste, a u cilju pružanja servisa na višim slojevima, zatim da mobilni čvor bude raspoloživ da komunicira i sa IP mobilnim i IP fiksnim korespondentima i da mobilni čvorovi budu na podjednakom nivou sigurnosti i pouzdanosti kao i fiksni čvorovi.

Postoje dva MIP standarda, i to MIPv4 definisan za IPv4 i MIPv6 definisan za IPv6 verziju Internet Protokola. MIPv4 predstavlja trenutno primenljiviju i zbog duže upotrebe zreliju tehnologiju, međutim usled nedostataka, objašnjenih u prvom delu ovog rada, MIPv4 ima brojna ograničenja. Pretpostavka je da će upravo upotreba MIPv6 standarda, kod koga su funkcionalnosti IPv4 integrisane u IPv6 standard, dovesti do bržeg potiskivanja IPv4 od strane IPv6.

2.1 Entiteti i osnovni pojmovi MIP arhitekture

Preduslov za opis podrške za IP mobilnost je definisanje terminologije koja se koristi u ovoj funkcionalnosti. U narednim delovima teksta biće opisani osnovni entiteti i pojmovi Mobilne IP arhitekture.

2.1.1 Mobilni čvor

Mobilni čvor (eng. *Mobile Node*) – MN, je host uređaj ili ruter koji menja tačku priključenja iz jedne mreže ili podmreže u drugu. Mobilni čvor može da menja svoju lokaciju bez promene IP adrese, čija mu permanentnost omogućava da nastavi komunikaciju sa ostalim Internet čvorovima, pod pretpostavkom da je konektivnost sloja veze dostupna na tački priključenja.

2.1.2 Domicilna adresa

Mobilni čvor ima dve adrese. Prva adresa je takozvana domicilna adresa (eng. *Home Address*) – HoA, odnosno adresa dodeljena mobilnom čvoru u njegovoj domicilnoj mreži (eng. *Home Network*). Domicilna adresa ostaje nepromenjena bez obzira na to gde je mobilni čvor priključen na Internetu.

2.1.3 CoA adresa

Druga adresa je takozvana CoA (eng. *Care-of Address*) koja je privremena IP adresa za mobilni čvor koja omogućava isporuku poruka kada se čvor povezuje van domicilne mreže. CoA adresa je zapravo krajnja tačka tunela ka mobilnom čvoru, za datagrame prosledene ka njemu dok se nalazi van svoje mreže. Postoje dve vrste CoA adrese.

Prva je CoA adresa je Strana CoA adresa odnosno FCoA (eng. *Foreign Care-of Address*) koju pruža takozvani strani agent (FA) preko svoje poruke oglašavanja. U ovom slučaju, CoA adresa je IP adresa stranog agenta. Strani agent je krajnja tačka

tunela, koja prima tunelovane datagrame, deenkapsulira ih i dostavlja do mobilnog čvora. U ovom režimu, mnogi mobilni čvorovi mogu imati istu CoA adresu, što smanjuje zahteve za IPv4 adresnim prostorom, a može čuvati propusnost mreže, jer prosleđeni paketi, od stranog agenta do mobilnog čvora, nisu enkapsulirani.

Druga CoA adresa je CCoA adresa (eng. *Co-Located Care-of Address*). CCoA omogućuje mobilnom čvoru da funkcioniše bez stranog agenta (FA), na primer, u mrežama kojima još nisu raspoređeni strani agent, ili mrežama koje nemaju potrebe za postojanjem stranog agenta (IPv6 mreže). CCoA adresa se može pribaviti od nekog drugog "saradnika", kao što je DHCP servis ili se može autokonfigurirati (IPv6). I ova adresa je privremenog karaktera i na upotrebi je sve dok mobilni čvor ne napusti stranu mrežu. Za razliku od FCoA adrese, kod koje je krajnja tačka tunela strani agent, kada se koristi CCoA adresa, krajnja tačka tunela je sam mobilni čvor.

2.1.4 Domicilna i strana mreža

Mobilni IP podrazumeva da mobilni čvor ima domicilnu adresu (HoA) koja pripada domicilnoj podmreži (eng. *Home Network*) – HN. Svaka druga mreža u kojoj se mobilni čvor može naći naziva se stranom mrežom (eng. *Foreign Network*). Kad se nalazi u stranoj mreži mobilni čvor koristi privremenu, odnosno CoA adresu.

2.1.5 Domicilni agent

Domicilni, ili matični, agent (eng. *Home Agent*) – HA, je ruter domicilne mreže mobilnog čvora koji „tuneluje“ datagrame za isporuku mobilnom čvoru kada je on van domicilne mreže i održava informacije o trenutnoj lokaciji čvora, koje identifikuje na osnovu CoA adrese mobilnog čvora.

2.1.6 Strani agent

Strani agent (eng. *Foreign Agent*) – FA, je ruter koji u stranoj mreži obezbeđuje servise rutiranja za mobilni čvor sve tok je on registrovan u toj mreži. Strani agent (FA) „detuneluje“ datagrame koji su „tunelovani“ od strane domicilnog agenta (HA) i isporučuje ih mobilnom čvoru. Za datagrame poslate za mobilni čvor, strani agent može služiti kao podrazumevani ruter registrovanog mobilnog čvora.

2.1.7 Korespodentni čvor

Korespodentni čvor (eng. *Correspondent Node*) – CN, je uređaj sa kojim mobilni čvor komunicira. Kao što je već navedeno, u terminološkom smislu svaki mobilni uređaj koji poseduje karakteristiku mobilnosti naziva se mobilni čvor, dok svaki uređaj ili server koji komunicira sa mobilnim čvorom nosi naziv korespodentni čvor. Korespodentni čvor može biti ili stacionarni ili, takođe mobilni uređaj. [10]

2.2 Osnovni principi Mobilnog IP-a

Suština Mobilnog IP-a je način obavljanja tri povezane funkcije:

- Otkrivanja agenta,

- Registracije agenta i,
- Tunelovanje.

13.12.1 Funkcija otkrivanja agenta

Mobilni čvor koristi navedenu metodu otkrivanja agenta za određivanje sledećih informacija: kada je prešao iz jedne mreže u drugu; da li se nalazi u svojoj domicilnoj mreži (HN) ili u stranoj mreži (FN); koje CoA adrese su ponuđene od strane stranog agenta (FA). Funkcija otkrivanja agenta se sastoji iz mehanizma „traženje agenta“ (eng. *Agent Solicitation*) i mehanizma „oglašavanja agenta“ (eng. *Agent Advertisement*).

Mehanizam „traženja agenta“ sprovodi mobilni čvor (MN), koji kroz definisanu ICMP poruku traženja agenta oglašava svoje prisustvo i zahteva navedene podatke. Učestalost oglašavanja mobilnog čvora je ograničena na slanje tri ICMP poruke u prvoj sekundi nakon što se mobilni čvor nađe u stranoj mreži. Nakon registracije mobilnog čvora broj slanja ICMP poruke u jedinici vremena se smanjuje.

Mehanizam „oglašavanja agenta“ sprovodi strani agent (FA), koji kroz definisanu ICMP poruku oglašavanja agenta oglašava svoje prisustvo i nudi navedene podatke. Može se desiti da je strani agent preuzet da opsluži dodatne mobilne čvorove. Međutim, strani agent i tada mora da nastavi da šalje poruke oglašavanja. Na ovaj način, mobilni čvorovi koji su već registrovani sa njim će znati da nisu preselili van dometa stranog agenta u novu stranu mrežu (MN), ili da strani agent nije uspeo obezbedi informacije koje mobilni čvor traži od njega.

13.12.2 Funkcija registracije agenta

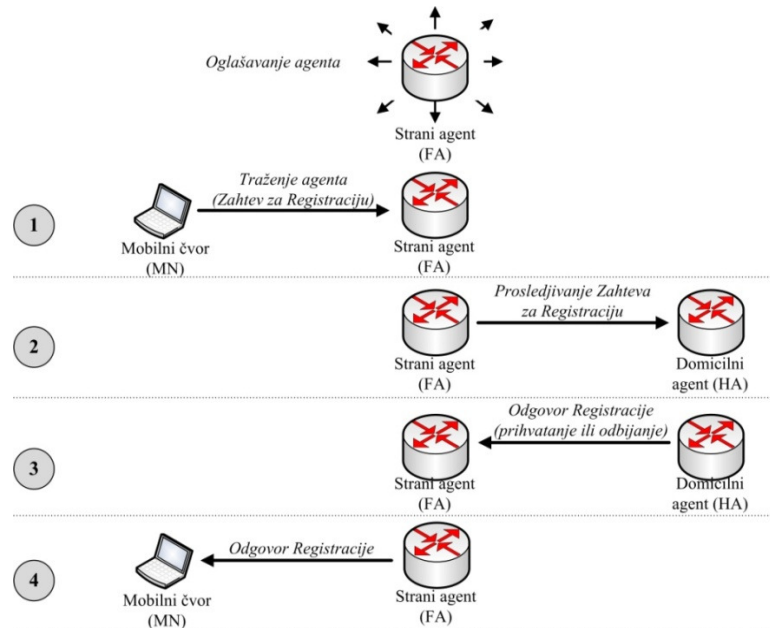
Za mobilni čvor možemo reći da je završio otkrivanje agenta, ukoliko zna da li se nalazi u svojoj domicilnoj ili u stranoj mreži. Ako se mobilni čvor nalazi u domicilnoj mreži on se ponaša kao običan IP uređaj, ali ukoliko se nalazi u stranoj mreži on komunicira kao Mobilni IP uređaj. Ovo zahteva da mobilni čvor razmeni podatke i instrukcije sa svojim domicilnim čvorom i obavesti ga o svom statusu. Metod pomoću koga mobilni čvor obaveštava svoj domicilni agent o svojim trenutnim podešavanjima naziva se registracija agenta, ili skraćeno registracija. Pojednostavljeno, kada se mobilni čvor nađe van svoje domicilne mreže, nakon dobijanja potrebnih informacija, on mora pribavljenu CoA adresu da registruje domicilnom agentu (HA), kako bi domicilni agent mogao da presretnute pakete namenjene za mobilni čvor i tuneluje ka privremenoj CoA adresi.

Postoje dva različita algoritma definisana za registraciju, u zavisnosti od vrste CoA adrese mobilnog čvora, kao i da li se čvor registruje (eng. *Registration*) na stranoj mreži, deregistruje (eng. *Deregistration*) tj. ponovo prijavljuje na svojoj domicilnoj mreži nakon povratka u nju, ili se reregistruje (eng. *Reregistration*) nakon prelaska u drugu stranu mrežu ili u slučaju isteka njegove registracije u stranoj mreži u kojoj se trenutno nalazi.

Prva, jednostavniji algoritam obično se koristi kada mobilni čvor koristi CCoA adresu. U toj situaciji, mobilni čvor može lako direktno da komunicira sa domicilnim agentom i

podešen je tako da neposredno prima informacije i datagrame od njega. Kada u stranoj mreži ne postoji strani agent, ovo je metoda koja se mora koristiti. Takođe, ova metoda se koristi kada se mobilni čvor deregistruje svom domicilnom agentu nakon povratka u domicilnu mrežu. Ova metoda ima samo dva koraka:

- Mobilni čvor (MN) šalje zahtev za registracije domicilnom agentu (HA).
- Domicilni agent (HA) vraća registracioni odgovor mobilnom čvoru.



Slika 8: Algoritam registracije agenta kada se koristi FA

Drugi algoritam registracije se koristi kada mobilni čvor koristi FCoA adresu, odnosno kada se registruje ili reregistruje. U ovoj situaciji, mobilni čvor nema svoju jedinstvenu IP adresu, već se koristi zajednička adresa stranog agenta, što isključuje direktnu komunikaciju između čvora i domicilnog agenta. [10] Algoritam registracije u ovim slučajevima prikazan je na Slici 8, i u ovoj situaciji proces ima četiri koraka:

- Mobilni čvor (MN) šalje Zahtev za Registraciju stranom agentu (FA).
- Strani agent (FA) obrađuje Zahtev za Registraciju i prosleđuje ga domicilnom agentu (HA).
- Domicilni agent (HA) šalje Odgovor Registracije stranom agentu (FA).
- Strani agent (FA) obrađuje Odgovor Registracije i prosleđuje ga mobilni čvoru (MN).

13.12.3 Tunelovanje

Paketi koji se šalju ka mobilnom čvoru bivaju "presretnuti" od strane njegovog domicilnog agenta i zatim tunelovani do mobilnog čvora preko njegove CoA adrese. Tunelovanje je metoda kojim se originalni paket enkapsulira podacima u zaglavlju koji se koriste za njegovo rutiranje, tako da je sam sadržaj paketa jasan samo njegovoj

početnoj i odredišnoj tački. Tunel je logička putanja kojom se enkapsulirani podaci usmeravaju kroz Internet. Kod Mobilnog IP-a jedan kraj tunela se uvek nalazi na domicilnom agentu (HA), dok se drugi kraj tunela može naći ili na stranom agentu (FA) ili na mobilnom čvoru (MN), u zavisnosti da li postoji FA ili ne.

Na jednom kraju tunela podaci se enkapsuliraju, zatim se tunelom usmeravaju kroz Internet, a pri stizanju na drugi kraj tunela vrši se deenkapsulacija paketa. Proces opisan u prethodnoj rečenici naziva se tunelovanje.

2.3 MIPv4 i njegova slabosti i ograničenja

Mobilni IP za IPv4 definiše da mobilni čvor (MN) mora da poseduje dve adrese, domicilnu adresu (HoA) domicilne podmreže (HN) i adresu (CoA), odnosno FCoA, koji dobija kada se prijavi na stranu podmrežu (FN).

2.5.1 Suština Mobilnog IP-a za IPv4

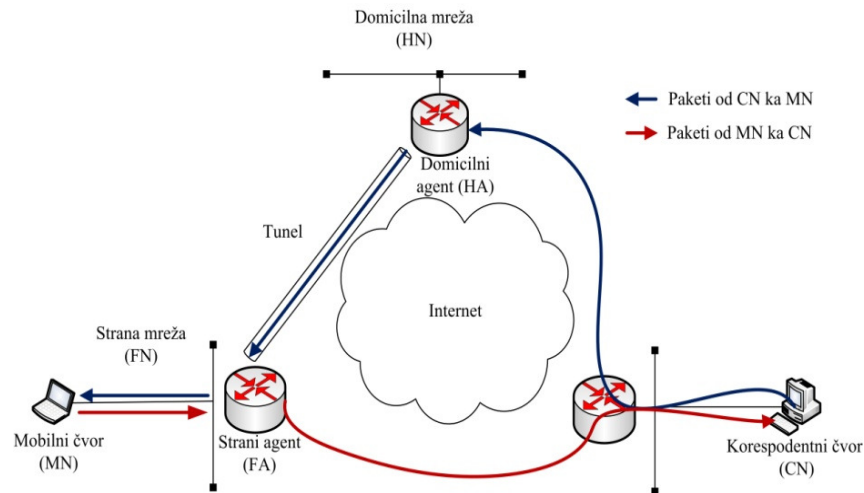
MIPv4 funkcioniše po principu posredovanja na mrežnom nivou ka stvarnoj lokaciji mobilnog čvora. Paketi koji se šalju od korespodentnog čvora (CN) ka mobilnom čvoru (MN) bivaju poslani do domicilnog agenta (HA). Domicilni agent vrši posredovanje obezbeđujući tunelovanje paketa adresiranih na HoA ka CoA adresi koju je mobilni čvor dobio u stranoj mreži, gde se nalazi kao posetilac. Kad se mobilni čvor kreće kroz stranu mrežu, njegov saobraćaj biva direktno poslat ka CN. [10]

2.5.2 Slabosti i ograničenja Mobilnog IP-a za IPv4

Zbog prirode IPv4 Mobilni IPv4 ima određene slabosti i ograničenja. Kao što je navedeno paketi poslani od strane korespodentnog čvora ka mobilnom čvoru moraju da se rutiraju preko domicilnog agenta mobilnog čvora. U suprotnom smeru, moguća je direktna komunikacija, odnosno paketi koje šalje mobilni čvor mogu biti direktno rutirani korespodentnom čvoru. Ovo dodatno rutiranje naziva se tripartitno (trougaono) rutiranje i predstavlja prvi problem MIPv4 protokola. Tripartitno rutiranje prikazano je na Slici 8. Dodatno rutiranje nije optimalno, posebno u slučajevima kada je korespodentni čvor veoma blizu mobilnog čvora.

Drugi nedostatak MIPv4 je preopterećenje. Enkapsulacijom paketa radi njegovog tunelovanja dolazi do preklapanja pojedinih polja iz zaglavlja novog enkapsuliranog paketa u originalni paket. Ovo dovodi do nepotrebnog i neekonomičnog trošenja prostora, a kao posledica može da dovede do smanjenje propusnih resursa mreže, odnosno da izazove preopterećenje mreže.

Prethodna navedena ograničenja, u kombinaciji sa činjenicom da sav saobraćaj od korespodentnog čvora do mobilnog čvora mora da prođe preko domicilnog agenta, koji kao takav predstavlja usko grlo, ali i moguću tačku otkaza za MIPv4, mogu da dovedu do problema u funkcionisanju aplikacija koje imaju potrebu za prenos podataka u realnom vremenu. Mogućnost otkaza domicilnog agenta se naziva i fragilnost (eng. *Fragility*). Fragilnost se može nedomestiti sa ugradnjom više domicilnih agenta u domicilnoj mreži. Time se postiže da, ukoliko jedan domicilni agent otkaže, drugi preuzme njegovu ulogu i nastavi preusmeravanje paketa ka mobilnom čvoru.



Slika 9: Problem tripartitnog rutiranja kroz princip funkcionisanja MIPv4

Sledeća slabost MIPv4 je potreba za postavljanjem stranih agenta u stranoj mreži. Samo tako je omogućeno da se odredi kretanje mobilnog čvora i da mu se dodeli CoA adresa. U mreži u kojoj ne postoji raspoređeni strani agent nije ni moguće povezivanje mobilnog čvora.

Verovatno najveća slabost kod MIPv4 je bezbednost. Kao što je već rečeno, paketi od mobilnog čvora do korespondentnog čvora se ne tuneluju, pa se domaćina adresa mobilnog čvora (HoA) koristi kao izvorišna adresa IPv4 paketa. Pošto je ova adresa topološki neispravna i ne pripada stranoj mreži, granični ruteri za filtriranje saobraćaja i firewall uređaji mogu da odbace i blokiraju pakete čija izvorna adresa ne pripada internom opsegu izvornošne mreže. Navedeni paketi mogubiti meta takozvanog spoofinga (metoda za zamenu IP adrese čvora koja mu dozvoljava da se maskira kao neki drugi čvor).

Navedena ograničenja i slabosti mogu biti ublaženi ili otklonjeni dodatnim mehanizmima. Međutim, Mobilnost za IPv6 ima podrazumevane mehanizme za ove slabosti. [10]

2.4 Osnove IPv6 Mobilnosti

Protokol MIPv6 je razvijen sa očekivanjem da, koristeći potencijale IPv6, otkloni i prevaziđe slabosti koje pokazuje MIPv4.

U osnovi, funkcionisanje IPv6 Mobilnosti je slično funkcionisanju IPv4 Mobilnosti. Mobilni čvor takođe mora da odredi svoju trenutnu lokaciju. Kada je mobilni čvor u svojoj domaćinskoj mreži on se ponaša kao fiksni čvor. Za razliku od MIPv4 kod IPv6 Mobilnosti mobilnom čvoru se, kada se nalazi van domaćinske mreže, pridružuju tri IP adrese. Prva adresa je, kao i kod MIPv4, domaćinska adresa (HoA) koja je permanentna, odnosno ne menja se sa promenom lokacije mobilnog čvora. Druga IP adresa pridružena mobilnom čvoru je njegova trenutna adresa lokalne veze (eng. *Link-local Unicast Address*). Treća IP adresa je CoA adresa, analogna CoA adresi kod MIPv4. CoA adresu mobilni čvor ima kada se nađe u stranoj mreži, ali za razliku od MIPv4,

CoA adresa kod MIPv4 se autokonfiguriše, tako da nije potrebno postojanje stranog agenta u stranoj mreži da bi se ostvarila funkcija mobilnosti, zato je ovde u upotrebi CCoA (*Co-Located Care-Of-Address*) kao vrste CoA adrese. Prefiks mreže CoA adrese mobilnog čvora je isti kao prefiks strane mreže u kojoj se mobilni čvor trenutno nalazi. Na taj način paketi upućeni ovoj CoA bivaju usmeravani normalnim mehanizmima Internet rutiranja.

IPv6 mobilnost, svojim funkcijama povezivanja, omogućava stvaranje dvosmernog tunela. Adresa domicilnog agenta (HA) nalazi se na jednom kraju tunela, dok je drugi kraj vezan za CoA adresu mobilnog čvora. Dvosmernost tunela se ogleda u tome da i paketi koji idu od mobilnog čvora prelaze preko domicilnog agenta, kao i oni koji idu ka mobilnom čvoru. Na ovaj način omogućena je topološka ispravnost adrese paketa i izbegava se problem mogućeg odbacivanja paketa od starane firewall-ova i rutera za njihovo filtriranje.

Ostvarivanje IPv6 Mobilnosti čvora podrazumeva ostvarenje sledećih uslova:

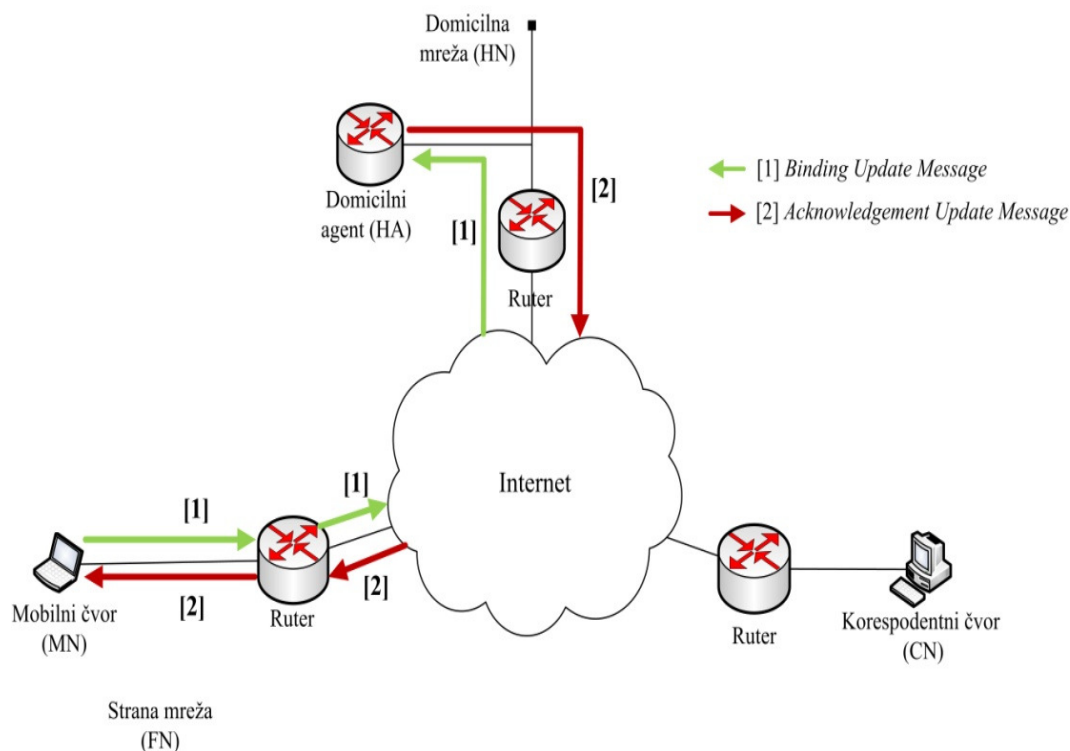
- Mobilni čvor (MN) mora da odredi svoju trenutnu lokaciju;
- Domicilni agent (HA) mora da stekne sposobnost da presreće pakete namenjene mobilnom čvoru;
- Mobilni čvor (MN) mora da obaveštava ostale čvorove u komunikaciju o svojoj trenutnoj CoA adresi;
- Paketi od Mobilnog čvora moraju biti direktno rutirani.

2.5 Operacije IPv6 mobilnosti

Mobilni čvor može imati jednu ili više CoA adresa dok je vezan za neki strani link, van svoje domicilne (matične) mreže. Dokle god mobilni čvor ima određenu CoA svi paketi adresirani na tu adresu biće dostavljani mobilnom čvoru. Prefiks CoA adresa mobilnog čvora je isti kao i prefiks podmreže pojedinačnog linka na kome je on trenutno povezan. Mobilni čvor može konfigurisati svoju CoA adresu na dva načina, i to:

- Nezavisnim mehanizmima atokonfiguracije adrese (eng. *Stateless autoconfiguration*), gde je CoA address = Network Prefix + Interface ID i
- Pomoću dodatnih servisa u stranoj mreži (eng. *Stateful autoconfiguration*), kao što je DHCPv6.

Asocijacija između domicilne adrese mobilnog čvora i CoA adrese se naziva “vezivanjem” (eng. *Binding*) mobilnog čvora. Kada se mobilni čvor nađe u stranoj mreži on registruje svoju primarnu CoA adresu ruteru (domicilnom agentu) u svojoj domicilnoj mreži. Registraciju vezivanja (eng. *Binding Registration*) obavlja mobilni čvor slanjem “poruke ažuriranja vezivanja” (eng. *Binding Update Message*) domicilnom agentu. Domicilni agent odgovara mobilnom čvoru, slanje “poruke potvrde vezivanja” (eng. *Binding Acknowledgement*). Proces registracije mobilnog čvora je dat na Slici 9.



Slika 10: Proces registracije MN kod MIPv6

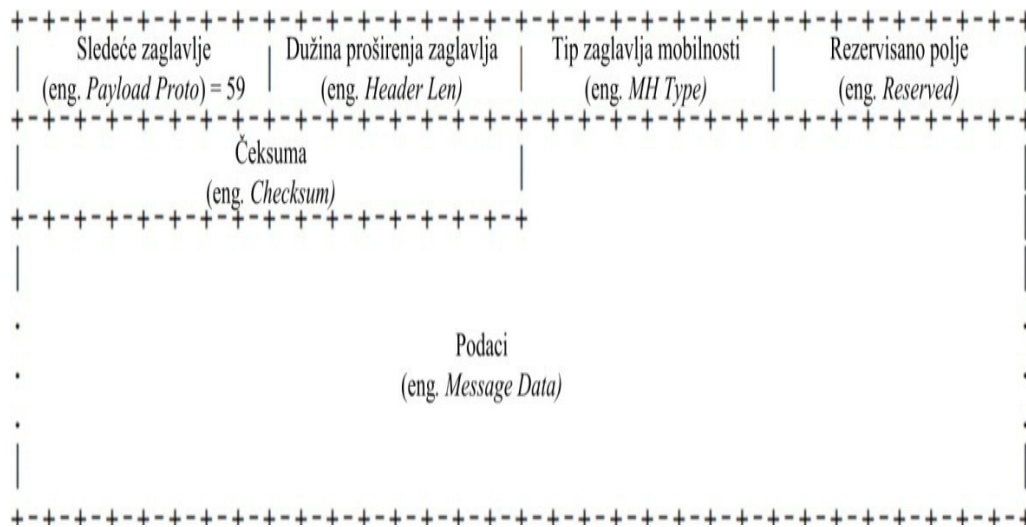
2.6 Zaglavlje za IPv6 mobilnost

Zaglavlje za IPv6 mobilnost, odnosno zaglavlje mobilnosti (eng. *Mobility Header*) je proširenje IPv6 zaglavlja, koje koriste mobilni čvorovi, korespondentski čvorovi i domicilni agenti u svim porukama koje se odnose na kreiranje i upravljanje funkcijama povezivanja. Zaglavlje mobilnosti se u polju “sledeće zaglavlje” (*Next Header*) u prethodnom zaglavlju ili osnovnom IPv6 zaglavlju, najavljuje vrednošću 135 (Tabela 1 ovog rada).

Opšti format zaglavlja za IPv6 mobilnost prikazan je na Slici 12, i njega čine sledeća polja:

- **Sledeće zaglavlje** (eng. *Payload Proto*) je osmобitno polje koje definiše tip zaglavlja koje sledi nakon zaglavlja mobilnosti. Ovo polje se može uporediti sa poljem osnovnog zaglavlja “sledeće zaglavlje” (*Next Header*) i ono je planirano da bude korišćeno u budućim proširenjima, pa je samim tim njegova trenutna vrednost 59 (ne postoji sledeće zaglavlje).
- **Dužina proširenja zaglavlja** (eng. *Header Len*) je takođe osmобitno polje, koje predstavlja dužinu zaglavlja mobilnosti u jedinicama od 8 okteta, ne računajući prvih 8 okteta.

- **Tip zaglavlja mobilnosti** (eng. *MH Type*) je osmobaritni selektor. Identifikuje koja je poruka mobilnosti u pitanju. Nepriznata vrednost MH Tip polja uzrokuje indikaciju greške.
- **Rezervisano polje** (eng. *Reserved*) je, kao i prethodna polja, osmobaritno i rezervisano je za buduću upotrebu. Pošiljaoc vrednost ovog polja mora da postavi na nulu, dok od strane primaoca polje mora biti ignorisano.
- **Kontrolno polje** (eng. *Checksum*) je polje od šesnaest bita. Koristi se kao kontrolno polje zaglavlja mobilnosti.
- **Podaci** (eng. *Message Data*) je polje promenljive dužine koji sadrži podatke specifične za naznačeni tip zaglavlja mobilnosti. [11]



Slika 11: Opšti format zaglavlja IPv6 mobilnosti

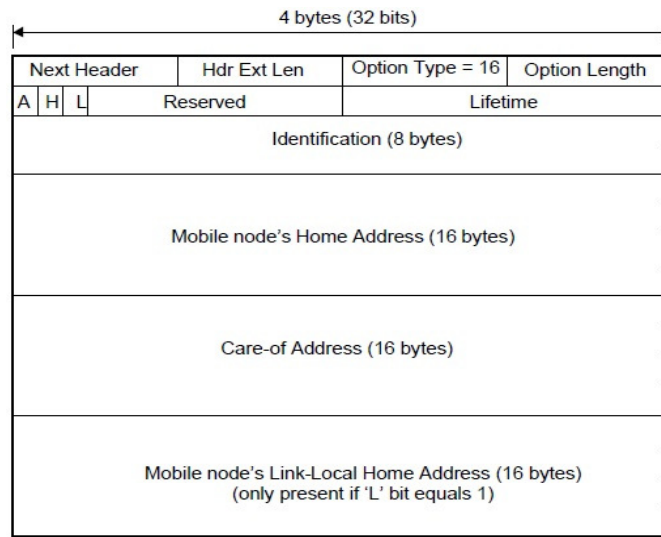
2.7 Poruke MIPv6

Poruke koje se koriste kod Mobilnog IPv6 protokola definisane su u zaglavlju proširenja opcije destinacije (eng. *Destination Options*). Opcije destinacije se upotrebljavaju da nose dodatne informacije koje treba ispitati samo na čvorovima destinacije. U sledećem delu biće objašnjene poruke koje se koriste u procesima registracije čvora. Zaglavlje za mobilnost se javlja u dva različita toka. Prvi je tok uspostavljanja vezivanja, odnosno asocijacije, a drugi je tok u okviru procedure utvrđivanja povratne rutabilnosti – RR (eng. *Return routability*) [11]. Na ovaj način se za MIPv6 obezbeđuje optimizacija rute.

Postoje četiri opcije destinacije za MIPv6:

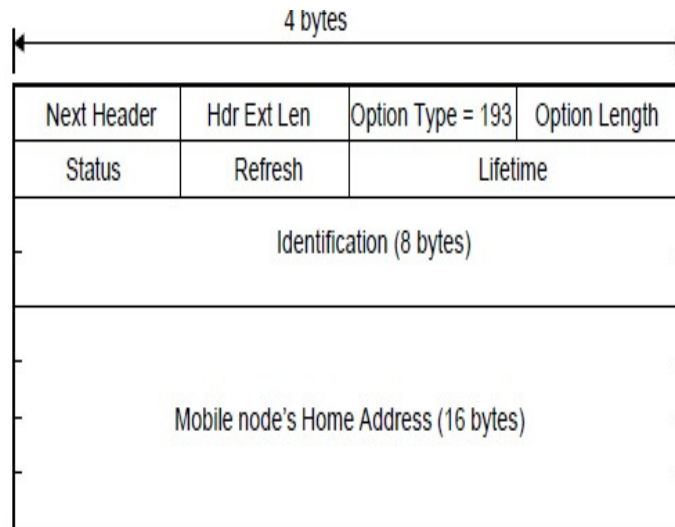
1. **Ažurivanje vezivanja** (eng. *Binding update*) koristi mobilni čvor da ažurira informacije kod korespondentnog čvora ili domicilnog agenta mobilnog čvora o svom trenutnom vezivanju. Preko ažuriranja vezivanja mobilni čvor vrši

registraciju svoje primarne *care-of* adrese kod domicilnog agenta. Ova registracija označava se kao “*home registration*”.



Slika 12: Zaglavlje opcija destinacija koje sadži opciju za ažuriranje vezivanja

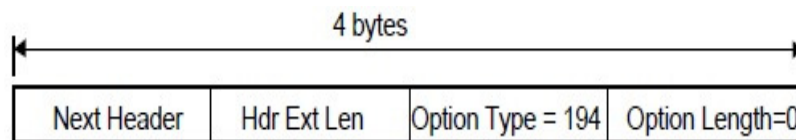
2. **Potvrda vezivanja** (eng. *Binding acknowledgement*) se koristi da se potvrdi prijem ažuriranja.



Slika 13: Zaglavlje opcija destinacija koje sadži opciju potvrde ažuriranja

3. **Zahtev vezivanja** (eng. *Binding request*) koristi svaki čvor da zahteva od mobilnog čvora slanje ažuriranja vezivanja sa svojom trenutnom *care-of* adresom. Zahtev za osvežavanjem vezivanja koristi korespodentni čvor kako bi tražio od mobilnog čvora da ponovo uspostavi vezivanje sa njim. Ova opcija destinacija se obično koristi kada postoji aktivno vezivanje, ali je njegov životni vek na isteku, pa ga je potrebno osvežiti. Kao indikaciju postojanja aktivnog vezivanja, na osnovu koje se šalje zahtev za osvežavanjem, korespodentni čvor

može koristiti nedavni saobraćaj ostvaren sa korespondentnim čvorom ili to može otkriti na osnovu otvorenog transportnog sloja.



Slika 14: Zaglavlje opcija destinacija koje sadži opciju zahteva vezivanja

4. **Home address** se koristi u paketu koji šalje mobilni čvor da informiše primaoca tog paketa o svojoj domicilnoj adresi.

Polje tip zaglavlja za mobilnost kod MIPv6 identifikuje sledeće poruke definisane u opcijama odredišta [11]:

Poruka zahteva za osvežavanjem ažuriranja vezivanja (eng. *Binding refresh request message*), odnosno BReq, je poruka koju šalje korespondentni čvor da zahteva od mobilnog čvora da ažurira svoje trenutno vezivanje. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 0.

Inicijalnu domicilnu test poruku (eng. *Home test init message*), odnosno skraćeno HoTI, koristi mobilni čvor da inicira proceduru povratne rutabilnosti i da zahteva domicilni *keygen token* od korespondentnog čvora. *Keygen token* predstavlja broj koji korespondentni čvor obezbeđuje kako bi mobilni čvor mogao da proračuna potrebni ključ za uspostavljanje asocijacije, odnosno vezivanja, koji se koristi za autorizaciju ažuriranja vezivanja. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 1.

Inicijalna care-of test poruka (eng. *Care-of test Init Message*), skraćeno CoTI, koristi se od strane mobilnog čvora da bi se inicirala procedura povratne rutabilnosti i da mobilni čvor zahteva *care-of keygen token* od korespondentnog čvora. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 2.

Domicilna test poruka (eng. *Home test message*), skraćeno HoT, je odgovor na inicijalnu domicilnu test poruku, i šalje je korespondentni čvor mobilnom čvoru. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 3.

Care-of test poruka je odgovor na inicijalnu *care-of test* poruka (CoTI), i šalje je korespondentni čvor mobilnom čvoru. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 4.

Poruka ažuriranja vezivanja (eng. *Binding Update*), skraćeno BU, se koristi od strane mobilnog čvora radi obaveštavanja ostalih čvorova o posedovanju nove *care-of* adrese. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 5.

Poruka potvrde vezivanja (eng. *Binding acknowledgement message*), odnosno BA, koristi se kao potvrda ažuriranja vezivanja. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 6.

Poruku greške vezivanja (eng. *Binding Error Message*), skraćeno Berr – Binding Error, koristi korespondentni čvor kako bi poslao signal o postojanju greške u vezi

mobilnosti. Primer greške može biti kada postoje pokušaji korišćenja opcije odredišta iz HoAddr bez postojanja uspostavljenog vezivanja. Ova poruka koristi zaglavlje mobilnost kod koga *polje tip zaglavlja* mobilnosti ima vrednost 7.

Kako bi izvršio registraciju, mobilni čvor šalje potpisanu *unicast* poruku ažuriranja (BU) domicilnom agentu, koristeći zaglavlje opcija destinacija dato na Slici 11, a u kome naznačava svoju domicilnu i *care-of* adresu. Da bi se prihvatilo novo vezivanje, domicilni agent proverava autentičnost naznačene *care-of* adrese, odnosno da li se ona možda već ne koristi sa nekim drugim domicilnim agentom ili možda već postoji na tom linku. Navedena provera se obavlja preko mehanizma za otkrivanja duplikata adresa (eng. *Duplicate Address Discovery*). Domicilni agent nakon prihvatanja vezivanja, koristi poruku potvrde vezivanja (BA) kako bi mobilni čvor obavestio o pozitivnom ishodu.

2.8 ICMP za IPv6 u funkciji MIPv6 i dinamičko otkrivanje adrese domicilnog agenta

ICMPv6 (eng. *Internet Control Message Protocol for IPv6*) je integralni deo IPv6 protokola koji omogućava čvorove da izvršavaju kontrolne funkcije i izveštavaju o greškama. Glavne funkcije ICMPv6 su:

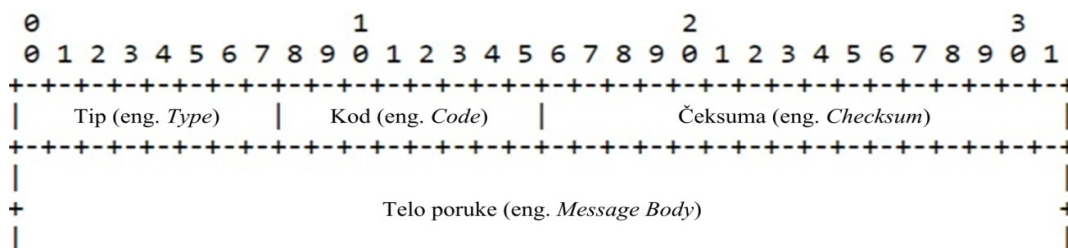
- Izveštavanje o greškama (eng. *Error Reporting*),
- Mrežna dijagnostika (eng. *Network Diagnostics*),
- Otkrivanje suseda (eng. *Neighbor Discovery*),
- Izveštavanje o pripadnosti multicast adresi (eng. *Multicast Membership Reporting*),
- Traženje i oglašavanje rutera (eng. *RouterHA Solicitation and RouterHA Advertisements*).

Svakoj ICMPv6 poruci prethodi IPv6 zaglavlje i nijedno ili više IPv6 zaglavlja proširenja. ICMPv6 zaglavlje se identifikuje vrednošću 58 polja *sledeće zaglavlje* (*Next Header*) u prethodnom zaglavlju ili osnovnom IPv6 zaglavlju [12]. Opšti format ICMPv6 je dat na Slici 14.

Polje Tip (eng. *Type*) označava vrstu poruke. Njegova vrednost određuje format ostalih podataka u poruci.

Polje Kod (eng. *Code*) zavisi od vrste poruke i koristi se za kreiranje dodatnih podataka u poruci.

Kontrolno polje (eng. *Checksum*) sa podacima iz IPv6 zaglavlja čini takozvani pseudo-zaglavlje, i omogućava ICMPv6 poruci da proveri integritet IPv6 zaglavlja.



Slika 15: Opšti format ICMPv6 poruke

MIPv6 protokol uključuje poruke za traženje (eng. *RouterHA Solicitations*) i oglašavanje rutera (eng. *RouterHA Advertisements*), koje postoje definisane i kod ICMP za IPv4, kao četiri nova tipa ICMPv6 poruka. Dva od ovih tipova se koriste za mehanizam dinamičkog otkrivanja adrese domicilnog agenta, a druge dve se koriste za renumeraciju i konfigurisanje adrese mobilnog čvora [1]. U Tabeli 3 su prikazane ICMPv6 koje su uključene u protokol IPv6 Mobilnosti.

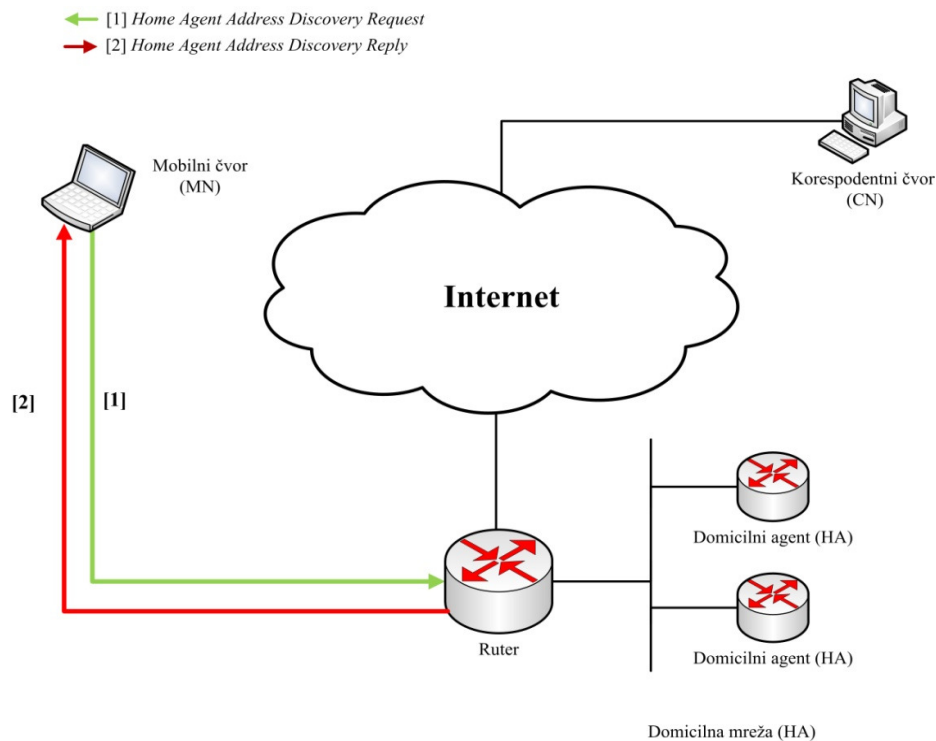
Funkcija ICMPv6 poruke	Vrednost polja Tip
Poruka traženje ruter (eng. <i>RouterHA Solicitations</i>)	133
Poruka oglašavanje rutera (eng. <i>RouterHA Advertisements</i>)	134
Poruka zahteva za otkrivanjem adrese domicilnog agenta (eng. <i>Home Agent Address Discovery Request</i>)	144
Poruka odgovora otkrivanja adrese domicilnog agenta (eng. <i>Home Agent Address Discovery Reply</i>)	145
Poruka traženja prefiksa mobilnog čvora (eng. <i>Mobile Prefix Solicitation</i>)	146
Poruka oglašavanja prefiksa mobilnog čvora (eng. <i>Mobile Prefix Advertisement</i>)	147

Tabela 3: ICMPv6 poruke uključene u MIPv6

Dinamičko otkrivanja adrese domicilnog agenta (eng. *Dynamic Home Agent Address Discovery*), skraćeno DHAAD, je samostalni, nezaštićeni mehanizam čija je namena da otkrije koji je, odnosno koji su, domicilni agenti dostupni na domicilnom linku mobilnog čvora. Mehanizam dinamičkog otkrivanja adrese domicilnog agenta se sastoji iz dva toka. Prvi tok čini *ICMPv6 poruka zahteva za otkrivanjem adrese domicilnog agenta* koju formira mobilni čvor i šalje je na *anycast* adresu svojih domicilnih agenta. *Anycast* adresu formira mobilni čvora na osnovu rezervisanog mrežnog sufiksa i prefiksa svoje podmreže. [13] Pomoću proširenja protokola za otkrivanje suseda domicilni agenti se otkrivaju na domicilnom linku, tako da kada neki domicilni agent primi DHAAD zahtev on preko *ICMPv6 poruke odgovora otkrivanja adrese*

domicilnog agenta ostvaruje drugi, povratni tok DHAAD mehanizma u kome mobilnom čvoru obezbeđuje uređenu listu domicilnih agenata.

Po odabiru agenta za priključenje u stranoj mreži, mobilni čvor dobija topološki ispravnu IPv6 adresu, koja predstavlja njegovu *care-of* adresu. [1] *Care-of* adresa, koja se najčešće konfiguriše automatski na jedan od dva ranije navedena načina, je izvor DHAAD procesa prikazanog na Slici 15.



Slika 16: DHAAD mehanizam

2.9 Optimizacija putanje

Jedan od načina komunikacije između mobilnog i korespondentnog čvora je optimizacija putanje (eng. *Route Optimization*). Preduslov za ovakav način komunikacije je da mobilni čvor izvrši registraciju svog trenutnog “vezivanja” direktno kod korespondentnog čvora, a ne kod domicilnog agenta. Na ovaj način, paket čiji je pošiljalac korespondentni čvor biva direktno poslat mobilnom čvoru na njegovu CoA adresu. Prilikom slanja paketa nekom IPv6 odredištu, korespondentni čvor proverava da li se adresa odredišta nalazi u njegovom “kešu vezivanja” (eng. *Cached Bindings*). Ukoliko je za mobilni čvor pronađeno “keširano vezivanje”, korespondentni čvor koristi novi tip zaglavlja IPv6 mobilnosti da usmeri paket ka mobilnom čvoru, koristeći njegovu CoA adresu definisanu u pronađenom vezivanju. Usmeravanje paketa direktno ka mobilnom čvoru preko njegove CoA adrese skraćuje, odnosno optimizuje put koji će se koristiti.

Pri optimizaciji putanje, korespodentni čvor adresu destinacije u IPv6 zaglavlju postavlja na CoA adresu mobilnog čvora. Takođe, mobilni čvor postavlja za izvorišnu adresu paketa u IPv6 zaglavlju svoju trenutnu CoA adresu. Kako bi čuvao svoju domicilnu adresu, mobilni čvor dodaje novu IPv6 opciju odredišta domicilne adrese. U tom slučaju mobilni čvor može da ne zna adresu svog domicilnog agenta, čak može da menja prefiks domicilne mreže tokom vremena. Mehanizam dinamičkog otkrivanja adrese domicilnog agenta omogućava mobilnom čvoru da dinamički otkrije IPv6 adresu domicilnog agenta na svom domicilnom linku, čak i kada je mobilni čvor daleko od svoje domicilne mreže. Mobilni čvorovi mogu da nauče nove informacije o prefiksu domicilne mreže preko mehanizma otkrivanja mobilnog prefiksa. [1]

2.10 Zaštita Mobilnog IPv6

Problem zaštite je ozbiljno razmatran u okviru dokumenata koji opisuje MIPv6. Kroz različita karakteristike, koristeći Ipsec, Mobilni IPv6 je kreiran tako da se u okviru njegovog funkcionisanja dokaže identitet svih aktera komunikacije kroz uspostavljanje povratne rutabilnosti (RR).

U okviru MIPv6 obezbeđena je zaštita ažuriranja vezivanja i za domicilne agente i za korespodentne čvorove, i to na dva načina: zaglavljem proširenja za IPsec ili opcijom autorizacije podataka vezivanja (eng. *Binding Authorization Data*). Opcija autorizacije podataka vezivanja podrazumeva definisanje ključa za upravljanje vezivanjem (eng. *Binding Management Key*), odnosno KBM, prilikom procedure ostvarivanja povratne rutabilnosti. Korišćenjem IPsec-a omogućava se i zaštita otkrivanja prefiksa mobilnog čvora.

Veoma je bitno da u slučaju napada budu zaštićeni i paketi sa korisnim sadržajem. Ovde se misli na pakete koji sadrže domicilnu adresu (HoAddr) opcija odredišta i zaglavlje za rutiranje. U tu svrhu postavljeno je ograničenje da se polje HoAddr opcije odredišta koristi samo kada korespodentni čvor u svom „kešu vezivanja“ ima zapis za navedenu domicilnu adresu.

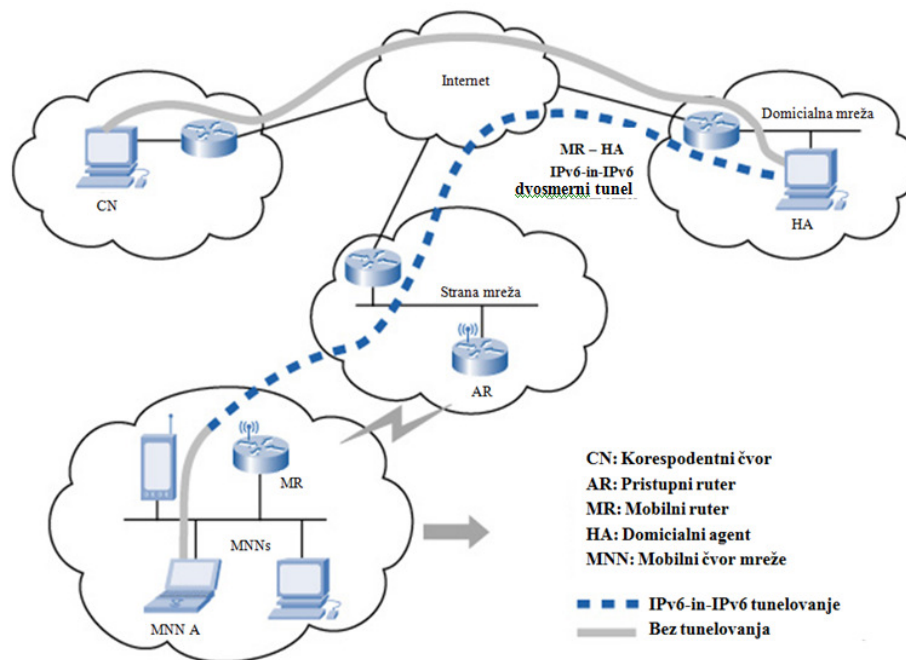
Sledeće, mobilni čvor verifikuje da li se spoljna IP adresa poklapa sa adresom njegovog domicilnog agenta. Takođe, domicilni agent vrši proveru da li spoljna adresa mobilnog čvora odgovara adresi koju je on prijavio prilikom poslednjeg vezivanja, odnosno slanja poruke ažuriranja vezivanja. Domicilni agent vrši i proveru mobilnog čvora preko domicilne adrese (HoAddr) njegovog unutrašnjeg izvorišnog paketa. [1]

2.11 IPv6 NEMO i mobilnost mreže

Mobilni čvorovi mogu biti različiti informacioni komunikacioni uređaji, kao što su laptopovi, mobilni telefoni, konzole, tableti i slično. Međutim, karakteristika mobilnosti, pored standardnih host uređaja, može se pridružiti i ruterima. Na ovaj način, obezbeđujući mobilnost jednom, ili više rutera, obezbeđujemo i mobilnost njima pridruženih mreža.

Operacije mobilnog rutera definiše NEMO (eng. *NEtwork MObility*) protokol. Osnovni NEMO protokol podrške omogućava Mobilnim IPv6 mrežama priključivanje na različitim tačkama na Internetu. NEMO protokol je produžetak Mobilnog IPv6, čija

uloga je da omogućava kontinuitet sesije za svaki čvor u mobilnoj mreži kada mobilna mreža menja svoje mesto priključenja – vezivanja. NEMO omogućava dostupnost svakog čvora u mobilnoj mreži. Mobilni ruter koji povezuje mobilnu mrežu sa Internetom, pokreće NEMO osnovni protokol podrške sa njegovim domicilnim agentom i na taj način omogućava mobilnost čitave mreže tako da servis mobilnosti bude dostupan za čvorove unutar mobilne mreže. [14]



Slika 17: NEMO operacije

Na Slici 16 prikazane su operacije u toku komunikacije koja se izvršava kada korespondentni čvor (CN), razmenjuje IP datagrame sa čvorom mobilne mreže (eng. *Mobile Network Node - MNN*). Navedena komunikacija se odvija na sledeći način:

- Korespondentni čvor šalje IP datagram namenjen za čvor mobilne mreže označen sa A (MNN A). Ovaj datagrama nosi kao adresu svog odredišta za IPv6 paket adresu MNN A čvora.
- Datagram koji šalje korespondentni čvor usmerava se ka NEMO domicialnoj mreži (HN), gde biva enkapsuliran unutar novog IP datagrama od strane domicialnog agenta (HA). Zatim se novi datagram šalje ka CoA adresi mobilnog rutera, sa adresom domicilnog agenta kao izvorišnom adresom. Ova enkapsulacija zadržava transparentnost mobilnosti, uz zadržavanje utvrđenih Internet veze na mobilnim čvorom mreže.
- Mobilni ruter prima enkapsulirani IP datagram, otklanja spoljno IPv6 zaglavlje, i donosi originalni datagram do mobilnog čvora mreže MNN A.

- Potpuno je analogna operacija u suprotnom smeru. Kada mobilni čvor šalje datagram, on biva enkapsuliran od strane mobilnog rutera, sa odredišnom adresom domicialnog agenta. Po pristizanju do svog prvog odredišta, odnosno domicialnog agenta, datagram biva deenkapsuliran sklanjanjem spoljnog IPv6 zaglavlja, a zatim se kroz dvosmerni tunel, šalje ka korespodentnom čvoru. Kao što je već navedeno ranije, svrha ove enkapsulacije je izbegavanje problema ulaznog filtriranja, jer mnogi ruteri i firewall-ovi sprovode, ranije pomenute, bezbednosne politike koji ne dozvoljavaju prosleđivanje paketa koji imaju izvornu adresu koja se pojavljuje topološki nekorektna.

2.12 Praktična upotreba MIPv6 protokola

Primeri praktične upotrebe Mobilnog IP protokola za verziju 6 su mnogobrojni. Skoro da postoji svakodnevna potreba da pojedinačni kominikacioni uređaji zadržavaju svoje mrežne identifikatore bez obzira sa koje lokacije uspostavljaju komunikaciju i na taj način omoguće neprekidno izvršavanje aplikacija na višim nivoima OSI referentnog nivoa.

Kroz IPv6 unapređuje se takozvana *plug-and-play* opciju za kojom ima potrebu sve veći broj mobilnih uređaja koji dobijaju IP podršku. Takođe primetna je i povećana potreba za kretanjem mobilnih mreža.

Oblasti u kojima se koristi mobilnost zasnovana na IPv6 protoklu su raznovrsne. Medicinske službe, vojska, policijske službe, kao i službe za specijalne operacije u vanrednim uslovima, su možda najekstremnije i najvažnije oblasti ljudskog delovanja gde IPv6 mobilnost može izraziti svoju neophodnost upotrebe.

Poslovni korisnici, koji imaju potrebu sa čestim putovanjima, imaju i potrebu za stalno dostupnim Internetom. Međutim, često ni to nije dovoljno, jer ovakvi korisnici imaju potrebu za stalnim uvođenjem novih prsta aplikacije, odnosno takozvanih „*push*“ servisa, kao što su različiti rezultati istraživanja ili berzanski izveštaji, i takozvanih „*peer-to-peer*“ servisa, kao što je razmena različitih multimedijalnih sadržaja. Da bi se ovo omogućilo korisniku, neophodno je da se on uvek priključuje na mrežu sa istim mrežnim identifikatorom, bez obzira odakle se povezuje.

IP mobilnost, kao napredni servis IPv6 protokola, je osmišljen da ispuni navedene zahteve. U sledećem delu rada biće prikazane imlementacije pojedinačnih elemenata IPv6 mobilnosti i izazovi njegove praktične upotrebe.

3. Implementacija MIPv6

Komande koje će dalje biti prikazivane, odnose se na CISCO IOS Software, a sama konfiguracija elemenat Mobilnog IPv6 u CISCO opremi je dostupna od 2001. godine, odnosno od verzija izdanja 12.3 i 12.4. [1]

3.1 Omogućavanje IPv6 Mobilnosti na ruteru

Da bi se omogućilo izvršavanje IPv6 mobilnosti na ruteru, potrebno je uraditi osam koraka sa opisanom svrhom:

1. Omogućiti privilegovani "EXEC" režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Odabrati tip i broj interfejsa na kome se želi omogućiti izvršavanja mobilnosti i ući u mod njegove konfiguracije.
Format komande: **interface type number**
4. Inicirati i pokrenuti mobilni IPv6, odnosno aktivirati funkciju domicialnog agenta na odabranom interfejsu .
Format komande: **ipv6 mobile home-agent** [*preference preference-value*]
5. Izaći iz moda konfiguracije interfejsa i vratiti se u globalni mod konfiguracije.
Format komande: **exit**
6. Izaći iz globalniog režim konfiguracije i vratiti se u privilegovani "EXEC" režim.
Format komande: **exit**
7. Prikazati globalne parametre IPv6 mobilnosti.
Format komande: **show ipv6 mobile globals**
8. Prikazati lokalne i otkriti susedne domicilne agente.
Format komande: **show ipv6 mobile home-agent** *interface-type interface-number* [*prefix*]

Komanda 1: Opšti primer koda koji omogućava IPv6 Mobilnost na ruteru

```
RouterHA> enable
RouterHA# configure terminal
RouterHA(config)# interface Ethernet 2
RouterHA(config-if)# ipv6 mobile home-agent
RouterHA(config-if)# exit
RouterHA(config)# exit
RouterHA# show ipv6 mobile globals
RouterHA# show ipv6 mobile home-agent
```

3.2 Podešavanje informacija vezivanja

Pre nego što se startuje IPv6 Mobilnost na određenom interfejsu, mogu se podesiti informacije vezivanja (eng. *Binding Information*) na ruteru, i to kroz osam koraka sa opisanom svrhom:

1. Omogućiti privilegovani “EXEC” režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Staviti ruter u mod konfiguracije domicilnog agenta.
Format komande: **ipv6 mobile home-agent**
4. Konfigurisati opcije vezivanja za funkciju domicilnog agenta.
Format komande: **binding access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*
5. Izaći iz moda konfiguracije domicilnog agenta i vratiti se u globalni mod konfiguracije.
Format komande: **exit**
6. Izaći iz globalnog moda konfiguracije i vratiti se u privilegovani “EXEC” režim.
Format komande: **exit**
7. Prikazati informacije kaša vezivanja.
Format komande: **show ipv6 mobile binding** **show ipv6 mobile binding** [**care-of-address** *address* | **home-address** *address* | *interface-type interface-number*]
8. Prikazati informacije o primljenim i poslatim zahtevima za vezivanjem.
Format komande: **show ipv6 mobile traffic**

Komanda 2: Opšti primer koda za podešavanje informacija vezivanja

```
RouterHA> enable
RouterHA# configure terminal
RouterHA(config)# ipv6 mobile home-agent
RouterHA(config-ha)# binding
RouterHA(config-ha)# exit
RouterHA(config)# exit
RouterHA# show ipv6 mobile binding
RouterHA# show ipv6 mobile traffic
```

3.3 Omogućavanje i konfigurisanje NEMO na IPv6 mobilnom ruteru

Osnovna NEMO podrška omogućava da čvorovi mobilne žene mogu da se prijavljuju na različite tačke Interneta, zadržavajući karakteristike IPv6 mobilnosti. Da bi se stvorili uslovi za to potrebno je da se izvrši omogućavanje i konfiguracija NEMO podrške na mobilnom ruteru za koji je nosilac mobilne pod mreže. Omogućavanje i konfigurisanje NEMO na IPv6 mobilnom ruteru izvršava se kroz sledećij jedanajest koraka sa opisanom svrhom:

1. Omogućiti privilegovani “EXEC” režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Omogućiti IPv6 NEMO funkcionalnost na ruter, i staviti ruter u IPv6 Mobile konfiguracioni mod.
Format komande: **ipv6 mobile router**
4. Koristiti MAC adresu određenog interfejsa za izvođenje domicilne IPv6 mobilne adrese.
Format komande: **eui-interface** *interface-type interface-number*
5. Navodi se prefiks domicilne mreže na mobilnom ruter. Korisnici imaju mogućnost konfigurirati unose do deset domicilnih mreža, i oni se koriste u redosledu unosa, koji je izvršen po prioritetu. Prefiks identifikuje domicilnu mrežu mobilnog rutera i koristi se za otkrivanje kada je mobilni ruter prikačen na domicilnu adresu.
Format komande: **home-network** *ipv6-prefix*
6. Navodi se domicilna adresa mobilnog rutera korišćenjem IPv6 adrese ili identifikatora interfejsa. Kada se konfigurira više domicilnih adresa, preporučuju se da se koristi komandna sintaksa **home-address home-network**, tako da mobilni ruter pravi par domicilne adrese i domicilne mreže, koji odgovaraju jedna drugoj.
Format komande: **home-address** {**home-network** | **ipv6-addressidentifier** | **interface**}
7. Registracija IPv6 prefiksa povezanog sa mobilnim ruterom.
Format komande: **explicit-prefix**
8. Kontrolisati parametre za registraciju mobilnog rutera.
Format komande: **register** {**extend** **expire seconds** **retry number interval seconds** | **ifetime seconds** | **retransmit initial milliseconds maximum milliseconds retry number**}
9. Izaći iz moda konfiguracije mobilnog rutera i vratiti se u globalni mod konfiguracije.
Format komande: **exit**
10. Izaći iz globalnog moda konfiguracije i vratiti se u privilegovani “EXEC” režim.
Format komande: **exit**
11. Prikazati informacije o konfiguraciji i statističkim podacima o IPv6 mobilnom ruteru.
Format komande: **show ipv6 mobile router running-config** | **status**]

Komanda 3: Opšti primer koda za omogućavanje i konfigurisanje NEMO na IPv6 mobilnom ruteru

```
RouterMR> enable
RouterMR# configure terminal
RouterMR(config)# ipv6 mobile router
RouterMR(IPv6-mobile-router)# eui-interface Ethernet0/0
RouterMR(IPv6-mobile-router)# home-network 2001:0DB1:1/64
RouterMR(IPv6-mobile-router)#   home-address   home-network
eui-64
RouterMR(IPv6-mobile-router)# explicit-prefix
RouterMR(IPv6-mobile-router)# register lifetime 600
```

```
RouterMR(IPv6-mobile-router)# exit
RouterMR(config)# exit
RouterMR # show ipv6 mobile router
```

3.4 Omogućavanje NEMO domicilnog agenta na mobilnom ruteru

1. Omogućiti privilegovani "EXEC" režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Omogućiti proces rutiranja NEMO na domicilni agenta i postavite ruter u ruter mod konfiguracije.
Format komande: **ipv6 router nemo**
4. Definirati administrativne distance za NEMO rute.
Format komande: **distance [mobile-distance]**

Komanda 4: Opšti primer koda za omogućavanje NEMO domicilnog agenta na IPv6 mobilnom ruteru

```
RouterMR> enable
RouterMR# configure terminal
RouterMR(config)# ipv6 router nemo
RouterMR(config-rtr)# distance 10
```

3.5 Omogućavanje rominga ("lutanja") na interfejsu mobilnog ruteru

1. Omogućiti privilegovani "EXEC" režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Odabrati tip i broj interfejsa koji se želi konfigurisati i ući u njegov mod konfiguracije.
Format komande: **interface type number**
4. Omogućiti "lutanje" na interfejsu mobilnog rutera.
Format komande: **ipv6 mobile router-service roam [bandwidth-efficient | costefficient | priority value]**

Komanda 5: Opšti primer koda za omogućavanje rominga ("lutanja") na interfejsu mobilnog ruteru

```
RouterMR> enable
RouterMR# configure terminal
RouterMR(config)# interface ethernet 0/0
RouterMR(config-if)# ipv6 mobile router-service roam
```

3.6 Filtriranje zaglavlja proširenja Mobilnog IPv6 protokola

Kao deo IPv6 komponente pristupnih listi (eng. Access List), na CISCO ruterima je uvedena karakteristika koja omogućava ruteru da poredi pakete koji sadrže IPv6 zaglavlja proširenja. Cilj je obezbediti detaljniju kontrolu zaglavlja rutiranja i ICMPv6

poruka. Ovo je potrebno kako bi se domilni agent omogućio da bez bezbednosnih propusta vrši MIPv6 operacije.

1. Omogućiti privilegovani "EXEC" režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Definirati IPv6 pristupnu listu i staviti ruter u mod konfiguracije pristupnih listi.
Format komande: **ipv6 access-list** *access-list-name*

4. Navesti uslove dozvole ili zabrane za određena opciona zaglavlja Mobilnog IPv6 u IPv6 pristupnoj listi.

Format *permit* komande: **permit icmp** {*source-ipv6-prefix / prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* *portnumber*] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*portnumber*]] [*icmp-type* [*icmp-code*] | *icmp-message*][**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**][**mobility**] [**mobility-type** [*mh-number* | *mh-type*]][**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Format *deny* komande: **deny icmp** {*source-ipv6-prefix / prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* *portnumber*] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmpmessage*][**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flowlabel** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mhtype*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Komanda 6: Opšti primer koda za postavljanje liste dozvole

```
RouterHA> enable
RouterHA# configure terminal
RouterHA(config)# ipv6 access-list list1
RouterHA(config-ipv6-acl)#permit icmp host 2001:DB8:0:6::37
any routing-type 2
```

Komanda 7: Opšti primer koda za postavljanje liste zabrane

```
RouterHA> enable
RouterHA# configure terminal
RouterHA(config)# ipv6 access-list list1
RouterHA(config-ipv6-acl)#deny icmp host 2001:DB8:0:6::37
any routing-type 2
```

3.7 Kontrolisanje ICMP poruka za nedostupno odredište

U pogledu gubljenja paketa prilikom transporta ka adredištu, IPv6 protokol je podjednako nepouzdan kao i IPv4. Ovo je najčešće privremeni problem zbog trenutnog prekida veze ili zagušenja saobraćaja. Tada je potrebno ugraditi mehanizam povratne sprege, kako bi postojala povratna informacija o nedostupnosti odredišta. ICMP poruka

za nedostupno odredište obezbeđuje kod greške na osnovu kog se može odrediti zbog čega je nastao problem i mogu preduzeti odgovarajuće mere. Zato je potrebno omogućiti kontrolu poruka nedostupnog odredišta za svaki paket isporučen na određeno odredište:

1. Omogućiti privilegovani “EXEC” režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Odabrati tip i broj interfejsa koji se želi konfigurisati i ući u njegov mod konfiguracije.
Format komande: **interface type number**
4. Omogućiti kontrolu ICMP poruka nedostupnog odredišta za svaki paket isporučen na određeno odredište.
Format komande: **ipv6 unreachable**

Komanda 8: Opšti primer koda za postavljanje liste zabrane

```
RouterMR> enable
RouterMR# configure terminal
RouterMR(config)# interface ethernet 0/0
RouterMR(config-if)# ipv6 unreachable
```

3.8 Verifikacija prirodnog (native) IPv6 tunelovanja za Mobilni IPv6

1. Omogućiti privilegovani “EXEC” režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Izlistati tunele mobilnog IPv6 na domicilnom agentu.
Format komande: **show ipv6 mobile tunnels [summary | tunnel if-number]**

Komanda 9: Opšti primer koda za verifikaciju tunelovanja

```
RouterHA> enable
RouterHA# configure terminal
RouterHA(config)# show ipv6 mobile tunnels
```

3.9 Konfiguracija i verifikacija grupe hostova mobilnih čvorova na domicilnom agentu

Korisnici mogu da kreiraju mobilne korisnike ili grupe polisa, koristeći mogućnost konfiguracije grupe hostova. Profil grupe hostova traži interfejs koji će dozvoliti potraživanja od profila povezanog sa pošiljaocem ažuriranja vezivanja (BU) koristeći ime profila pošiljaoca, IPv6 adresu ili NAI (eng. *Network Access Identifier*). Takođe, profil grupe hostova traži interfejs i navodeći svojstva autentifikacije za IPv6 mobilni čvor stvaranjem ili jednosmernog ili dvosmernog SPI (eng. *Security Policy Index*).

Mobilni čvor može da se identifikuje koristeći svoje ime profila ili domicilnu adresu, koju poruka Mobilnog IPv6 protokola koristi kao identifikator u svojim porukama registracije. Međutim, za neke raspoređivanja neophodno je da mobilni čvor ima

sposobnost da se identifikuje pomoću logičnog identifikatora, kao što je NAI pre nego sa mrežnom adresom [1].

1. Omogućiti privilegovani “EXEC” režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Staviti ruter u mod konfiguracije domicialnog agenta.
Format komande: **ipv6 mobile home-agent**
4. Konfigurisati opcije vezivanja domicilnog agenta za funkcije mobilnog IPv6.
Format komande: **binding [access access-list-name | auth-option | seconds| maximum | refresh**
5. Kreirati konfiguraciju domaćina u mobilnim IPv6. Više različitih instanci profila sa različitim imenima se može kreirati.
Format komande: **host group profile-name**
6. Navesti domicilnu adresu IPv6 mobilnog čvora.
Format komande: **address {ipv6-address | autoconfig**
7. Navesti NAI (eng. *Network Access Identifier*) IPv6 mobilnog čvora.
Format komande: **nai realm | user | macaddress] {user @ realm| @ realm**
8. Navesti svojstva autentifikacione za IPv6 mobilni čvor kreiranjem ili jednosmernog ili dvosmernog SPI (eng. *Security Policy Index*).
Format komande: **authentication inbound-spi {hex-in | decimal decimal-in} outbound-spi {hex-ou t| decimal decimal-out} | spi {hex-value | decimal decimal-value}} key {ascii string | hex string}[algorithm algorithm-type] [replay within seconds**
9. Izaći iz moda konfiguracije domicialnog agenta i vratiti se u globalni mod konfiguracije.
Format komande: **exit**
10. Izaći iz globalniog moda konfiguracije i vratiti se u privilegovani “EXEC” režim.
Format komande: **exit**
11. Prikazati informacije o Mobilni IPv6 host grupama .
Format komande: **show ipv6 mobile host groups profile-name]**

Komanda 10: Opšti primer koda za konfiguraciju i verifikaciju grupe hostova

```
RouterHA> enable
RouterHA# configure terminal
RouterHA(config)# ipv6 mobile home-agent
RouterHA(config-ha)# binding 15
RouterHA(config-ha)# host group profile1
RouterHA(config-ha)# address baba 2001:DB8:1
RouterHA(config-ha)# nai @cisco.com
RouterHA(config-ha)# authentication spi 500 key ascii cisco
RouterHA(config-ha)# exit
RouterHA(config)# exit
```

```
RouterHA# show ipv6 mobile host groups
```

3.10 Modifikacija Mobilnog IPv6 na interfejsu

Podešavanje parametara konfiguracije interfejsa može da se izvrši pre nego što se startuje Mobilni IPv6 ili dok je Mobilni IPv6 u funkciji.

1. Omogućiti privilegovani “EXEC” režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
3. Odabrati tip i broj interfejsa koji se želi konfigurisati i ući u njegov mod konfiguracije.
Format komande: **interface type number**
4. Konfigurisati prioritetnu vrednost na interfejsu mobilnog IPv6 domicilnog agenta.
Format komande: **ipv6 mobile home-agent [preference preference-value**
5. Ući u globalni mod konfiguracije.
Format komande: **configure terminal**
6. Konfigurisati opciju intervala oglašavanja.
Format komande: **ipv6 nd advertisement-interval**
7. Konfigurisati interval između prenosa oglašavanja rutera – RA (eng. *Router Advertisement*) na interfejs.
Format komande: **ipv6 nd ra interval {maximum-secs [minimum-secs] | msec maximummsecs [minimum-msecs]}**

Komanda 11: Opšti primer koda za modifikaciju Mobilnog IPv6 na interfejsu

```
Router> enable
Router# configure terminal
Router(config)# interface serial 3
Router(config-if)# ipv6 mobile home-agent preference 10
Router(config-if)# ipv6 nd advertisement-interval
Router(config-if)# ipv6 nd prefix 2001:DB8::/35 1000 900
Router(config-if)# ipv6 nd ra interval 201
```

3.11 Praćenje i održavanje Mobilog IPv6 na ruteru

1. Omogućiti privilegovani “EXEC” režim (Uneti lozinku ako bude zatražena).
Format komande: **enable**
2. Brisati Mobilni IPv6 keš vezivanja na ruteru.
Format komande: **clear ipv6 mobile binding [care-of-address prefix | home-address prefix | interface type interface-number**
3. Brisati listu suseda domicilnog agenta.
Format komande: **clear ipv6 mobile home-agents [interface-type interface-number**
4. Brisati brojače veza Mobilog IPv6.

Format komande: **clear ipv6 mobile traffic**

5. Omogućavanje prikaza informacija otklanjanja grešaka za Mobilni IPv6.

Format komande: **debug ipv6 mobile binding-cache | forwarding | home-agent | registration**

6. Prikaza poruka otklanjanih grešaka za IPv6 mobilne mreže.

Format komande: **debug ipv6 mobile networks**

7. Prikaza poruka otklanjanih grešaka za IPv6 mobilni ruter.

Format komande: **debug ipv6 mobile router [detail]**

Komanda 12: Opšti primer koda za praćenje i održavanje Mobilnog IPv6 na ruteru

```
Router> enable
```

```
Router# clear ipv6 mobile binding
```

```
Router# clear ipv6 mobile home-agents
```

```
Router# clear ipv6 mobile traffic
```

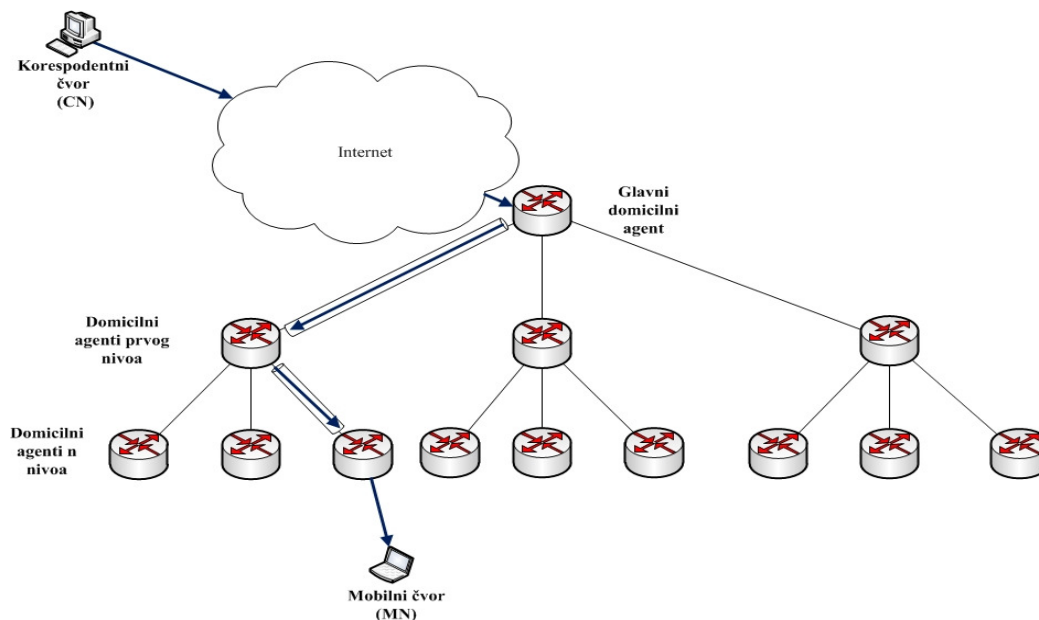
```
Router# debug ipv6 mobile registration
```

```
Router# debug ipv6 mobile networks
```

```
Router# debug ipv6 mobile router
```

3.12 Mobilna domicilna mreže

Mobilna mreža može da ima dvojaku funkciju, sa jedne strane može biti mobilna mreža, ali istovremeno može imati ulogu domicilne mreže. U tom slučaju pojedini ruteri mobilne mreže uzimaju ulogu domicilnog agenta. Na ovaj način rutri iz različitih mreža formiraju neku vrstu hijerarhijskog stabla.



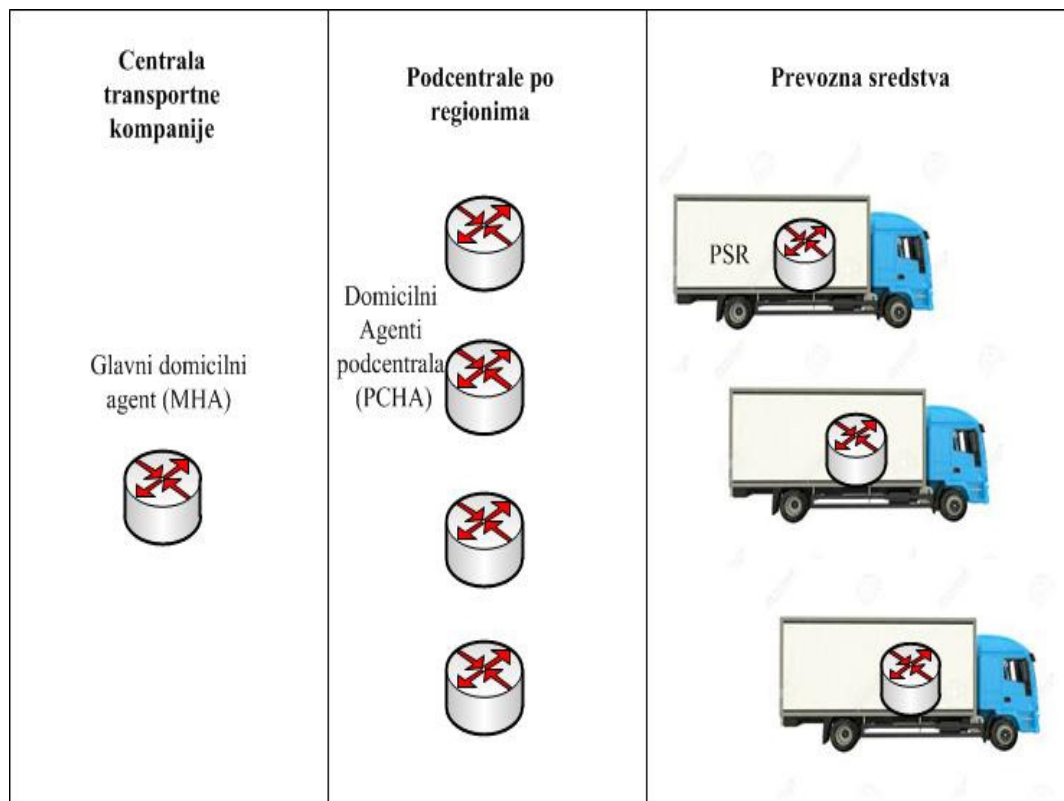
Slika 18: Kretanja paketa od korespondentnog čvora do mobilnog čvora mobilne domicilne mreže

Proces je kretanja paketa od korespodentnog čvora do mobilnog čvora mobilne domicilne mreže je prikazan na Slici 18, i on se odvija po sledećem:

- glavni ruter obaveštava ostale o domicilnoj strukturi,
- paketi koji dolaze van ove infrastrukture dolaze do glavnog rutera,
- glavni ruter ih tuneluje ka ruteru odgovornom za sledeći nivo stabla,
- zatim ih i ovaj ruter dekapulira i enkapsulira pakete, kako bih tunelovao do sledećeg odgovornog rutera,
- navedeni proces se ponavlja sve dok paketi ne budu isporučeni do konačnog odredišta.

13.12.1 Konfiguracija mobilne domicilna mreže

Kao primer mobilne domicilne mreže može se uzeti velika transportna internacionalna kompanija sa centralom u Beogradu. U centarali transportne kompanije nalazi se glavni domicilni ruter (agent), dok se domicilni agenti sledećeg nivoa nalaze po podcentralama smeštenim po regionima Srbije. Svakom transportnom sredstvu je pridružen po jedan mobilni ruter (domicilni agent poslednjeg nivoa). U prevoznom sredstvu se nalazi i personalna mobilna kominakciona oprema. Navedena hijerarhijska topologija je prikazana na Slici 19.



Slika 19: Mobilna domicilna mreža transportne kompanije

Komanda 13: Konfiguracija glavnog domicilnog agenta u centrali transportne kompanije

```
RouterMHA# show running
interface Ethernet0
  ip address 10.0.5.1 255.255.255.0
  ipv6 enable
  ipv6 nd ra suppress
  ipv6 Mobile Router-service door
interface Ethernet1
  ip address CAB:C0:CA5A:CA5A::CA5A::/64
  ipv6 enable
  ipv6 nd advertisement-interval
  ipv6 nd ra interval msec 1000
  ipv6 mobile home-agent run
```

Komanda 14: Konfiguracija domicilnog agenta u podcentrali kompanije

```
RouterPCHA# show running
ip Mobile Router
  home-network CAB:C0:CA5A:CA5A::/64 discover
  home-address home-network ::5F0
  home-door 10.0.5.1
  explicit-prefix
interface Ethernet0
  ip address dhcp
  ipv6 address autoconfig
  ipv6 enable
  ipv6 nd ra suppress
  ipv6 Mobile Router-service roam try-the-door
interface Ethernet1
  ip address CAB:C0:5F0:5F0::5F0/64
  ipv6 enable
  ipv6 nd advertisement-interval
  ipv6 nd ra interval msec 1000
  ipv6 mobile home-agent run
```

Komanda 15: Konfiguracija rutera u jednom prevoznom sredstvu

```
RouterPSR# show running
ip Mobile Router
  home-door 10.0.5.1
  home-network CAB:C0:5F0:5F0::/64 discover
  home-address home-network ::CAB1
  explicit-prefix
!
interface Ethernet0
  ip address dhcp
  ipv6 address autoconfig
```

```
ipv6 enable
ipv6 nd ra suppress
ipv6 Mobile Router-service roam try-the-door
!
interface Ethernet1
 ip address 10.0.4.1 255.255.255.0
 ip address CAB:C0:5F0:CAB1::CAB1/64 ,
 ipv6 enable
 ipv6 nd advertisement-interval
 ipv6 nd ra interval msec 1000
```

Zaključak

Kada IPv4 je dizajniran, kao prva verzija Internet protokola koji se globalno koristio, procenjeno je da će se koristiti duže vreme. Međutim, eksponencionalni rast broja uređaja koji se povezuju na mrežu je suočio IPv4 sa nekoliko problema. Nedostatak adresa je jedan od važnih problema IP-a. Ljudi koriste sve više uređaja kao što su laptopovi, PDA i telefona i na taj način zahtevaju IP adrese koje su postale kritični resurs.

Odgovor na IPv4 je sledeća generacija ovog protokola, odnosno IPv6, čiji je zadatak da eliminiše ograničenja IPv4. IPv6 pruža veći adresni prostor, dužina adrese u IPv4 je 32 bita, a u IPv6 je povećana na 128 bita. Bezbednost je drugo bitno poboljšanje IPv6, jer IPsec u IPv4 nije obavezno, a sva odgovornost za bezbednost pripada krajnjim čvorovima. U IPv4, konfiguracija IP se vrši ručno ili korišćenjem dodatnih protokola kao što je DHCP. Kod IPv6 postoji mehanizam automatske konfiguraciju IP adrese. Mobilnost je još jedan nedostatak IPv4, a IPv6 poboljšava pokretljivost mobilnog čvora koji menja lokaciju.

Ipak, IPv6 protokol je dokaz da ne postoji savršena tehnologija. Postoji samo stalni razvoj tehnologije kroz se rešavanje problema i novi postavljani izazovi. IPv6 je sa sobom doneo mnoga poboljšanja koja su navedena, međutim postoje i mnogi problemi i nedostaci.

Isti slučaj je i sa IPv6 mobilnošću sa čijom primenom su rešeni problemi optimizacije rute i trougaonog rutiranja, ali procesi detekcije duplikata adresa i otkrivanje suseda su doneli dodatna kašnjenja kada su u pitanju aplikacije koje se izvršavaju u realnom vremenu.

Kada se pravi poređenje MIPv4 i MIPv6 može se reći da je osnovni nedostatak MIPv4 opcionalna mogućnost optimizacije rute. Naime, u IPv4 Mobilnosti funkcija optimizacije rutiranja je opcionalna komponenta koja ne mora biti podržana od strane svih IPv4 stanica. Za razliku od IPv4 Mobilnosti, IPv6 Mobilnost ima integrisanu funkciju optimizacije rute, što znači da je proces rutiranja brži i dozvoljava da paketi budu dostavljani direktno, bez posredništva domicilne mreže.

Najveće slabosti MIPv4 i MIPv6 pokazuju u trenutku kada mobilni čvor menja podmrežu vezivanja. Naime, tokom periodu kada mobilni čvor kreće kroz mreže, pre nego što zahteva CoA adresu, novi strani agent ne može da obavesti starog agenta o kretanju mobilnog čvora. Paketi poslani ka prethodnoj CoA adresi u toku navedenog perioda bivaju izgubljeni. Zato neke aplikacije, koje se izvršavaju u realnom vremenu imaju potrebe za dodatnim funkcionalnostima koje se bave vremenski kritičnim aspektima određenih servisa i aspekata. Ovde se pre svega podrazumevaju brže detektovanje i prepuštanje mobilnog čvora novom stranom agentu.

Dalji razvoj i unapređenje IPv6 posmatra se kroz potrebe koje on treba da ispunji. Očekivano je da sve više govorne komunikacije u budućnosti bude obavljano preko Voice over IP i preko IPv6 mobilnosti, kao osnovne tehnologije u slučajevima kada mobilni komunikacioni uređaj menja lokaciju i tačku vezivanja na Internetu. Problemi koji se javljaju u razmatranju daljeg pravca razvoja su već pomenuto detektovanje

kretanja i uspostavljanja nove konekcije. Odgovor na ovaj problem je sposobnost mobilnog čvora da uspostavi novu konekciju pre prekida stare konekcije (*make-before-break*). Jedan od tih sposobnosti je takozvana „brza IP mobilnost“ (eng. *Fast Mobility IP*) – MIP.

IPv6 protokol predstavlja važan napredak u svetu Interneta, ali još uvek ne predstavlja zrelu tehnologiju i zaočekivati je da kako preuzima primat u odnosu na IPv4, tako se javljaju i problemi, ali i iskustvo u rešavanju tih problema. Svakako će biti zanimljiv dalji razvoj zavremenih mrežnih tehnologija. Pretpostavke i vizija, je da će sa povećavanjem broja uređaja povezanih na Internet, doći do sveopšte povezanosti i do takvog rasta i promene načina funkcionisanja Interneta, da možda neće ličiti na ono kako ga znamo danas. Razvoj IPv6 i MIPv6 će svakao odigrati ključnu ulogu u daljem razvoju Interneta.

Literatura

- [1] Ciprian Popoviciu, Eric Levy-Abegnoli i Patrick Grossetete, "Deploying IPv6 Networks", Cisco Press, 2006.
- [2] Mladen Veinović, Aleksandar Jevremović, „Uvod u računarske mreže“, Univerzitet Singidunum Fakultet za poslovnu informatiku, 2007.
- [3] Network Working Group: S. Deering – Cisco, R. Hinden – Nokia, „Internet Protocol, Version 6 (IPv6) Specification“, Request for Comments: 2460, 1998.
- [4] Network Working Group: R. Hinden – Nokia, S. Deering – Cisco Systems, „IP Version 6 Addressing Architecture“, Request for Comments: 4291, 2006.
- [5] Benedikt Stockebrand, „IPv6 in Practice , A Unixer's Guide to the Next Generation Internet“, Springer, 2007.
- [6] Network Working Group: R. Hinden – Nokia, S. Deering – Cisco, E. Nordmark – Sun, „IPv6 Global Unicast Address Format“, Request for Comments: 3587, 2003.
- [7] Network Working Group: R. Hinden – Nokia, B. Haberman – JHU-APL, „Unique Local IPv6 Unicast Addresses“, Request for Comments: 4193, 2005.
- [8] Network Working Group: B. Haberman – Consultant, D. Thaler – Microsoft, „Unicast-Prefix-based IPv6 Multicast Addresses“, Request for Comments: 3306, 2002.
- [9] Network Working Group: R. Hinden – Nokia, S. Deering – Cisco Systems, „Internet Protocol Version 6 (IPv6) Addressing Architecture“, Request for Comments: 3513, 2003.
- [10] James D. Solomon, „Mobile IP, The Internet Unplugged“, Prentice Hall, 1998.
- [11] Network Working Group: D. Johnson – Rice University, C. Perkins – Nokia Research Center, J. Arkko – Ericsson, „Mobility Support in IPv6“, Request for Comments: 3775, 2004.
- [12] Network Working Group: A. Conta – Transwitch, S. Deering – Cisco Systems, M. Gupta – Tropos Networks, „Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification“, Request for Comments: 4443, 2006.
- [13] Network Working Group: D. Johnson – Carnegie Mellon University, S. Deering – Cisco Systems, Inc., „Reserved IPv6 Subnet Anycast Addresses“, Request for Comments: 2526, 1999.
- [14] Network Working Group: V. Devarapalli – Nokia, R. Wakikawa – Keio University, A. Petrescu – Motorola, P. Thubert – Cisco Systems, „Network Mobility (NEMO) Basic Support Protocol“, Request for Comments: 3963, 2005.