

Upravljanje mobilnošću u All-IP mrežama

Anić, Augustin

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:119:312251>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2025-01-28**



Repository / Repozitorij:

[Faculty of Transport and Traffic Sciences -
Institutional Repository](#)



SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Upravljanje mobilnošću u All-IP mrežama

Diplomski rad

Mentor: izv. prof. dr. sc. Štefica Mrvelj

Student: Augustin Anić

Zagreb, rujan 2016.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Upravljanje mobilnošću u All-IP mrežama
Mobility management in All-IP networks

Mentor: izv. prof. dr. sc. Štefica Mrvelj

Student: Augustin Anić

Zagreb, rujan 2016.

ZAHVALA

Zahvaljujem se svojoj mentorici izv. prof. dr. sc. Štefici Mrvelj za veliki trud i strpljenje prilikom izrade moga diplomskog rada. Svojim stručnim sugestijama i komentarima uvelike je doprinijela kvaliteti i konačnoj formi rada.

Zahvaljujem se svim ljudima koji me okružuju, posebno roditeljima koji su me tokom cijeloga obrazovanja bezrezervno podupirali i savjetovali, pokojnoj baki i djedu koji su uvijek bili uz mene tokom mojeg odrastanja i sazrijevanja, rodbini koja me u svim važnim trenucima života bodrila kako bi ostvario sve zacrtane ciljeve, prijateljima koji su me podržavali i veselili se svakom ostvarenom rezultatu.

Veliko hvala profesorima i asistentima Fakulteta prometnih znanosti na zalaganju i prenošenju znanja koje će mi biti daljnji poticaj za učenje i usavršavanje.

Augustin Anić

Sažetak i ključne riječi

Mobilnost korisnika u današnjem telekomunikacijskom okruženju ključan je faktor zadovoljenja korisničkih potreba. Mobilnost podrazumijeva omogućavanje kontinuirane komunikacije korisnicima prilikom kretnje korištenjem bilo koje pristupne mreže i tehnologije. Pristupanje uslugama korištenjem bilo koje vrste pristupne mreže i tehnologije omogućeno je kroz All-IP mrežu. All-IP mreža predstavlja jezgrenu mrežu u potpunosti baziranu na Internetnom protokolu koja konvergira sve pristupne mreže u jedinstveno IP mrežno okruženje. Mobilnost korisnika unutar All-IP mrežnog okruženja postiže se primjenom protokola za upravljanje mobilnošću. IP protokola za podršku mobilnosti korisnika i *proxy* IP protokol za podršku mobilnosti korisnika omogućuju kvalitetan nadzor i upravljanje korisničkih komunikacija prilikom kretanja.

KLJUČNE RIJEČI: mobilnost korisnika, All-IP mreža, IP protokol za podršku mobilnosti korisnika, *proxy* IP protokol za podršku mobilnosti korisnika

Summary and keywords

The mobility of users in today's telecommunications environment is a key factor to satisfy user requirements. Mobility means enabling continuous communications to users during movements using any of access networks and technologies. Accessing the Services using any type of access network and technology is enabled through the All-IP network. All-IP network is a core network completely based on the Internet Protocol, which converges all access networks into a single IP network environment. User mobility within the All-IP network environment is achieved using the protocols for mobility management. IP protocol to support the mobility of users and proxy IP protocol to support the mobility of users provide quality supervision and management of user communication during movement.

KEYWORDS: user mobility, All-IP network, IP protocol to support the mobility of users, a proxy IP protocol support for user mobility

Sadržaj

1. Uvod	1
2. Razlozi za uvođenjem i pogodnosti implementacije All-IP koncepta	3
2.1. Razlozi migracije prema All-IP konceptu	4
2.2. Prednosti implementacije All-IP mreže	7
2.2.1. Usluga prijenosa govora Internet protokolom	8
2.2.2. IP televizija (IPTV)	11
2.2.3. Internet stvari (IoT)	14
3. Arhitektura i funkcioniranje All-IP mreže	20
3.1. Evoluirana paketska jezgrena mreža	22
3.1.1. Entitet upravljanja mobilnošću	24
3.1.2. Uslužni prilazni čvor	25
3.1.3. Paketski mrežni prilazni čvor	26
3.1.4. Čvor za upravljanje resursima i terećenjem	27
3.1.5. Poslužitelj domaćih pretplatnika	28
3.2. IP višemedijski podsustav	29
3.3. E-UTRAN pristupna mreža	32
4. Mobilnost u All-IP mrežama	34
4.1. Mobilnost i vrste prekapčanja	35
4.2. Vrste mobilnosti	37
4.2.1. Mobilnost sjednice	38
4.2.2. Mobilnost osobe	38
4.2.3. Mobilnost terminalnog uređaja	39
4. 3. Utjecaj mobilnosti na kvalitetu usluge	40

5. IP protokol za podršku mobilnosti korisnika	42
5.1. Funkcionalne komponente MIP protokola	43
5.2. Otkrivanje agenta	45
5.3. Registracija mobilnog čvora	47
5.4. Tuneliranje	49
6. Proxy IP protokol za podršku mobilnosti korisnika	51
6.1. Funkcionalne komponente PMIP protokola	52
6.2. Otkrivanje agenta	55
6.3. Ažuriranje tablice pod mreže	57
6.4. Registracija mobilnog uređaja	58
6.5. Tuneliranje	60
6. Zaključak	62
Literatura	64
Popis akronima	66
Popis slika	69
Popis dijagrama	70

1. Uvod

Ubrzani rast i razvoj telekomunikacijskog tržišta primorao je telekomunikacijski operatere na kreiranje i realizaciju kvalitetnijih usluga koje su korisnicima uvijek i svugdje dostupne uz odgovarajuću razinu kvalitete. Shodno tome telekomunikacijska mreža, kao najvažniji faktor pružanja spomenutih usluga, morala je doživjeti određeni redizajn kako bi bila u stanju odgovoriti na visoke zahtjeve korisnika u pogledu kvalitete i dostupnosti usluga.

Kao jednostavno i kvalitetno rješenje pojavila se All-IP mreža koja predstavlja jezgrenu mrežu koja je u potpunosti bazirana na IP (*eng. Internet protocol*) protokolu. Karakteriziraju ju jednostavnija arhitektura te efikasnije usmjeravanje i prosljeđivanje IP paketa u odnosu na prethodna rješenja uz minimalnu latenciju. All-IP mreža omogućuje migraciju svih vrsta mreža na IP baziranu okosnicu. Korisnike se time ne ograničava na korištenje određenih pristupnih mreža i tehnologija već uslugama mogu pristupiti putem bilo kojeg oblika mreže i bilo koje tehnologije.

Svrha istraživanja je identificirati prednosti i nedostatke MIP (*eng. Mobile IP Protocol*) i PMIP (*eng. Proxy Mobile IP Protocol*) protokola za upravljanje mobilnošću u All-IP mrežama te načiniti usporednu analizu značajki spomenutih protokola.

Cilj istraživanja je prikazati način funkcioniranja upravljanja mobilnosti u All-IP mrežama korištenjem MIP i PMIP protokola te pomoću odgovarajućih dijagrama opisati rad protokola.

Diplomski rad podijeljen je u sljedeće cjeline:

- uvod,
- razlozi za uvođenjem i pogodnosti implementacije All-IP koncepta,
- arhitektura i funkcioniranje All-IP mreže,
- mobilnost u All-IP mrežama,
- *mobile* IP protokol,
- *proxy mobile* IP protokol,
- zaključak.

U drugoj cjelini definirani su razlozi migracije prema All-IP mreži, kao i pogodnosti koje sa sobom donosi spomenuti koncept.

Trećim poglavljem rada opisana je arhitektura mreže i njezine temeljne funkcionalnosti. U četvrtome dijelu definirane su i opisane osnovne vrste mobilnosti korisnika, terminalnog uređaja i toka podataka.

Peti i šesti dio rada donose analizu protokola za upravljanje mobilnošću korisnika koji su temeljni dio ovoga rada. Petim poglavljem detaljno se opisuju procedure vezane uz MIP protokol kao i njegove osnovne komponente. U šestom dijelu analiziran je PMIP protokol. Navedene su i opisane njegove osnovne komponente te je detaljno razrađeno njegovo funkcioniranje kroz osnovne procedure.

2. Razlozi za uvođenjem i pogodnosti implementacije All-IP koncepta

Konkurentska pozicija kao i poslovno okruženje u kojem se nalaze telekom operatori te pružatelji usluga neprestano se mijenja. Svjedoci smo ubrzanog razvoja i pojavljivanja raznolikih poslovnih rješenja kao i usluga za privatne korisnike koje omogućuju nove komunikacijske tehnologije odnosno telekomunikacijski sustavi. Kako bi opstali u takvome tržišnom okruženju, telekom operatori primorani su nuditi usluge na efikasniji i fleksibilniji način kako bi ostvarili evoluciju prema višeslužnom mrežnom okruženju gdje će se nove usluge korisnicima nuditi uz povoljnije i kvalitetnije uvjete.

Upravo je ubrzani rast usluga zasnovanih na širokopojasnom pristupu u fiksnim i mobilnim mrežama jedan od glavnih pokretača za ostvarenje All-IP mrežnog okruženja. All-IP mreže omogućuju efikasno uvođenje atraktivnih multimedijских usluga uz ispunjavanje uvjeta kao što su visoka kvaliteta, sigurnost i međusobna kompatibilnost. Usluge bazirane na širokopojasnom pristupu, koji omogućuju velike brzine prijenosa uz minimalna kašnjenja, predstavljaju najbrže rastući segment u povijesti telekomunikacija.

Drugi najznačajniji pokretač migracije prema All-IP mrežnom okruženju je konvergencija koja omogućuje efikasno pružanje usluga krajnjim korisnicima neovisno o pristupnoj tehnologiji koju koriste. Konvergencija smanjuje operativne troškove telekom operatorima te predstavlja još jedan dodatan faktor za konvergiranje mreže i usluga. Višemedijski podsustav temeljen na internetskom protokolu (*eng. IP Multimedia Subsystem*) predstavlja konvergentno rješenje gdje je sav prijenos signalizacijskog prometa i prijenos korisničkih podataka omogućen putem IP tehnologija te sve pristupne mreže podržavaju IP protokol, [1].

2.1. Razlozi migracije prema All-IP konceptu

All-IP mreža svojom konfiguracijom i funkcionalnostima ostvaruje mnoge prednosti i dodanu vrijednost za korisnike i pružatelje usluga. Neki od ključnih aspekata All-IP koncepta su sljedeći:

- u potpunosti IP bazirana mreža,
- podržava različite vrste pristupnih mreža,
- napredno upravljanje mobilnošću korisnika,
- poboljšano upravljanje sesijama,
- kvalitetnije usluge,
- poboljšane mrežne performanse,
- jednostavnije upravljanje mrežom,
- veća razina sigurnosti i privatnosti korisnika,
- garantirana kvaliteta usluge odnosno QoS (*eng. Quality of Service*),
- jednostavna identifikacija korisnika.

All-IP mreža u potpunosti je bazirana na IP protokolu. Segmenti unutar All-IP koncepta jednoznačno su identificirani sa IP adresom te se paketi informacija između njih usmjeravaju upravo na osnovu dodijeljenih IP adresa. Funkcionalnosti mreže prebačene su na rubni dio mreže, čime se omogućuje međudjelovanje sa ostalim vrstama mreža koje nisu bazirane na IP protokolu i koje koriste stariju mrežnu opremu. Time je korisnicima omogućen pristup All-IP mreži i njezinim funkcionalnostima neovisno o vrsti pristupne mreže koju koriste.

Upravljanje mobilnošću korisnika odvija se unutar pristupnih mreža. Karakterizira ju brzo prekapčanje odnosno *handover* između različitih pristupnih mreža, čime se korisnicima omogućuje korištenje usluga zadovoljavajuće kvalitete i u trenutcima njihova kretanja. Podržani su mehanizmi prekapčanja koji su bazirani na unaprijed definiranoj razini kvalitete usluge. Spomenuti mehanizmi obavljaju prekapčanje na drugu pristupnu točku u trenutku kada detektiraju degradaciju usluge čime se korisnicima osigurava zadovoljavajuća razina kvalitete usluge koju koriste.

Korisnicima koji se nalaze unutar All-IP mreže omogućene su tri vrste mobilnosti, a to su mobilnost sjednice, osobe i terminalnog uređaja. Mobilnost sjednice podrazumijeva održavanje postojeće sjednice i u trenutku kada korisnik mijenja terminalni uređaj. Mobilnost osobe omogućuje korisniku pristup usluzi putem bilo kojeg terminalnog uređaja na temelju svog profila. Mobilnost terminalnog uređaja podrazumijeva sposobnost uređaja da koristi uslugu iako je u pokretu te kontinuirano mijenja svoj položaj.

Poboljšano upravljanje sesijom, koja je jedna od odlika All-IP koncepta, omogućuje korisnicima korištenje kvalitetnijih usluga koje su neovisne o korištenom terminalnom uređaju i o trenutnim performansama mreže. Na taj se način aktualna sesija bez ikakve intervencije korisnika može preusmjeriti na drugi terminalni uređaj na temelju korisničkog identifikatora.

Podržano je korištenje tradicionalnih usluga kao i novih naprednih telekomunikacijskih usluga. Moguća je integracija sličnih usluga, kao što su integracija klasičnog i video poziva. Omogućeno je korištenje grupne komunikacije kroz razne aplikacije za dopisivanje kao i mogućnost obavljanja poziva između više sudionika.

All-IP mreža u mogućnosti je efikasno upravljati različitim vrstama IP prometa kao što su to komunikacija između dva sudionika (*eng. user-to-user*) te komunikacija jednog korisnika sa grupom sudionika (*eng. user-to-multicast*).

Razina sigurnosti mreže i korisnika povećana je u odnosu na prethodne modele mreža. Sigurnost mreže ostvaruje se skrivanjem elemenata mreže čime se onemogućuju sigurnosni napadi na mrežu odnosno njegove elemente. Sigurnost korisnika ostvaruje se kroz napredne mehanizme autorizacije i autentikacije, dok se njihove komunikacije zaštićuju primjenom naprednih enkripcijskih mehanizama.

Razina kvalitete usluge odnosno QoS-a glavna je odlika svake mreže i usluge. All-IP mreža u mogućnosti je osigurati garantiranu razinu usluge od izvorišta do odredišta komunikacije. Neovisno o načinu prijenosa informacija, bio to *unicast* ili *multicast* promet, korisnicima su u svakome trenutku dostupne usluge po prethodno dogovorenoj razini kvalitete.

Korisnici koriste usluge različitih davatelja usluga kojima pristupaju kroz autentikacijske parametre. Ukoliko korisnik koristi nekoliko usluga odjednom, povećava se kompleksnost njihova korištenja. All-IP koncept, i u ovome problemu, pronalazi rješenje u vidu grupe identiteta (*eng. Identity Federation*). Na taj način, korisnik prilikom svoje autentikacije na jedan servis odnosno uslugu davatelja usluga, ostvaruje i pristup na ostale usluge koje pruža taj davatelj usluge, ukoliko se identitet nalazi unutar ranije spomenute grupe identiteta, [2].

2.2. Prednosti implementacije All-IP mreže

Migracija i implementacija All-IP koncepta sa sobom donosi mnoge pogodnosti. Omogućeno je kreiranje i korištenje kvalitetnijih telekomunikacijskih usluga nego prije. Korisnicima je omogućena mobilnost te su u stanju koristiti usluge bilo gdje i sa bilo kojeg terminalnog uređaja koristeći bilo koji oblik pristupne mreže. Kvaliteta prijenosa informacija mrežom značajno je poboljšana kroz povećani propusni pojas, jednostavnije upravljanje mrežom i kvalitetnije sigurnosne mehanizme.

Osim spomenutih poboljšanih mrežnih performansi, All-IP koncept omogućuje jednostavnije korištenje raznovrsnih usluga uz garantiranu razinu kvalitetu. Postojeće telekomunikacijske usluge su uznapredovale te se pojavio veliki broj inovativnih usluga koje su upravo omogućene kroz All-IP mrežu i njezine funkcionalnosti.

Konvergencija različitih mreža i tehnologija u jedan segment te omogućavanje komunikacije korisniku prilikom kretanja glavni je aspekt All-IP mreže. Mobilnost korisnika odnosno njegove komunikacije omogućuje se primjenom protokola za mobilnost korisnika kao što su to MIP (*eng. Mobile IP protocol*) i PMIP (*eng. Proxy Mobile IP protocol*). Upravo su spomenuti protokoli temeljni aspekt ovog istraživanja te će detaljno biti razrađeni u sklopu 5. i 6. poglavlja ovog rada.

U nastavku ovog poglavlja biti će razrađene neke od glavnih usluga baziranih na Internetskom protokolu i All-IP mrežnom okruženju kao što su VoIP (*eng. Voice over IP*), IPTV (*eng. Internet Protocol Television*) i Internet stvari (*eng. Internet of Things*). Spomenute usluge predstavljaju poboljšanje dosadašnjih usluga prijenosa govora i videa te pojava potpuno novog tehnologijskog i telekomunikacijskog okruženja koje nudi koncept Internet stvari.

2.2.1. Usluga prijenosa govora Internet protokolom

Telefon odnosno prijenos govora odavno je bitan faktor svakodnevnice kako u privatnom okruženju, tako i poslovnome. Funkcioniranje kompanija nezamislivo je bez korištenja telefona kao osnove za svako uspješno poslovanje. Kako bi smanjili troškove prijenosa govora, kao rješenje se pojavilo korištenje jeftine komunikacijske tehnologije kao što je IP protokol. Integracija standardne telefonije i komunikacije putem IP protokola omogućila je prijenos govora putem IP mreže. *Voice over IP* ili skraćeno VoIP predstavlja rješenje prijenosa govora putem Internet protokola.

Metoda prijenosa govora kod standardne telefonije je komutacija kanala što znači da je svakom razgovoru odnosno komunikaciji predodređen jedan kanala za komuniciranje. VoIP tehnologija se uvelike razlikuje od standardne telefonije iz razloga što se analogni telefonski signal pretvara u digitalni oblik. Nakon digitalizacije signala obavlja se njegovo komprimiranje te zatim i paketiziranje. Novo kreirani signal odnosno digitalna poruka ne šalje se na govorni kanal već putuje podatkovnim linijama lokalnog intraneta ili pak globalnog Interneta.

Prednosti *Voiceover IP* tehnologije su sljedeće:

- jeftiniji u odnosu na klasičnu telefoniju,
- broj poziva po liniji nije ograničen,
- korisniku omogućuje mobilnost pri korištenju broja uz uvjet postojana Internet mreže,
- nepostojanje troškova poziva unutar lokalne mreže odnosno intraneta,
- neovisnost o telefonskoj mreži.

VoIP sa sobom povlači određene nedostatke i uvjete:

- oba sudionika istovremeno moraju imati pristup IP mreži,
- kvaliteta poziva ovisna je o brzini i pouzdanosti mreže,
- mogućnost prisluškivanja poziva putem malicioznih softvera, [3].

VoIP i klasična telefonija, kao što je spomenuto, uvelike se razlikuju u načinu funkcioniranja i ostvarenja usluge na način da koriste različite tehnologije, pristup samoj usluzi i protokole. Međutim, neke od komponenata spomenutih sustava prisutne su u oba sustava uz razliku u načinu njihove implementacije i funkcioniranja. VoIP tehnologija pruža sve funkcionalnosti koje su vezane za klasičnu telefoniju uz dodatnu mogućnost slanja podataka.

VoIP sustav sastoji se od sljedećih komponenata:

- mrežna infrastruktura,
- procesori,
- prevodioci,
- VoIP terminali,
- osobna računala.

Mrežna infrastruktura VoIP usluge u potpunosti je izvedena unutar IP platforme te predstavlja temeljnu komponentu za pružanje same usluge. VoIP mrežu možemo gledati kao logičku glasovnu mrežu distribuiranu putem IP okosnice. IP mreža, kao temelj distribucije VoIP usluge, mora biti u stanju odgovoriti na sve zahtjeve VoIP usluge kako bi korisnici u potpunosti mogli koristiti sve njezine pogodnosti.

Procesori predstavljaju module koji služe za uspostavljanje i kontroliranje poziva. Njihova zadaća je autorizacija korisnika, pružanje odnosno ostvarenje telefonske usluge kao i nadziranje brzine prijenosa (*eng. bandwidth*) glasovnih paketa za svaku pojedinačnu liniju.

Temeljna zadaća prevodioca (*eng. Signaling gateways*) je stvaranje poziva kao i njihova detekcije. Pretvaraju glas iz analognog oblika u glasovne digitalne pakete kako bi isti mogli biti odaslani putem IP mreže. Također omogućuju i prijelaz između različitih tehnologija, poput IP-a i ISDN-a (*eng. Integrated Services Digital Network*), kako bi se VoIP korisnicima omogućila komunikacija sa korisnicima klasične telefonije.

Kako bi korisnici bili u mogućnosti koristiti sve pogodnosti VoIP usluge moraju posjedovati odgovarajuće terminalne uređaje. Postoje različite vrste terminalnih uređaja u ovisnosti o načinu na koji korisnici koriste uslugu pa tako postoje klasični, konferencijski i mobilni VoIP terminalni uređaji.

Osobna računala također mogu biti korištena kao terminalni uređaj. Uz osnovnu opremu, za ostvarenje VoIP usluge korisnici moraju posjedovati slušalice sa mikrofonom. Primjer korištenja osobnog računala za ostvarenja glasovne i video komunikacije je *Skype* usluga, [4].

2.2.2. IP televizija (IPTV)

Pojava koncepta IP televizije odnosno IPTV-apredstavlja najveći iskorak u okruženju TV usluga nuđenjem većeg broja interaktivnih mogućnosti. IP televizija predstavlja skup usluga te podržava emitiranje klasičnog TV sadržaja, videa na zahtjev, plaćanja po gledanom sadržaju, usluge prijenosa televizijske slike visoke razlučivosti i usluge osobnog videorekordera.

IP televizija je sustav namijenjen za primanje i prikaz tijekom video podataka kodiranog kao niz IP paketa. Predstavlja novu generaciju televizije koja omogućuje, uz praćenje televizijskog programa kao i kod klasične televizije, slušanje radio kanala kao i korištenje mnogih interaktivnih usluga. Suvremeni pametni televizori poprimili su sva glavna obilježja osobnih računala te se njihova primjena ne razlikuje značajno od primjene računala.

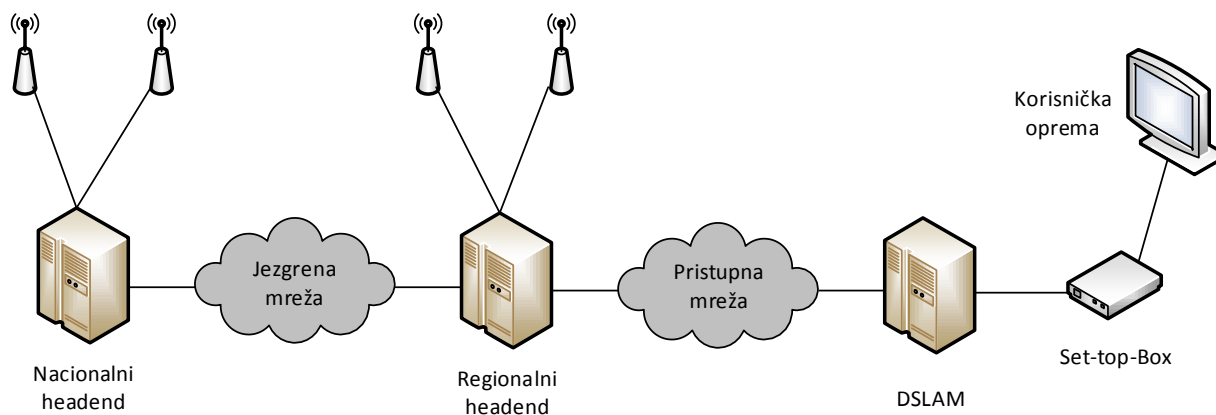
Neke od glavnih značajki IPTV-a su:

- televizija uživo,
- mogućnost zaustavljanja TV programa i gledanje prethodnog sadržaja,
- mogućnost posuđivanja filmova kao i bilo kakvog sadržaja nevezanog uz TV program poznatijim pod nazivom VOD (*eng. Video On Demand*).

Za ostvarenje i ugodno korištenje takovih usluga potrebna je brza pristupna mreža dostatnih prijenosnih kapaciteta kako bi se kreirani IP paketi na određite dostavili sa zadovoljavajućom razinom kvalitete. Krajnji korisnik mora posjedovati podatkovnu brzinu u dolaznome smjeru iznad 20 Mbit/s.

IPTV funkcioniše na zatvorenom mrežnom okruženju uz osiguranu razinu propusnosti neophodne za nesmetan protok video podataka visoke kvalitete. Za razliku od Internet TV-a koji koristi *best-effort* metodu, IPTV koristi unaprijed rezervirani opseg propusnosti isključivo za prijenos video sadržaja. Kako bi se IPTV mogao koristiti potreban je poseban uređaj *Set-Top-Box* (STB). Glavna karakteristika IP televizijskog sustava je da predstavlja zatvoreni sustav u kojem davatelji usluge određuju i rezerviraju odgovarajući broj kanala koji će biti dostupni krajnjem korisniku kako bi mogao koristiti uslugu,[5.]

Kako bi se usluga IP televizije na efikasan i kvalitetan način dostavila do krajnjih korisnika nužno je postojanje adekvatne mrežne infrastrukture. Mrežna arhitektura IP televizije sastoji se od četiri glavna dijela, a to su *headend*, transportna i pristupna mreža te kućna mreža korisnika.



Slika 1. Mrežna arhitektura IPTV usluge

Izvor: [22]

Headend predstavlja adapter koji se nalazi između različitih izvora sadržaja u različitim formatima i mreže operatora. *Headend* rješenja sadrži distribuiranu arhitekturu gdje se sadržaj za prijenos do krajnjeg korisnika priprema na više različitih lokacija.

Transportna mreža zadužena je za prijenos video sadržaja u prilagođenom formatu od *headend-a* do pristupne mreže. Prijenos video sadržaja putem transportne mreže moguć je na dva načina, *multicast* ili *unicast* prijenosom. *Unicast* prijenos predstavlja vrstu prijenosa informacija od jednog izvora do jednog krajnjeg korisnika. Radi uštede prijenosnih resursa, češće se koristi *multicast* prijenos IPTV usluge iz razloga što se iz jednog izvora video sadržaj može prenijeti do većeg broja korisnika.

Pristupna mreža zadužena je za prijenos video i audio sadržaja od transportne mreže do krajnjeg korisnika. Kreirani sadržaj se prenosi do ADSL (*eng. Asymmetric Digital Subscriber Line*) modema ili TILGIN modema ukoliko korisnik posjeduje optičku pristupnu mrežu. Pristupna mreža završava na spomenutim modemima.

Kućna mreža korisnika sastoji se od modema koji se *Ethernet* kablom povezan na STB uređaj. Uloga STB uređaja je dekriptiranje i dekodiranje video sadržaja. STB uređaj se zatim povezuje sa samim TV prijarnikom, [6].

2.2.3. Internet stvari (IoT)

Ubrzani razvoj Interneta omogućuje stvaranje nove vizije i budućnosti Internet poznatiju pod nazivom IoT (*eng. Internet of Things*). Sadašnji Internet predstavlja mrežu međusobno povezanih računala, dok Internet stvari predočuje mrežu međusobno povezanih objekata u kojoj pojam „stvari“ pokriva široki spektar aktivnih uređaja kao su senzori, mjerači i druge naprave. Koncept Internet stvari podrazumijeva povezanost pametnih uređaja i konvencionalnih potrošačkih elemenata omogućavajući na taj način pojavu mnogih inovativnih i vrlo korisnih mogućnosti. Prednosti koje sa sobom povlači IoT nisu samo sociološkog i tehnološkog napretka, već će u budućnosti predstavljati i značajan element ekonomskog aspekta odnosno ušteda.

Veliki broj senzora danas su već ugrađeni u različite objekte i elemente što će uvelike doprinijeti još bržoj pojavi IoT koncepta. Neke studije o Internet stvari predviđaju da će do 2020. godine biti povezano oko 50 milijardi senzora i uređaja. Povezivanje tako velikog broja senzora i uređaja te njihova međusobna komunikacija omogućiti će pojavu mnoštva inovativnih usluga kao i pojednostavljenje postojećih.

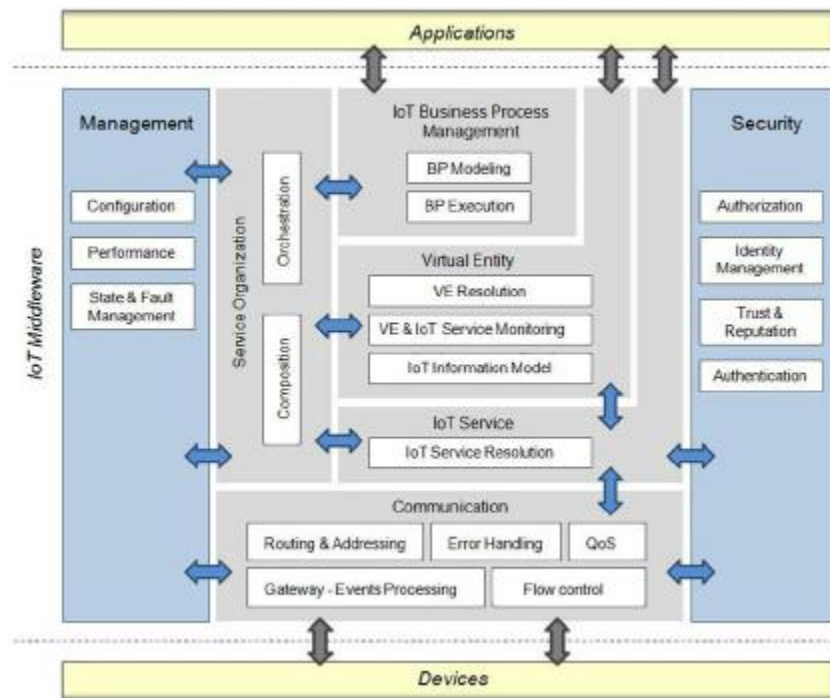
Internet stvari predstavlja koncept i paradigmu koja proučava objekte, uređaje i senzore koji bežičnim ili žičnim povezivanjem, uz primjenu jednostavnih adresnih shema, ostvaruju mogućnost međusobne komunikacije i suradnje, a sve u cilju ostvarenja novih aplikacija i usluga. Temeljna funkcija povezanih uređaja je prikupljanje informacija iz njihovog neposrednog okruženja te dijeljenje prikupljenih i obrađenih podataka putem mreže bazirane na IP protokolu. Podijeljene informacije koriste se za daljnju obradu i korištenje kako bi se ostvarila određena dobit njihovom uporabom.

Za razliku od dosadašnjeg vertikalnog razvoja pojedinih područja i tehnologija, kao što su tehnologije povezivanja uređaja u pokretu, bežičnih senzorskih mreža, obrade velikih količina podataka, dodavanjem novog programskog međusloja moguće je ostvariti koncept Interneta stvari. Programski međusloj zadužen je za povezivanje različitih tehnologija i platformi te čini okosnicu za razvoj naprednih usluga bez posjedovanja, do sada potrebnih, znanja o svakoj tehnologiji zasebno. Umrežavanjem sve većeg broja objekata koji nas okružuju rezultirati će velikom količinom generiranih podataka koji moraju biti pohranjeni, obrađeni i prezentirani u prihvatljivom obliku. Mogućnost korištenja usluga u okruženju Internet stvari su raznolike, od korisničkih aplikacija koje će pružati dodanu vrijednost samo korisniku koji ih je definirao do cjelokupnih grana znanosti kojima je omogućeno pojednostavljeno dijeljenje resursa, prikupljanje podataka iz velikog broja senzora, statistička analiza tih podataka ili čak zaključivanje nad podacima u stvarnom vremenu.

Objekti i senzori u sklopu IoT koncepta definiraju se kao stvarni fizički odnosno virtualni subjekti koji imaju mogućnost međusobne detekcije, kao i međusobne komunikacije u vidu razmjenjivanja potrebnih informacija. Identificiraju se na temelju dodijeljenih identifikacijskih brojeva, imena, lokacijskoj adresi ili IP adresi. Objekti međusobno komuniciraju putem mreže bazirane na IP protokolu na način da će svakome objektu biti dodijeljena jednoznačna IP adresa, [7].

Arhitektura sustava Internet stvari sastoji se od nekoliko komponenata od kojih svaka ima specificiranu funkciju. Prema mogućnostima i definiranim funkcijama spomenute komponente svrstavaju se u razinu izvora podataka koja je zadužena za prikupljanje informacija iz okoline i posredničku razinu koja je zadužena za obradu i distribuciju prikupljenih informacija.

Za prikaz arhitekture sustava Internet stvari najoptimalnije je korištenje IoT-A referentnog modela, prikazanog slikom 2., koji predstavlja njegovu generičku arhitekturu. Cilj referentnog modela je omogućiti projektantima sustava izradu arhitektura i rješenja prema vlastitim zahtjevima iz razloga što referentni model opisuje osnovne elemente sustava te omogućuje izbor dizajna koji se može nositi sa specifičnim zahtjevima vezanim uz funkcionalnosti, performanse, sigurnost i razvoj pojedinih aplikacija. IoT-A platforma sastoji se od sloja uređaja, komunikacijskog, upravljačkog te aplikacijskog sloja.



Slika 2. IoT-A referentni model, [23]

Sloj uređaja (*eng. Devices*) zadužen je za integraciju uređaja različitih funkcionalnosti i dobavljača. Komunikacijski sloj (*eng. Communication*) predstavlja skup metoda za međusobno povezivanje i komunikaciju uređaja čak i ako sami uređaji ne koriste isti protokol. Također i obavlja usmjeravanje prikupljenih informacija na temelju samog sadržaja.

Unutar sloja usluge (*eng. IoT service*) nalaze se podaci o svim uslugama te ovisno u usluzi daje poveznicu prema resursima koje pojedina usluga zahtijeva. Spomenuti sloj obavlja i obradu prikupljenih informacija te šalje obavijesti o resursima i objektima koje usluga koristi. Sloj virtualnog entiteta (*eng. Virtual entity*) posjeduje informacije o fizičkim objektima i resursima. Omogućuje pretragu usluga na temelju fizičkih objekata s kojima je sama usluga povezana na način da vraća adrese svih usluga koje su povezane na pojedini objekt.

Sloj organizacije usluge (*eng. Service organization*) predstavlja centralni sloj čija je zadaća povezivanje upita viših slojeva ili vanjskih aplikacija sa uslugama koje resursi Internet stvari omogućuju. Omogućuje i povezivanje više različitih jednostavnih usluga u svrhu rješavanja upita dobivenog od višeg sloja, kao što je na primjer povezivanje usluge detekcije vlage i usluge očitavanja temperature kako bi se dobila pravovremena informacija o nastaloj požaru odnosno usluga detekcije požara.

Sloj upravljanja IoT poslovnim procesima (*eng. IoT business process management*) vrši integraciju postojećih tradicionalnih poslovnih rješenja sa IoT-A referentnim modelom. Time je omogućeno proširenje i obogaćenje trenutnih poslovnih rješenja te na taj način kompanije mogu iskoristiti sve prednosti koncepta Internet stvari. Rezultat toga su smanjenje troškova poslovanja, kao i izbjegavanje dodatnih financijskih opterećenja, zbog dodatnih ulaganja u postojeća rješenja.

Sloj upravljanja (*eng. Management layer*) odgovoran je za praćenje i sastavljanje svih akcija koje uključuju jedan ili više slojeva. Tako je sloj upravljanja primjerice zadužen za stavljanje IoT sustava u stanje spavanja radi uštede energije kao i za ponovno stavljanje sustava u produkcijsko stanje.

Sigurnosni sloj (*eng. Security layer*) odgovoran je za sigurnost i privatnost sustava Internet stvari. Zadužen je za autorizaciju i autentikaciju klijenata na IoT mrežu čime se osigurava da samo provjereni klijenti imaju pristup uslugama. Osigurava zaštitu privatnih korisničkih podataka, kao i sigurnu komunikaciju između krajeva sustava koji si međusobno vjeruju.

S obzirom na buduću globalnu primjenu IoT okruženja nužna je standardizacija arhitekture, platforme i komunikacije među komponentama sustava. Izazovi prilikom realizacije koncepta Internet stvari vezani su za regulaciju tržišta, naplate, sigurnosti te poboljšanja performansi, kao i podrške za kvalitetu usluge.

U području obrade podataka u stvarnome vremenu nužna je standardizacija upitnog jezika, određivanja parametara za evaluaciju komponenata te prilagodba algoritma za obradu tokova računalstvu u oblaku i karakteristikama ulaznih podataka. Aspekt sigurnosti vrlo je bitan kako bi se osigurala otpornost cjelokupnog sustava na sigurnosne napade. Iz tog razloga potrebna je adekvatna kontrola pristupa i provjera podataka kao i očuvanje privatnosti korisnika sustava. Prilikom određivanja komunikacijskih protokola i izrade uređaja posebnu pažnju treba obratiti energetske učinkovitosti. Smanjenje utroška električne energije moguće je ostvariti prebacivanjem logike i odlučivanja na rubne krajeve IoT arhitekture odnosno na senzorski sloj ukoliko sama usluga ne zahtjeva velike procesorske resurse.

Objekti IoT arhitekture moraju imati mogućnost međusobne komunikacije kako bi pružali informacije o sebi, kao i prihvaćali informacije koje su prikupili drugi objekti. S ciljem povezivanja objekata i uređaja sa velikim bazama podataka i mrežama, nužan je jednostavan i jeftin sustav identifikacije. RFID (*eng. Radio Frequency Identification*) tehnologija dobro je rješenje za međusobnu identifikaciju uređaja i objekata. Nakon identifikacije objekata moguće je prikupljanje podataka o njima te njihova obrada. Kako bi se podaci prikupili nužna je uporaba senzora koji imaju mogućnost detekcije promjene fizičkog statusa objekta.

S obzirom na sve prethodno navedeno, neki od ključnih izazova prilikom realizacije koncepta Internet stvari su:

- sigurnost, privatnost i povjerenje,
- upravljanje heterogenih aplikacija, okruženja i uređaja,
- ograničenja mrežnih kapaciteta,
- upravljanje velikom količinom informacija i obrada velike količine podataka,
- regulacija tržišta,
- projektiranje učinkovite arhitekture za umrežavanje senzora i pohranu prikupljenih podataka,
- razvijanje mehanizma za obradu toka podataka prikupljenih senzorskim mrežama,
- napajanje uređaja i senzora, [8].

3. Arhitektura i funkcioniranje All-IP mreže

Zamisao 3GPP (*eng. Third Generation Partnership Project*) projekta je da se mobilne tehnologije unaprijede na veću razinu realizacijom veće propusnosti (*eng. bandwidth*), boljim korištenjem spektra, širom pokrivenosti i boljom interoperabilnosti različitih pristupnih mreža i tehnologija. Sve prethodno navedeno efikasno se može riješiti primjenom All-IP jezgrene mreže sa dobro definiranom suradnjom sa sustavima baziranim na komutaciji kanala. All-IP mreža predstavlja hibridno rješenje koje podržava različite pristupne mreže i tehnologije.

All-IP mrežna arhitektura podržava E-UTRAN (*eng. Evolved UMTS Terrestrial Radio Access Network*) pristupnu mrežu. Samim time smanjuje se broj elemenata mreže, omogućuje se jednostavnije funkcioniranje mreže, povećava se zalihost resursa i što je najvažnije, omogućeno je povezivanje i prekapčanje na druge fiksne linije i bežične tehnologije. Na taj način mobilni operateri mogu korisnicima ponuditi iskustvo potpune mobilnost gdje sami korisnici nemaju nikakvo ograničenje niti su svjesni korištenja različitih pristupnih mreža i tehnologija.

Jezgrena mreža EPC (*eng. Evolved Packet Core*) u potpunosti je zasnovana na komutaciji paketa odnosno prijenosu paketiziranih informacija posredstvom IP protokola. Prijenos govora, koji se prije prenosio komutacijom kanala, uz pomoć IMS-a (*eng. IP Multimedia Subsystem*) prenosi se komutacijom paketa. All-IP mreža, osim mrežnih elemenata koji će biti razrađeni u poglavljima 3.1.1., 3.1.2., 3.1.3., 3.1.4., i 3.1.5., sastoji se i od kontrolnih elemenata kao što su server za autorizaciju i autentikaciju te elemenata za kontrolu kvalitete usluge.

Jezgrena i pristupna mreža kao cjelokupni sustav ostvaruju mnoge funkcionalnosti kao što su:

- kontrola pristupa mreži,
- usmjeravanje i prijenos IP paketa mrežom,
- upravljanje mobilnošću,
- održavanje sigurnosti komunikacije,
- upravljanje prijenosnim resursima,
- upravljanje mrežom u cjelini, [9].

3.1. Evoluirana paketskajezgrena mreža

Većina suvremenih usluga odnosno aplikacija koriste telekomunikacijsku mrežu kako bi pružale svoje funkcionalnosti korisnicima te je time znatno povećan mrežni promet odnosno količina paketa u mobilnim telekomunikacijskim mrežama. LTE/EPC (*eng. Long Term Evolution / Evolved Packet Core*) tehnologija omogućava znatno efikasnije slanje takvih paketa podataka u odnosu na 3G mobilne sustave. Ovo tehnologiju karakterizira niska latencija u prijenosu podataka koja omogućuje prijenos glasa odnosno govora komutacijom paketa.

Evoluirana paketskajezgrena mreža usvojena je kao nova arhitektura jezgrene mreže, koja omogućuje efikasniji prijenos IP paketa, za postojeće 2G i 3G mobilne telekomunikacijske sustave. Prethodno spomenuta tehnologija, koja kao jezgrenu mrežu koristi upravo EPC, danas predstavlja globalni standard usvojen od strane mobilnih operatera širom svijeta.

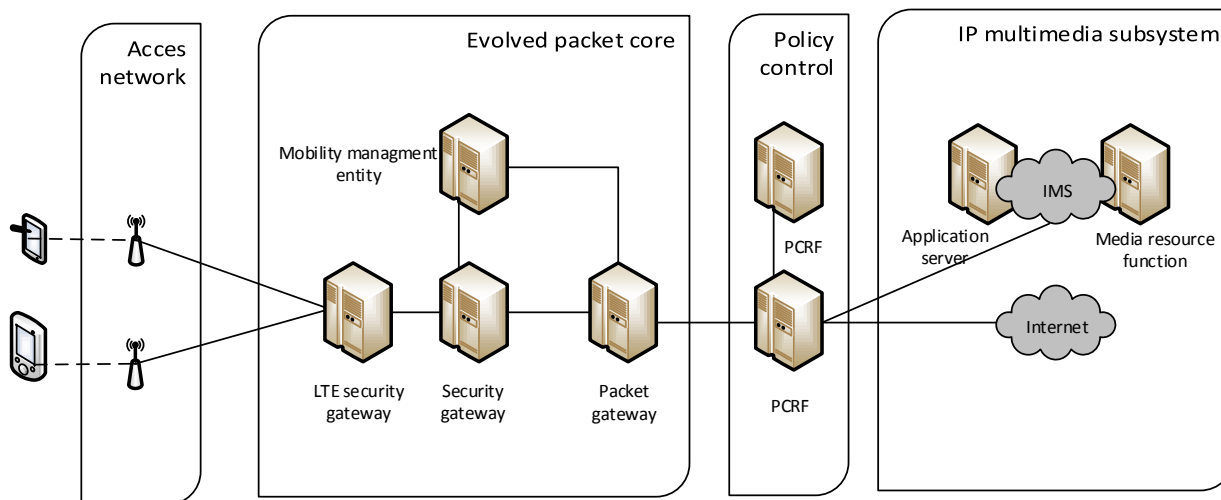
EPC predstavlja jezgrenu mrežu baziranu na IP protokolu te je standardizirana u 8. izdanju 3GPP projekta. Omogućuje integraciju sinkronog načina prijenosa odnosno STM (*eng. Synchronous Transfer Mode*), asinkronog načina prijenosa odnosno ATM (*eng. Asynchronous Transfer Mode*) i internet protokola u postojećim 3G mobilnim sustavima.

Ovakva jezgrena mreža omogućuje migraciju bilo koje mreže na IP baziranu okosnicu. Samim time telekom operaterima je omogućeno učinkovitije nuđenje različitih usluga kao što je prijenos glasa temeljenog na IP protokolu (VoIP) putem IMS-a. Osim toga, korištenjem EPC-a moguće je istovremeno spajanje na više mreža baziranih na prijenosu paketa na način da se prijenos podataka odvija putem Interneta, dok se prijenos glasa odnosno govora odvija uz pomoć IP multimedijskog podsustava (IMS). Također, omogućuje i prekapčanje (*eng. Handover*) između pristupnih mreža kao što su 2G ili 3G sustavi ili WiFi (*eng. Wireless Fidelity*) ili CDMA2000 (*eng. Code Division Multiple Access*) sustavi.

S obzirom na sve navedeno, neke od najznačajnijih karakteristika evoluirane paketske jezgre mreže su sljedeće:

- predstavlja globalni standard,
- u potpunosti bazirana na IP protokolu,
- omogućuje “*always-on*” povezanost,
- prijenos glasa se odvija uz pomoć IP paketa (VoIP),
- omogućuje povezanost i sa mrežama koje nisu obuhvaćene sa 3GPP-om.

Arhitektura EPC-a prikazana je slikom 3. te se sastoji od MME (*eng. Mobility Management Entity*), S-GW (*eng. Serving Gateway*), PDN-GW (*eng. Packet Data Network Gateway*) i PCRF (*eng. Policy and Charging Rules Function*). Elementi EPC arhitekture biti će razrađeni u sljedećim poglavljima, [10].



Slika 3. Arhitektura evoluirane paketske jezgre mreže

Izvor: 24

3.1.1. Entitet upravljanja mobilnošću

Mobility management entity (MME) odnosno entitet upravljanja mobilnošću predstavlja temeljni čvor jezgrene mreže. Njegova funkcija je obrada i prosljeđivanje signalizacijskih poruka koje se izmjenjuju preko kontrolne ravnine između korisničke terminalne opreme i ostalih čvorova jezgrene mreže. Signalizaciju obavlja uz pomoć NAS (*engl. Non Access Stratum*) protokola. Entitet upravljanja mobilnošću također je zadužen i za čvorove pristupne mreže.

Temeljne funkcije entiteta upravljanja mobilnošću su sljedeće:

- NAS signalizacija,
- sigurnost NAS signalizacije,
- kontrola sigurnosti u pristupnom sloju,
- odabir PDN-GW i S-GW elemenata,
- upravljanje mobilnošću prilikom prelaska na druge mreže,
- odabir SGSN-a prilikom prekapčanja između LTE i 3GPP 2G/3G pristupnih mreža,
- autentikacija korisnika,
- upravljanje retransmisijom i funkcijama pronalaska korisničke opreme, [11].

3.1.2. Uslužni prilazni čvor

Serving gateway (S-GW) ili uslužni prilazni čvor zadužen je za povezanost korisničke opreme i *Packet Data Network Gatewaya* (PDN-GW). Uslužni prilazni čvor tunelira podatke prema PDN-GW te prati kretanje korisničkog terminalnog uređaja između baznih stanica pristupne mreže. Ukoliko korisnik prijeđe u područje druge bazne stanice dolazi do promjene uslužnog prilaznog čvora.

Zadužen je za reguliranje uspostave veze sa korisnicima neke druge mreže te predstavlja lokalnu točku za proces prekapčanja između baznih stanica i za pokretljivost između 3GPP mreža.

Neke od funkcionalnosti uslužnog pristupnog čvora su sljedeće:

- slanje i prosljeđivanje podatkovnih paketa,
- zakonsko presretanje poziva,
- označavanje paketa na transportnoj razini za ulaznu i silaznu vezu,
- upravljanje privremenom pohranom paketa u stanju mirovanja,
- upravljanje zahtjevima za uslugom, [11].

3.1.3. Paketski mrežni prilazni čvor

Packet data network gateway (PDN-GW) odnosno paketski mrežni prilazni čvor predstavlja završnu točku podatkovnog sučelja prema podatkovnoj mreži baziranoj na IP protokolu. Kao i uslužni prilazni čvor, osigurava vezu između korisničke opreme i SAE-GW, kojeg čine S-GW i PDN-GW .

Paketski mrežni prilazni čvor svojim sučeljem s jedne strane povezan je s uslužnim prilaznim čvorom, a sa druge strane sa IP podatkovnom mrežom. Za razliku od uslužnog prilaznog čvora koji se mijenja sa promjenom lokacije korisnika, paketski mrežni prilazni čvor ostaje isti sve dok je korisnički terminal povezan na mrežu.

Paketski mrežni prilazni čvor sadrži mnogo funkcionalnosti, a neke od njih su:

- alokacija IP adrese korisničkog terminala,
- filtriranje i provjera paketa,
- zakonsko presretanje poziva,
- označavanje paketa na transportnoj razini u silaznoj i uzlaznoj vezi,
- *online* naplata, [11].

3.1.4. Čvor za upravljanje resursima i terećenjem

Policy charging and rules function (PCRF) odnosno čvor za upravljanje resursima i terećenjem zadužen je za donošenje odluka o upravljanju resursima te za kontrolu naplate na temelju protoka podataka kroz PDN-GW. Zadužen je i za autorizaciju kvalitete usluge kojom se odlučuje na koji način će se tretirati pojedini tok podataka u skladu sa korisnički pretplatničkim ugovorom.

Čvor za upravljanje resursima i terećenjem nadležan je za nadzor mreže. Od PDN-GW prima informacije o mediju i sjednici koje prije spremanja provjerava jesu li sigurne i pouzdane, [12].

3.1.5. Poslužitelj domaćih pretplatnika

Home subscriber server (HSS) odnosno poslužitelj domaćih pretplatnika zadužen je za upravljanje korisničkim profilima. U skladu s time, vrši autentikaciju i autorizaciju korisnika. Korisnički profili sastoje se od informacija vezanih za pretplatu, sigurnost, kvalitetu usluge i pristupna ograničenja kod prekapčanja na stranu mrežu te lokaciji na kojoj se trenutno nalazi korisnik odnosno njegov terminalni uređaj.

Posjeduje informacije o paketskim podatkovnim mrežama (*eng. Packet Data Network - PDN*) na koje korisnik ima mogućnost povezivanja u obliku imena pristupne točke ili kao PDN adresa koja ukazuje na pretplatničku IP adresu.

HSS također sadrži i dinamičke informacije o identitetu MME-a na koji je korisnički terminalni uređaj upravo spojen odnosno registriran. Posjeduje centar za autentikaciju i sigurnosne lozinke pa tako kada MME zaprimi zahtjev od korisnika za povezivanje na mrežu, MME šalje zahtjev na provjeru poslužitelju domaćih pretplatnika kako bi se provjerila autentičnost podataka, [13].

3.2. IP višemedijski podsustav

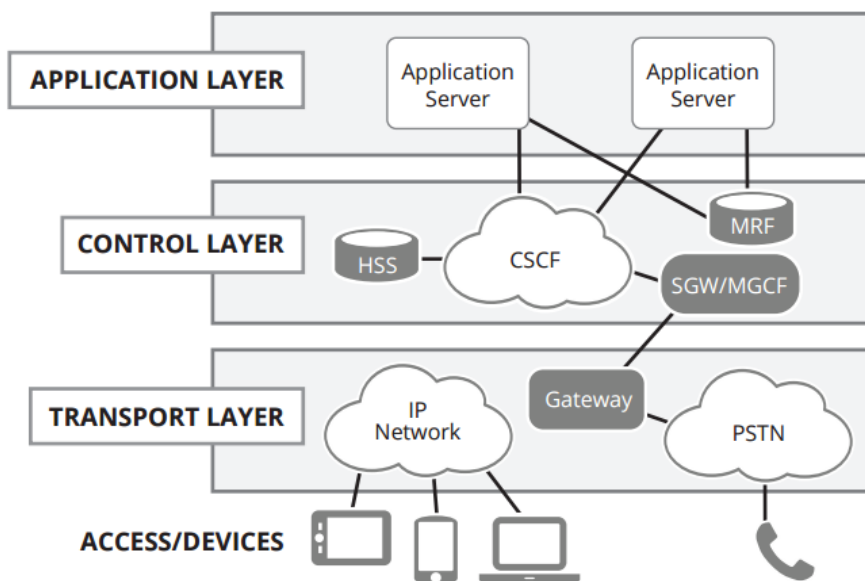
IP višemedijski sustav odnosno IMS (*eng. IP Multimedia Subsystem*) definiran je skupinom standarada koje je izdao 3GPP i druga standardizacijska tijela okupljena oko 3GPP-a. Predstavlja standard za multimedijalne komunikacijske usluge u stvarnome vremenu. Njegova arhitektura u potpunosti je bazirana na IP protokolu te se sastoji od sloja aplikacije, sloja kontrole sjednice i sloja kontrole medija.

Omogućuje fiksnim i mobilnim korisnicima glasovnu i video komunikaciju, razmjenu poruka u realnom vremenu, igranje igara u stvarnom vremenu kao i informaciju o dostupnosti drugoga korisnika te načinu na koji on želi komunicirati. Predstavlja okvir za nezavisan pristup putem LTE, UMTS (*eng. Universal Mobile Telecommunications System*), GPRS (*eng. General Packet Radio Service*), WLAN (*eng. Wireless Local Area Network*), ADSL (*eng. Asymmetric Digital Subscriber Line*) ili PSTN (*eng. Public Switched Telephone Network*) mreže.

Uloga IP višemedijskog sustava u jezgrenoj mreži bežičnih operatora je omogućavanje integracije raznih naprednih i višemedijskih sustava te konvergencija postojećih mreža s Internetom kako bi se kreirala jedinstvena pokretna širokopolasna mreža. U jezgrenoj mreži nepokretnih operatora cilj IMS-a je kreiranje jedinstvene platforme za pružanje usluga i unificiranje mjesta odakle se usluge pružaju na način da se same usluge odvoje od mreže.

Bitan element IP višemedijskog sustava je kvaliteta usluge koju osiguravaju sloj kontrole sjednice ili kontrolni sloj i sloj kontrole medija ili transportni sloj. Upravljanje kvalitetom usluge s kraja na kraj onemogućuje kašnjenja paketa, pristizanje paketa krivim redoslijedom, gubljenje ili odbacivanje paketa. Korisnički terminalni uređaj pregovara o kapacitetima te time definira QoS zahtjeve tijekom uspostavljanja ili tijekom trajanja veze.

Kao što je spomenuto, IP višemedijski podsustav koristi troslojnu arhitekturu koja se sastoji od transportnog, kontrolnog i aplikacijskog sloja te je grafički prikazana na slici 4.



Slika 4. Prikaz arhitekture IP višemedijskog podsustava, [25]

Transportni sloj zadužen je za SIP (*eng. Session Initiation Protocol*) signalizaciju odnosno uspostavu i prekid sesije. Unutar IP višemedijskog sustava nalaze se čvor SGSN (*eng. Serving GPRS Support Node*) koji je zadužen za podatkovne usluge prema mobilnoj stanici i čvor GGSN (*eng. Gateway GPRS Support Node*) koji služi kao *gateway* prema Internetu ili nekoj drugoj podatkovnoj mreži. MRFP (*eng. Multimedia Resource Function Processor*) zadužen je za osiguranje resursa za multimediju dok IM-MGW (*eng. IP Multimedia – Media Gateway*) omogućuje konvergenciju između mreža temeljenih na komutaciji kanala i mreža temeljenih na komutaciji paketa.

Funkcija kontrolnog sloja je uspostava sesije te njezin nadzor kao i upravljanje nad njome. Unutar ovoga sloja nalazi se CSCF (*eng. Call Session Control Function*) koji je zadužen za registraciju krajnjih korisnika, usmjeravanje SIP poruka odgovarajućem aplikacijskom poslužitelju te autoriziranje kvalitete usluge. Povezan je sa HSS-om te time posjeduje informacije o svim korisnicima te njihovim profilima. Centralizacijom spomenutih informacija aplikacije imaju mogućnost dijeljenja te se na taj način stvaraju jedinstveni profili za sve usluge. Za kontrolu resursa i *mediagatewaya* zaduženi su MGCF (*eng. Media Gateway Control Function*) i MRFC (*eng. Media Resource Function Controller*).

Aplikacijski sloj zadužen je za spremanje raznih aplikacija i sadržaja potrebnih za uslugu. U aplikacijski sloj spadaju podatkovni centri aplikacijskih poslužitelja i web poslužitelji, [14].

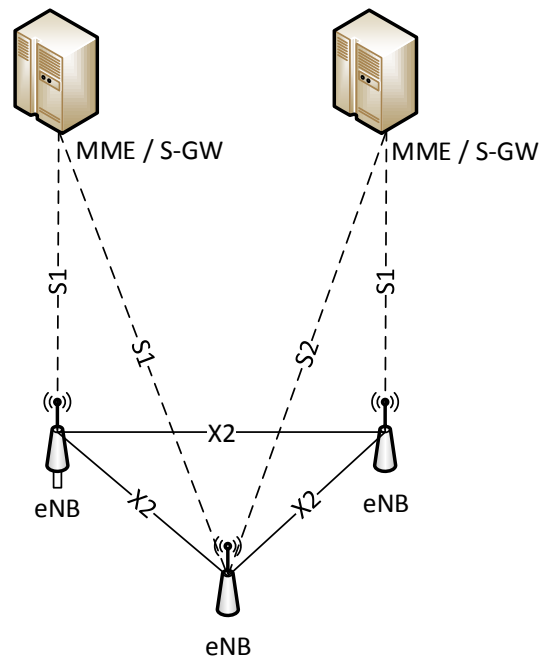
3.3. E-UTRAN pristupna mreža

E-UTRAN (*eng. Evolved UMTS Terrestrial Radio Access Network*) predstavlja nadogradnju radio pristupnog sučelja za mobilne mreže. Ova pristupna mreža namijenjena je kao zamjena za postojeće UMTS, HSDPA (*eng. High Speed Downlink Packet Access*) i HSUPA (*eng. High Speed Downlink Packet Access*) pristupne tehnologije. Omogućuje veće brzine prijenosa podataka i nižu latenciju te je optimizirana isključivo za prijenos informacija unutar IP paketa.

U silaznome smjeru (*eng. downlink*) koristi OFDMA (*eng. Orthogonal Frequency Division Multiple Access*) tehniku višestrukog pristupa. OFDMA tehnika omogućuje većem broju korisniku istovremeno slanje podataka na različitim podnositeljima. U ulaznoj vezi, E-UTRAN koristi višestruki pristup s frekvencijskom raspodjelom na jednom nositelju odnosno SC-FDMA (*eng. Single Carrier Frequency Division Multiple Access*).

E-UTRAN odgovoran je za sve radijski povezane funkcije. Upravljanje radio resursima vezano je za sve funkcije koje se odnose na radio nosioce kao što je kontrola radio nositelja, kontrola radio prijema, kontrola radio mobilnosti te raspoređivanje i raspodjela sredstava za korisničke uređaje. Kompresijom zaglavlja E-UTRAN nastoji učinkovito koristiti radijsko sučelje. Svi podaci koji se prenose putem pristupne mreže moraju biti kriptirani kako bi se zadovoljio sigurnosni aspekt prijenosa podataka. Razmjenom signalizacijskih poruka odnosno signalizacijom sa entitetom upravljanja mobilnošću (MME) te određivanjem puta prema uslužnom prilaznom čvoru (S-GW) E-UTRAN ostvaruje povezanost sa jezgrenom mrežom (EPC).

Arhitektura E-UTRAN-a prikazana slikom 5. sastoji se od čvorova eNodeB koji se povezuje sa korisničkom terminalnom opremom. Cilj pojednostavljena arhitekture pristupnog dijela mreže je smanjenje latencije operacija radio sučelja. eNodeB čvorovi međusobno su povezani putem X2 sučelja dok se eNB (eng. *Evolved Node B*) čvor sa jezgrenom mrežom (EPC) povezuje putem S1 sučelja.



Slika 5. Arhitektura E-UTRAN pristupne mreže

Izvor: 25

S obzirom na prethodno spomenuto neke od funkcionalnosti eNodeB čvorova su sljedeće:

- kontrola radijskih resursa svojih ćelija,
- kontrola mobilnosti odnosno prekapčanja,
- kriptiranje podataka,
- upravljanje resursima dijeljenog kanala,
- adaptacija paketa podataka na veličinu prijenosnog bloka,
- upravljanje retransmisijom podataka,
- automatizirani rad i nadzor, [15].

4. Mobilnost u All-IP mrežama

Popularizacija korištenja Interneta i terminalnih uređaja, kao što su prijenosna računala i pametni telefoni, dovelo je do zahtjeva za mobilnosti i pokretljivosti korisnika na način da korisnici svoje terminalne uređaja mogu prenositi bilo gdje te započinjati novu vezu sa Internetom.

Kako bi terminalni uređaji mogli komunicirati u sklopu Interneta moraju biti jednoznačno identificirani sa IP adresom kako bi se znalo odredište paketa informacija koji su namijenjeni njemu. Pokretljivost terminalnih uređaja dovelo je do problema jer IP protokol ne dopušta da se prvotno dodijeljena IP adresa koristi u drugoj mreži te bi terminalni uređaj prilikom svakog prijelaza u drugu IP mrežu morao zatražiti novu IP adresu u skladu sa mrežom unutar koje se nalazi. Proces promijene IP adrese doveo bi do nepostojanja stalne veze što je u današnjim okvirima pružanja telekomunikacijskih usluga nepoželjno i dovodi do degradiranja kvalitete same usluge.

Kretanjem korisnika mobilni uređaj napušta područje pokrivanja jedne bazne stanice te se mora spojiti na drugu. Proces prekapčanja sa jedne priključne točke na drugu naziva se prekapčanje odnosno *handover*. Postupak prekapčanja može izazvati smanjenje razine kvalitete komunikacije ili pak njezin prekid stoga se proces prekapčanja mora odvijati na način da što manje utječe na kvalitetu komunikacije.

Iz tog razloga javila se potreba za kreiranjem sheme koja omogućuje da su čvorovi stalno dostupni te održavaju stalnu vezu pri prijelazu odnosno *handoveru* između dvije mreže. U svrhu toga kreirani su razni protokoli i mehanizmi za upravljanje mobilnošću kako bi se postupak prekapčanja na drugu priključnu točku obavio uz što manji zastoj u komunikaciji. U daljnjem radu, poseban značaj biti će dan na protokole za upravljanju mobilnošću na mrežnome sloju kao što su to Mobile IP i Proxy Mobile IP protokol.

4.1. Mobilnost i vrste prekapčanja

Proces mobilnosti započinje spajanjem mobilnog uređaja odnosno čvora na lokalnu bežičnu mrežu. Mobilni uređaj povezuje se na lokalnu mrežu kada uđe u područje pokrivanja bežične pristupne točke (*eng. Access point*). Time se ostvaruje povezanost uređaja i pristupne točke na sloju podatkovne veze. Kako bi mobilni uređaj mogao komunicirati izvan svoje lokalne mreže potrebna mu je IP adresa kako bi bila moguća povezanost na mrežnom sloju. Nakon što uređaj jednoznačno bude identificiran pomoću IP adrese moguće je usmjeravanje informacija u IP paketima prema njemu i od njega.

Kretanjem korisnika mobilni uređaj izlazi iz područja pokrivenosti lokalne pristupne točke te otkriva drugu pristupnu točku na koju se može spojiti. Cilj prekapčanja na drugu pristupnu mrežu je da se ne prekida sesija odnosno konekcija prema Internetu.

Kako bi se prekapčanje na drugu pristupnu točku odvio uz što manji utjecaj na kvalitetu usluge, ključno je kvalitetno upravljanje mobilnošću kojom se proces prekapčanja izvodi na način da se ne prekida sesija odnosno komunikacija za što su zaduženi MIP i PMIP protokoli. Mobilnost omogućuje bežičnim i mobilnim podatkovnim mrežama pretragu i lociranje mobilnih uređaja koji žele ostvariti mrežnu komunikaciju, kao i upravljanje mrežnom ili aplikacijskom sesijom prilikom prelaska mobilnog uređaja u područje pokrivanja druge mreže. Upravljanje mobilnošću sastoji se od upravljanja lokacijom i upravljanja prekapčanjem.

Upravljanje lokacijom podrazumijeva prijavu i ažuriranje položaja kako bi se mreži omogućila detekcija trenutne točke pristupa mobilnog uređaja za isporuku paketa informacija. Mobilni uređaj mora periodično obavještavati sustav za ažuriranje relevantne baze podataka sa informacijama o svojoj trenutačnoj lokaciji.

Upravljanje prekapčanjem na drugu pristupnu mrežu omogućuje mreži da održava konekciju mobilnog uređaja sa Internetom usprkos tome što je korisnik u kretanju te mijenja pristupne točke prema Internetu.

Postoje različite vrste prekapčanja kao što su vertikalno i horizontalnoprekapčanje, prekapčanje inicirano od strane mreže ili mobilnog uređaja, prekapčanje kontroliran od strane mreže ili mobilnog uređaja te brzo i besprijekorno prekapčanje.

Horizontalno prekapčanje podrazumijeva prekapčanje između bežičnih pristupnih točaka odnosno baznih stanica iste tehnologije, dok vertikalno prekapčanje podrazumijeva prekapčanje između dvije različite mreže koje koriste različite tehnologije.

Kod prekapčanja iniciranog od strane mobilnog uređaja, mobilni uređaj zadužen je za uspostavu zahtjeva za prekapčanjem, dok kod prekapčanja iniciranog od strane mreže, mreža je zadužena za otkrivanje da se prekapčanje mora izvršiti.

Prekapčanje kontrolirano od strane mobilnog uređaja zahtjeva da mobilni uređaj sudjeluje u procesu. Ukoliko je prekapčanje kontrolirano od strane mreže, mreža je zadužena za čitavi proces prekapčanja na drugu pristupnu točku.

Brzo prekapčanje nastoji smanjiti latenciju prilikom prekapčanja, dok je cilj besprijekornog prekapčanja da se mobilni uređaj prespoji na drugu pristupnu točku bez prekida i gubitka odlazne sesije te bez poremećaja i smetnji u komunikaciji, [16].

4.2. Vrste mobilnosti

Pokretljivost korisnika i mobilnih uređaja podrazumijeva promjenu mjesta pristupa odnosno mjesta priključka. Promjena mjesta priključka mora se odvijati na način da se održi kontinuitet komunikacije bez prekidanja usluge, a sve u svrhu postizanja kontinuirane komunikacije u pokretu.

Mobilnost osoba, mobilnih uređaja, usluga i mreža može se razmatrati kroz različita stajališta. Temeljna podjela mobilnosti je na *micro* i *macro* mobilnost. *Micro* mobilnost predstavlja pokretljivost korisnika između različitih podmreža pod istim vlasništvom, dok se *macro* mobilnost koristi za upravljanje pokretljivošću korisnika između bežičnih mreža pod različitim vlasništvom.

Podjela mobilnosti najčešće se razmatra sa stajališta pokretljivosti entiteta. Sukladno tome, mobilnost se može podijeliti na mobilnost sjednice, mobilnost korisnika i mobilnost terminala. Spomenute vrste mobilnosti entiteta bit će razrađene u poglavljima 4.2.1., 4.2.2. i 4.2.3, [17].

4.2.1. Mobilnost sjednice

Mobilnost sjednice je vrsta mobilnosti koja omogućuje održavanje postojeće sjednice ukoliko korisnik mijenja terminalni uređaj. Na taj način korisniku je omogućen prijem paketa informacija bez ponovne uspostave iste komunikacije odnosno istog toka podataka prilikom promijene terminalnog uređaja za prikaz informacija.

Zahvaljujući mobilnosti sjednice korisnik primjerice može početi pregledavati video odnosno VoD uslugu na svome prijenosnome računalu te nastaviti pregledavanje istog videa na svome pametnom telefonu. Također, korisniku je omogućeno gledanje videa na jednom uređaju dok se zvuk videa projicira na drugom terminalnom uređaju, [17].

4.2.2. Mobilnost osobe

Mobilnost osobe omogućuje korisniku pristup telekomunikacijskim uslugama putem bilo kojeg terminalnog uređaja na temelju svog profila koji predstavlja njegov jedinstveni identifikator. Telekomunikacijska mreža, putem koje korisnik želi pristupiti usluzi, mora biti u mogućnosti identificirati korisnika kako bi korisnik bio poslužen sa odgovarajućim tokom podataka.

Korisnik tako može nastaviti koristiti uslugu na nekom drugom terminalnom uređaju bez ponovno unosa svojih korisničkih podataka. Na taj način, korisniku je omogućena pokretljivost prilikom koje uopće ne osjeća prekid korištenja usluge. Postoje mnoge usluge koje korisnik želi kontinuirano koristiti bez učestale identifikacije. Primjer takvih usluga su sveprisutne društvene usluge, kao što su to Facebook i usluge stvarnovremenskog dopisivanja, te usluge maila i slične aplikacije, [17].

4.2.3. Mobilnost terminalnog uređaja

Mobilnost terminalnog uređaja predstavlja sposobnost uređaja da pristupi i koristi telekomunikacijsku uslugu sa različitih lokacija. Telekomunikacijska mreža mora biti u mogućnosti identificirati i locirati terminalni uređaj u pokretu. Ova vrsta mobilnosti omogućuje neprekidnu komunikaciju usprkos kretnji mobilnog uređaja na način da se ne prekida tok podataka prilikom promijene točke priključka odnosno *handovera*.

Kako bi se održao kontinuitet komunikacije prilikom kretnje mobilnog uređaja odnosno njegove mobilnosti vrlo je bitan uspješan proces prekapčanja na drugu pristupnu mrežu. Prekapčanje se mora izvesti na način da se mobilni uređaj priključi na drugu priključnu točku bez prekida ili smanjenja kvalitete usluge, [17].

4. 3. Utjecaj mobilnosti na kvalitetu usluge

Mobilnost između mreža koje koriste istu ili različitu tehnologiju izaziva određeni utjecaj na kvalitetu same usluge. Iz tog razloga, pored nastojanja da se smanji vrijeme nepostojanja usluge prilikom prekapčanja, posebnu pažnju treba obratiti i na utjecaj mobilnosti na samu kvalitetu usluge.

Prilikom svakog spajanja na točku priključka, bilo da se radi o inicijalnom pristupu ili obnavljanju pristupa uzrokovanog pokretljivošću, korisnik i njegov mobilni uređaj moraju proći kroz nekoliko koraka. Prvi korak je zasigurno izvršavanje sigurnosnih procedura oko korisničkog profila kako bi se korisniku omogućio ili odbio pristup novoj mreži. Paralelno s time, korisnik mora čekati izvršenje signalizacijskih procedura čija je zadaća uspostava sesije.

Sve navedeno dovodi do kašnjenja koje je uzrokovano identifikacijom i provjerom korisnika, uspostavom sjednice kao i prekidom usluge prilikom prekapčanja na drugu priključnu točku. Pokretljivošću korisnika kojom stalno mijenja točke priključka, povećava se i mrežni promet kojeg generiraju sigurnosne i signalizacijske procedure odnosno njihova razmjena informacija. Povećanjem upravljačkog mrežnog prometa dolazi i do povećanja zagušenja na mreži koje izaziva određeni utjecaj na kvalitetu i pouzdanost same usluge. Zagušenje mreže može dovesti do nemogućnosti uspostave nove sesije te se postupak mora iznova započeti. Posljedica toga je nemogućnost ostvarenja kontinuiteta usluge što je primarni cilj procedura vezanih uz mobilnost korisnika, [17].

Nadziranje sigurnosti korisnika prilikom prekapčanja odvija se kako bi se zaštitio integritet korisnika te kako bi se ostvarila pouzdanost komunikacije. U tu svrhu pristupni čvor obavlja proces autorizacije i autentikacije korisnika koji se izvršava na transportnome sloju. Spomenute sigurnosne procedure uzrokuju pojavu dodatnog mrežnog prometa i povećanja trajanja prekida prilikom prekapčanja što zasigurno ima utjecaj na razinu kvalitete usluge. Kako bi se utjecaj sigurnosnih procedura na kvalitetu usluge smanjio, koriste se mehanizmi koji se temelje na IPSec protokolu (*eng. Internet Protocol Security*).

Preuzimanje točke priključka najbitniji je faktor osiguranja trenutne razine kvalitete usluge. Upravljanje mobilnošću najčešće se odvija na mrežnome sloju, iako svi slojevi međusobno surađuju kako bi se smanjilo vrijeme prekida usluge. Za upravljanje mobilnošću na mrežnome sloju zaduženi su MIP protokol i PMIP protokol. Spomenuti protokoli imaju svoje verzije, a to su MIPv4, MIPv6, PMIPv4 i PMIPv6 protokoli za upravljanje mobilnošću na mrežnome sloju. Navedeni protokoli funkcioniraju na principu dodjeljivanja nove IP adrese domaćoj mreži kako bi se zadržao kontinuitet komunikacije. Za upravljanje pokretljivošću na aplikacijskom sloju zadužen je SIP protokol koji omogućuje kraće vrijeme potrebno za preuzimanje nove točke priključka, a samim time i održavanje kontinuiteta zadovoljavajuće razine usluge.

Značajan utjecaj na razinu kvalitete usluge ima i obnavljanje signalizacijskih procedura prilikom preuzimanja točke priključka. Kako bi se uspostavila sesija potrebna je upotreba signalizacijskih protokola koji su zaduženi za pregovaranje o parametrima sesije kao i za uspostavu iste. Pokretljivošću korisnika povećava se mrežni promet kojeg generiraju signalizacijske informacije što dovodi do zagušenja na mreži, gubitka paketa i na kraju prekida usluge. Iz tog razloga potrebno je optimizirati procese obnavljanja sesije kako bi se izbjegli navedeni problemi te se povećala kvaliteta usluge, [18].

5. IP protokol za podršku mobilnosti korisnika

Povećana uporaba mobilnih uređaja i pojava mnogih usluga baziranih na konstantnoj povezanosti i kretanju uređaja, dovela je do potrebe za održavanjem konstantne povezanosti sa Internetom. Implementacija mehanizama i protokola koji omogućuju pokretljivost uređaja uz kontinuiranu povezanost najjednostavnija je na mrežnom sloju.

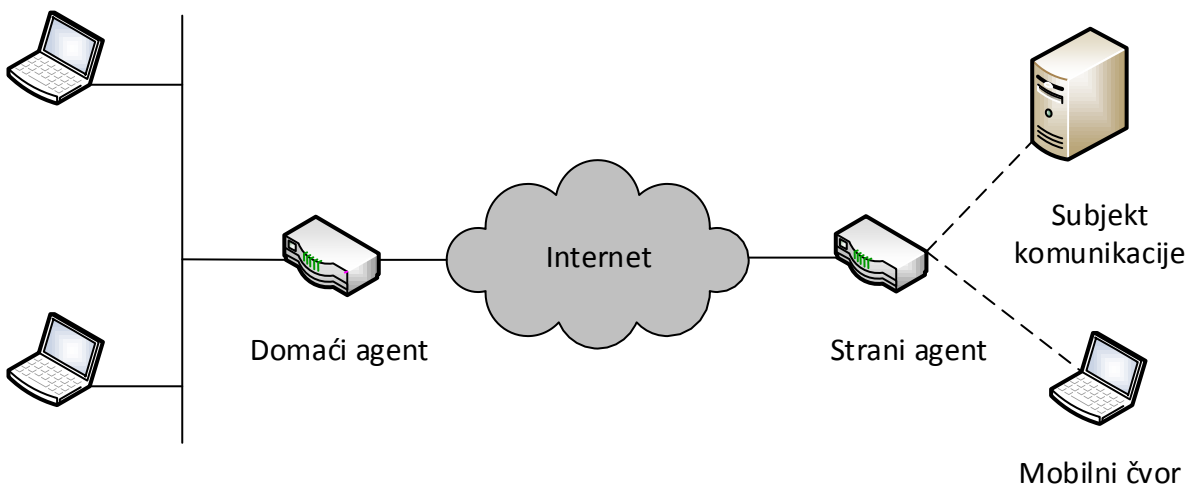
Najveći izazov realizacije takovog rješenja je održavanje iste IP adrese tijekom cijele komunikacije iz razloga što je TCP/IP struktura izgrađena isključivo za komunikaciju stacioniranih subjekata. Kretanjem korisnik napušta područje prekrivanja prvotne bazne stanice odnosno podmreže te prelazi u područje druge podmreže. Promjenom mreže mijenja se i IP adresa koja mu se dodjeljuje uzrokujući prekide komunikacije prilikom prekapčanja. Kako bi se omogućila kontinuirana povezanost i komunikacija pojavila se potreba za mehanizmom i protokolom koji će upravljati mobilnošću korisnika na način da se održava prvotna IP adresa dodijeljena od strane polazne odnosno domaće mreže.

IP protokol za upravljanje mobilnošću predstavlja jedno od rješenja spomenutog problema. MIP protokol ima dvije verzije ovisno o mrežama unutar kojih funkcionira, a to su MIPv4 protokol za mreže bazirane na IPv4 adresama i MIPv6 protokol za mreže bazirane na IPv6 adresama. MIP protokol omogućuje mobilnim uređajima korištenje dvije IP adrese i to jednu za identifikaciju te jednu za usmjeravanje.

Upravljanje i omogućavanje mobilnosti uređaja MIP postiže seizvođenjem tri procesa, a to su otkrivanje agenta kojem pripada, registracija mobilnog uređaja odnosno čvora te tuneliranja kojim se paketi prosljeđuju odgovarajućem subjektu komunikacije. Spomenuti procesi biti će razrađeni u poglavljima 5.2., 5.3. i 5.4, [19].

5.1. Funkcionalne komponente MIP protokola

U svome djelovanju Mobile IP protokol koristi razne komponente, kako bi ostvario svoju funkcionalnost, kao što su mobilni čvor, domaći i strani agent, domaća i strana mreža te mobilni agent.



Slika 6. Prikaz funkcionalnih komponenata MIP protokola

Izvor: [19]

Mobilni čvor predstavlja mobilni uređaj ili *ruter* koji mijenja točku priključka sa jedne podmreže na drugu ili na novu mrežu bez promijene svoje IP adrese. Na taj način mobilnom čvoru je omogućena kontinuirana komunikacija sa drugim mrežnim priključcima bez promijene IP adrese. Izvjestiteljski čvor je čvor s kojim komunicira mobilni čvor, a može biti stacionirani ili pak mobilni.

Domaći agent predstavlja *ruter* na mobilnom čvoru koji se nalazi u domaćoj mreži koji dostavlja IP pakete odnosno datagrame udaljenim mobilnim čvorovima. Strani agent je *ruter* koji se nalazi na stranoj mreži te surađuje sa domaćim agentom odnosno *ruterom* kako bi se isporučili odgovarajući IP datagrami. Strani agent ujedno šalje specijalne poruke odnosno pakete kako bi potvrdio svoju prisutnost.

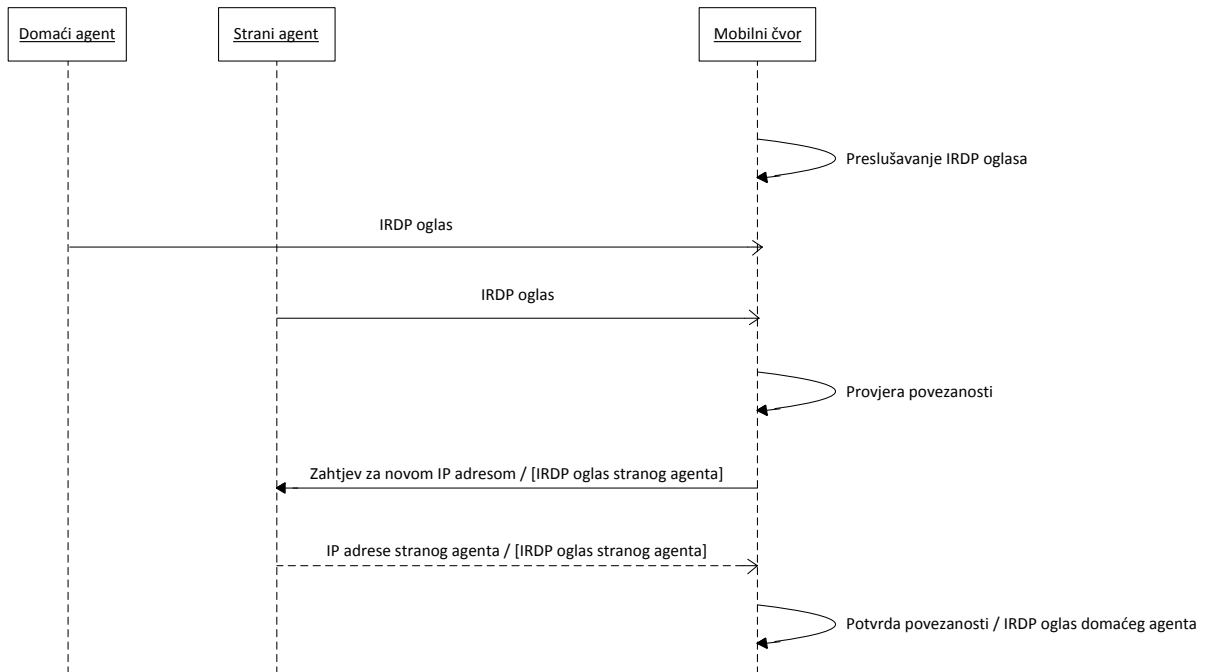
Domaća mreža je mreža koja ima identičan prefiks IP adrese kao i mobilni uređaj odnosno mobilni čvor koji se nalazi unutar te mreže. Domaća adresa je IP adresa koja je dodijeljena iz domaće mreže mobilnom čvoru. Strana mreža predstavlja sve mreže s kojima mobilni čvor komunicira, a da nisu domaća mreža, [19].

5.2. Otkrivanje agenta

Prva faza procesa kod MIP-aje otkrivanje agenta prikazana dijagramom 1. Unutar procesa otkrivanja agenta domaći i strani agent oglašavaju svoje usluge na mreži uz pomoć IRDP (*eng. ICMP Router Discovery Protocol*) protokola. Mobilni čvor sluša oglašavanja domaćeg i stranog agenta kako bi odredio da li je spojen sa domaćom ili stranom mrežom.

IRDP oglas sadrži MIP ekstenziju koja definira da li je agent domaći ili strani. Zadužen je za IP adrese, vrste usluga koje pruža kao što su obrnuto tuneliranje i generička usmjernička enkapsulacija te je zadužen za dozvoljeno vrijeme registracije ili vrijeme priključka na stranu mrežusa strane mobilne čvorove. Mobilni čvor može poslati poruku iščekivanja agentu kako ne bi trebao čekati oglašavanje agenta. Poruka iščekivanja prisiljava svakog agenta da pošalje poruku oglašavanja kako bi odredio na koju je mrežu spojen.

Kada mobilni čvor utvrdi da je spojen na stranu mrežu, on preuzima brigu o IP adresi. Adresa koja je ustupljena mobilnom čvoru je IP adresa stranog agenta čije se sučelje nalazi na stranoj mreži na koje se povezao mobilni čvor. Postoje dvije vrste takvih adresa, a to su adresa dobivena od strane stranog agenta i kolocirana adresa. Adresa dobivena od strane stranog agenta mogu koristiti i drugi mobilni čvorovi, dok se kolociranom adresom koristi jedan mobilni čvor. Kada mobilni čvor primi oglašavanje stranog agenta i razazna da je izašao iz područja pokrivanja domaće mreže, započinje proces registracije, [20].



Dijagram 1. Otkrivanje agenta u sklopu MIP procesa

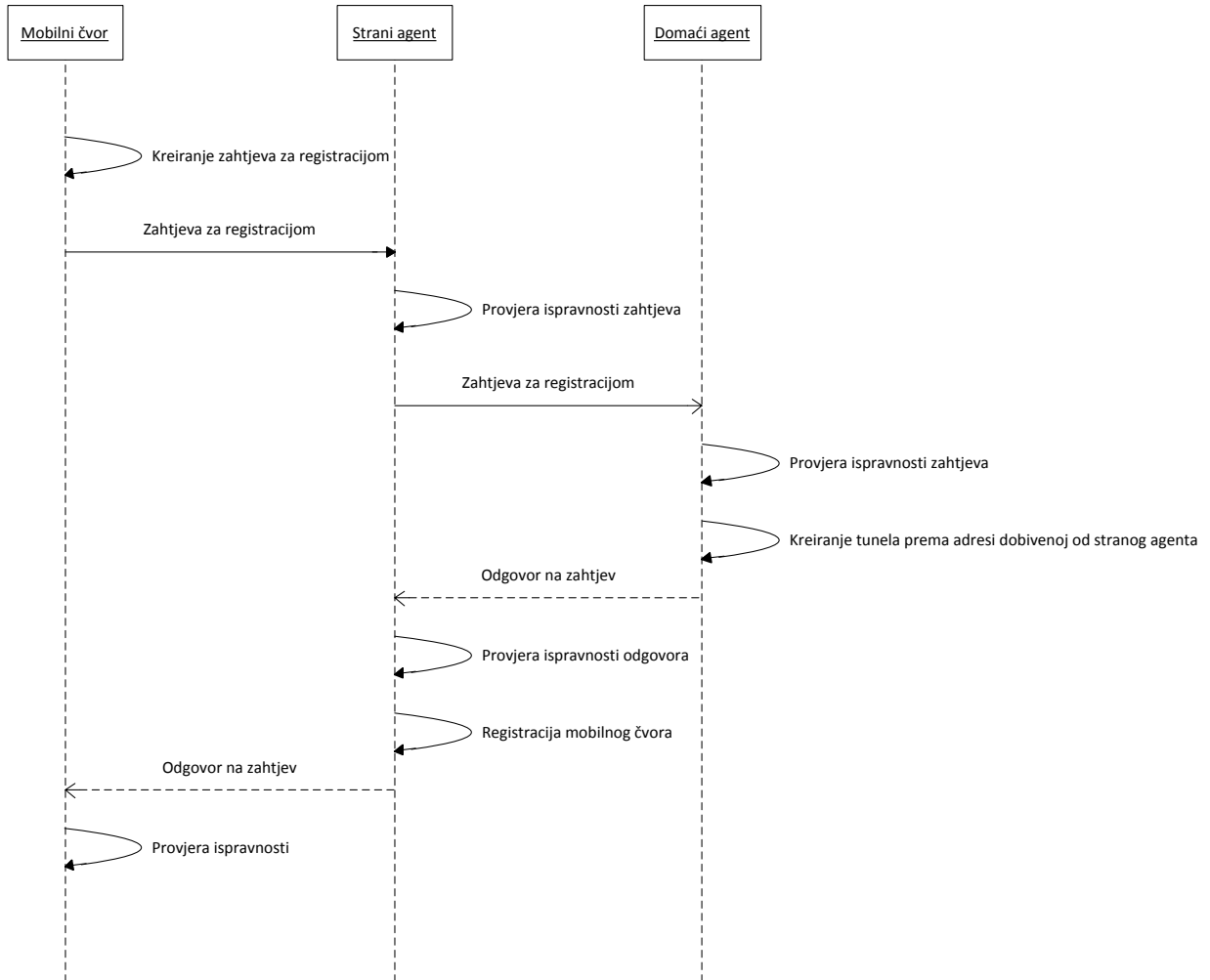
5.3. Registracijamobilnog čvora

Svaki mobilni čvor jednoznačno je identificiran sa svojom IP adresom te ju koristi zajedno sa informacijom koju je dobio od stranog agenta kako bi kreiraoMIP registracijski zahtjev prema unaprijed definiranim koracima koji su prikazani dijagramom 2. Kreirani zahtjev stavlja na svoju listu čekanja te zahtjev za registracijom šalje domaćem agentu bilo posredstvom stranog agenta, ukoliko se radi o kolociranoj adresi, ili direktno ukoliko više mobilnih čvorova koristi istu adresu. Ukoliko je zahtjev poslan posredstvom stranog agenta, on provjerava ispravnost zahtjeva te nakon toga stavlja gostujući mobilni čvor na svoju listu čekanja prije nego zahtjev za registracijom proslijedi domaćem agentu.

Domaći agent također izvršava provjeru ispravnosti zahtjeva za registracijom. Ukoliko je ispravan, kreira tunel prema adresi dodijeljenoj od strane stranog agenta te upisuje usmjerivačke funkcije za prosljeđivanje paketa prema domaćoj IP adresi kroz prethodno kreirani tunel. Zatim domaći agent šalje odgovor na zahtjev putem stranog agenta ili direktno mobilnom čvoru.

Strani agent potom provjerava ispravnost odgovora na zahtjev za registracijom. Ukoliko je ispravan, strani agent stavlja mobilni čvor na listu posjetitelja, unosi podatke za usmjeravanje kako bi se paketi mogli prosljeđivati prema domaćoj adresite prosljeđuje odgovor na zahtjev mobilnom čvoru.

Mobilni čvor također provjerava ispravnost odgovora te ukoliko je ispravan, proces registracije je uspješno izvršen. Mobilni čvor obavlja ponovnu registraciju prije nego istekne vrijeme registracije, a u sklopu procesa ponovne registracije domaći i strani agent ažuriraju svoju vezu za mobilnost i unose u listu posjetitelja, [20].



Dijagram 2. Registracija mobilnog čvora unutar MIP procesa

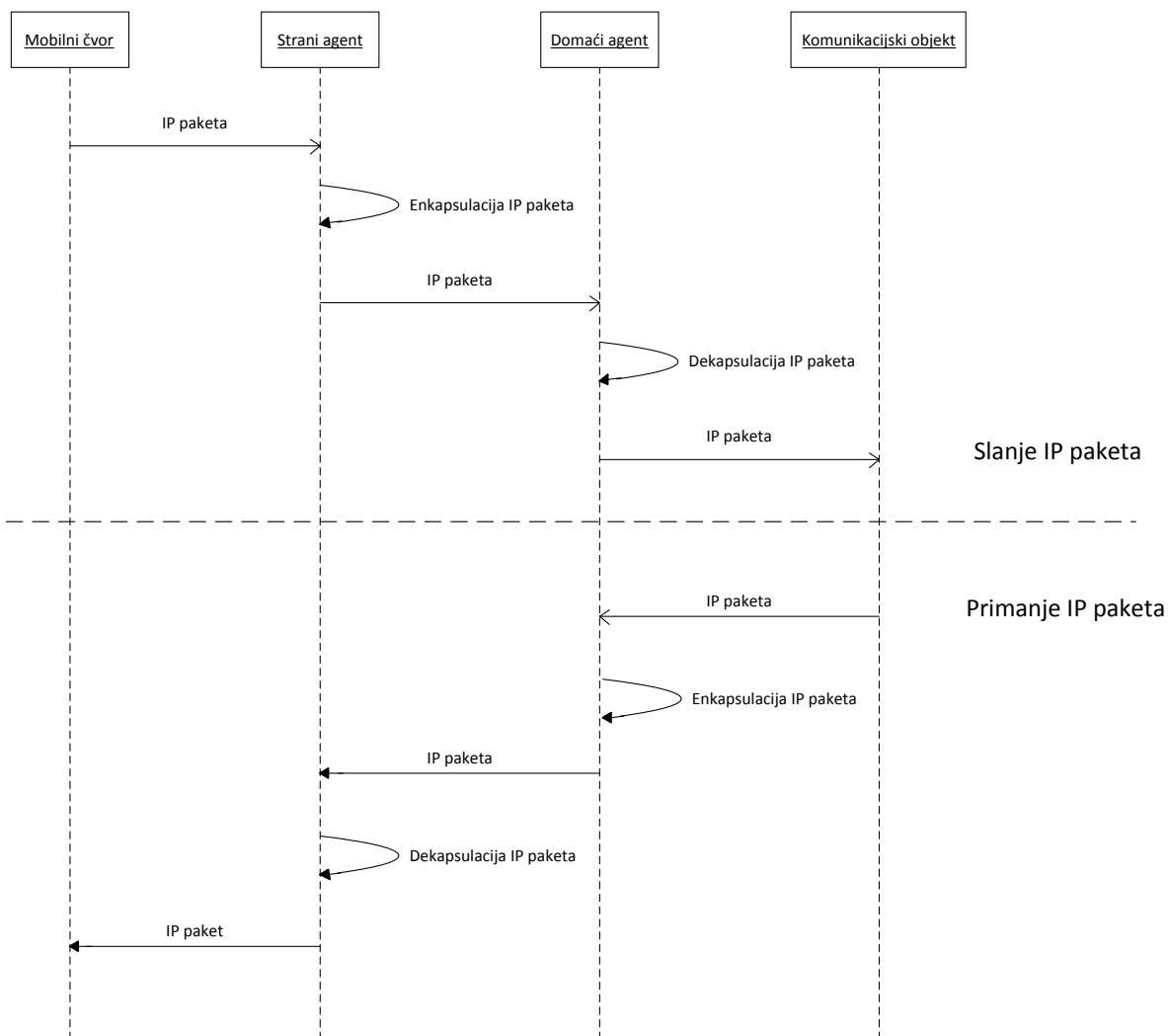
5.4. Tuneliranje

Tuneliranje je proces kojim se paketi informacija enkapsuliraju unutar novog paketa kako bi se omogućilo slanje i primanje paketa između čvorova koji se nalaze unutar druge mreže odnosno koji imaju različite prefikse IP adrese. Proces tuneliranja, prikazan dijagramom 3., odvija se između domaćeg i stranog agenta kako bi se omogućila komunikacija uređajima u pokretu.

Mobilni čvor prima pakete podatka koristeći svoju domaću IP adresu koju je dobio od domaće mreže čime se postiže dojam da se uvijek nalazi unutar svoje mreže. Ukoliko se korisnik kreće te se nalazi na području pokrivanja strane mreže njegove kretnje su poznate mobilnom ili stacionarnom čvoru s kojim komunicira.

Paketi podataka namijenjeni terminalnom uređaju odnosno mobilnom čvoru usmjeravaju se prema domaćoj mreži gdje je domaći agent zadužen za tuneliranje paketa prema adresi dobivenoj od strane stranog agenta odnosno strane mreže. U sklopu procesa tuneliranja obavlja se enkapsulacija i dekapulacija paketa. Paketi podataka na izvorišnoj strani se enkapsuliraju kako bi se mogli dostaviti mobilnom čvoru. Na odredišnoj strani, prilikom pristizanja paketa, obavlja se proces njihove dekapulacije.

Slanje paketa mobilni čvor obavlja uz pomoć stranog agenta koji pakete usmjerava do njihove destinacije. Mobilni čvor prilikom slanja paketa informacija šalje prvo prema stranom agentu. Strani agent primljene pakete prosljeđuje prema domaćem agentu na domaćoj mreži. Čvor s kojim terminalni uređaj korisnika komunicira prima paketizirane informacije od domaćeg agenta i time proces slanja odnosno tuneliranja podataka završava. Ovakav način slanja paketa naziva se reverzno tuneliranje, [20].



Dijagram 3. Tuneliranje IP paketa u sklopu Mobile IP procesa

6. Proxy IP protokol za podršku mobilnosti korisnika

Mobile IP protokol omogućuje i upravlja mobilnošću korisnika i njegovog terminalnog uređaja međutim sami protokol ima određene nedostatke. Mobilni čvor mora koristiti specijalizirani mobilni IP klijentski softver koji je nužan za komunikaciju sa drugim subjektima unutar Mobile IP konfiguracije kao što su domaći i strani agent. Implementacija spomenutog softver sa sobom povlači dodatna financijska ulaganja kao i povećanu količinu procesa implementacije i konfiguracije na subjektima Mobile IP protokola.

Proxy Mobile IP protokol podržava Mobile IP bez potrebe za implementacijom specijaliziranog softvera. Bežična pristupna mreža ponaša se kao *proxy* bežičnih klijenata koji nisu svjesni da prelaze u drugu mrežu. Pristupna točka upravlja IRDP komunikacijom sa stranim agentom i upravlja procesom registracije na domaćeg agenta. PMIP mehanizam sa sobom povlači manje troškove, manju potrebu za administracijom i konfiguracijom, a samim time omogućuje bržu implementaciju rješenja za mobilnost terminalnih uređaja.

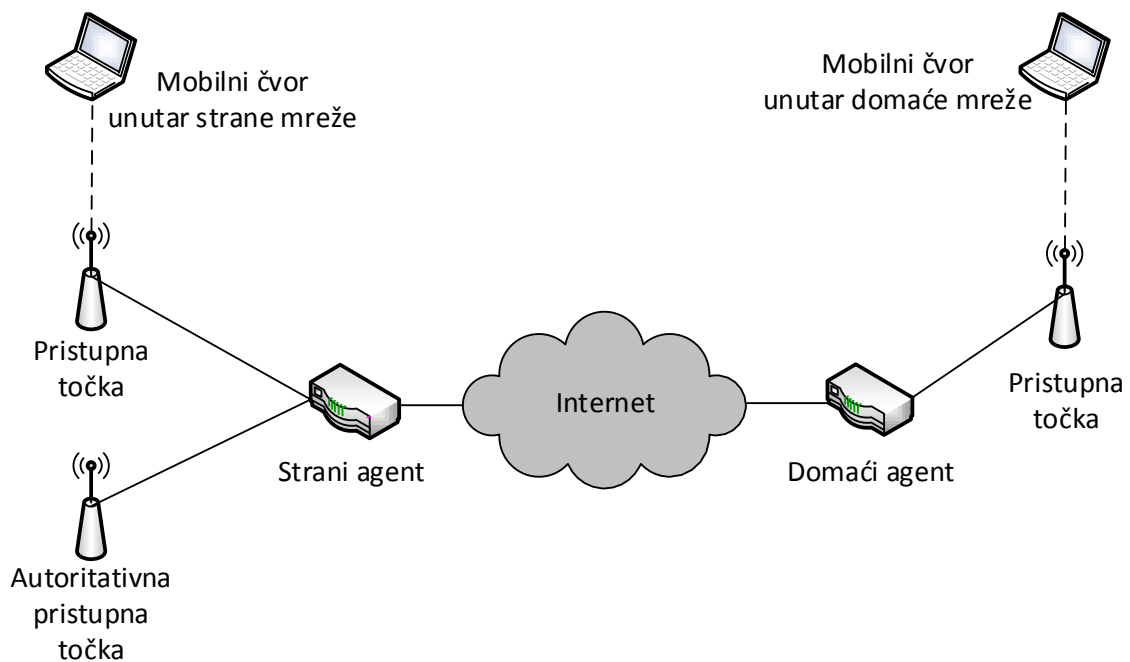
PMIP protokol za mobilnost u svome funkcioniranju obavlja četiri procesa, a to su:

- otkrivanje agenta,
- ažuriranje tablice podmreže,
- registracija mobilnog terminalnog uređaja,
- tuneliranje paketa prema odredištu.

6.1. Funkcionalne komponente PMIP protokola

Unutar mreža sa Proxy Mobile IP protokolom za upravljanje mobilnošću funkcioniraju pet uređaja koji su prikazani na slici 7., a to su:

- korisnički uređaj,
- pristupna točka,
- autoritativna pristupna točka,
- domaći agent,
- strani agent.



Slika 7. Funkcionalne komponente Proxy Mobile IP mreže

Izvor: [21]

Korisnički uređaj unutar PMIP mreže je svaki terminalni uređaj koji ima mogućnost mobilnosti kao što su to pametni telefoni i prijenosna računala. Specificirani mobilni uređaji ne trebaju poseban softver kako bi ostvarili sve prednosti PMIP protokola kao što je to slučaj prilikom korištenja MIP protokola.

Pristupna točka predstavlja entitet koji funkcionira u korist gostujućeg mobilnog uređaja u svrhu ostvarenja svih prednosti Mobile IP mehanizma. Pristupna točka koristi kartu podmreže kako bi pratila obavijesti domaćeg agenta. Od autoritativnih pristupnih točaka prikuplja informacije o novim domaćim agentima.

Autoritativna pristupna točka je pristupna točka zadužena za prikupljanje informacija o domaćim agentima koje su pohranjene u karti podmreže unutar koje se nalazi. Nakon što prikupi potrebne informacije, prosljeđuje ih ostalim pristupnim točkama za sve gostujuće mobilne uređaje.

Domaći agent je usmjeritelj na domaćoj mreži mobilnog čvora koji služi kao sabirna točka za komunikaciju sa pristupnom točkom i gostujućim mobilnim čvorom. Domaći paket tunelira paket između dva čvora koja komuniciraju uz pomoć stranog agenta.

Strani agent je usmjeritelj na stranoj mreži koji služi kao točka pristupa gostujućem uređaju kada se nalazi izvan svoje mreže. Zadužen je za usmjeravanje paketa od domaćeg agenta do gostujućeg uređaja.

IRDP protokol zadužen je za otkrivanje agenata uz uvjet da je omogućen na domaćem i stranom agentu, i to na sučelju usmjerivača na pristupnoj točki na koju je povezan. IRDP protokol omogućuje pristupnoj točki identifikaciju usluga koje nude lokalni Mobile IP subjekti te posjeduje informacije za registraciju mobilnog čvora na pristupnu točku.

Svaka pristupna točka na mreži mora biti dizajnirana kao autoritativna pristupna točka odnosno AAP (*eng. Authoritative Access Point*). Na taj način svaka pristupna točka obavještava sve ostale pristupne točke o mrežama koje imaju svoje mobilne čvorove povezane na nju. Nakon što je otkriven strani agent te su prikupljene sve informacije o mrežama koje su spojene na nju, pristupna točka je u stanju pružiti usluge mobilnom čvoru koji je ušao u njezino područje pokrivanja uslugom.

Domaći agent provjerava identitet mobilnog čvora bilo kroz svoje lokalne sigurnosne mehanizme ili pak kroz AAA (*eng. Authentication Authorization and Accounting*) server. Ukoliko je mobilni čvor valjan, domaći agent povezuje mobilni čvor sa stranim agentom odnosno sa IP adresom dobivenom od njega te na taj način kreira tunel za slanje paketa informacija između domaćeg i stranog agenta. Time se omogućuje usmjeravanje paketa od domaćeg do stranog agenta, od stranog agenta do priključne točke te od priključne točke sve do mobilnog čvora. Mobilni čvor ima mogućnost direktnog slanja IP paketa čvoru sa kojim komunicira, [21].

6.2. Otkrivanje agenta

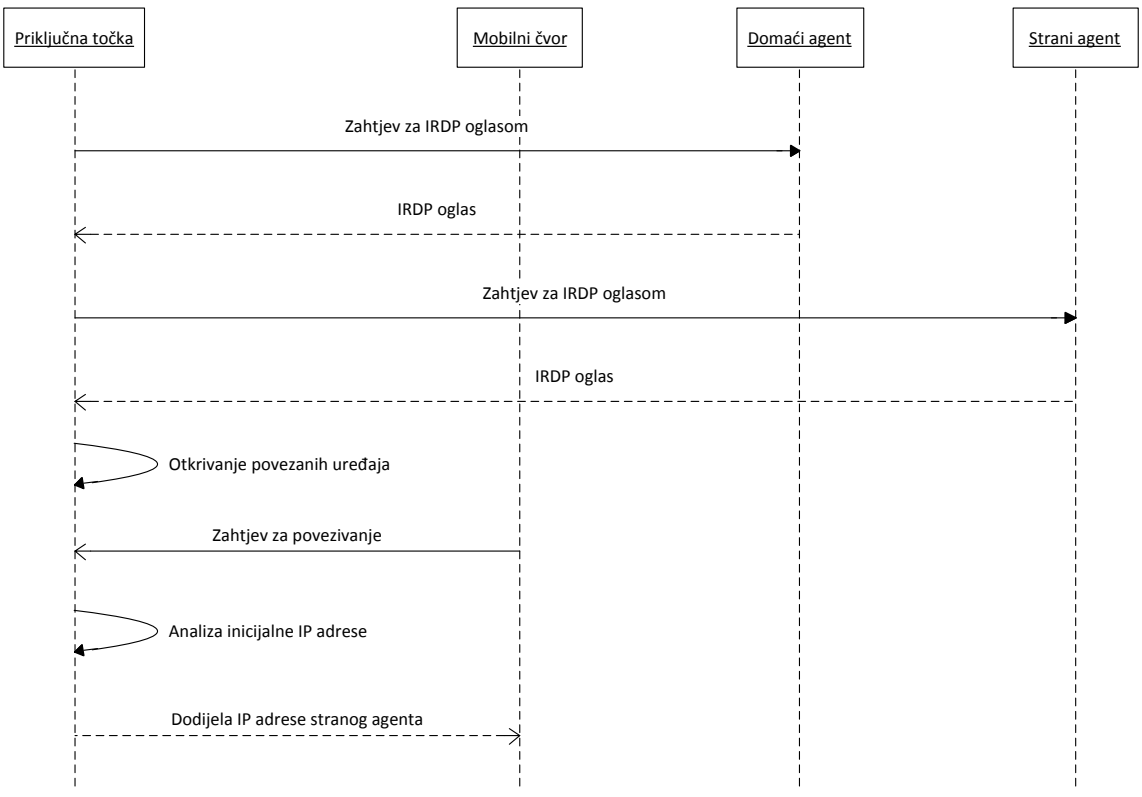
Proces otkrivanja agenta u sklopu Proxy Mobile IP protokola za mobilnost korisnika sličan je kao i kod Mobile IP protokola te je prikazan dijagramom 4. Domaći i strani agent oglašavaju svoju prisutnost i funkcije na mrežu koristeći IRDP protokol.

Unutar spomenutog oglašavanja agenata nalazi se mobilna IP ekstenzija koja definira da li je riječ o domaćem, stranom ili univerzalnom agentu koji se ponaša i kao domaći i strani agent. Oglas agenata također sadrži vrstu usluge koju nude na mreži, dozvoljen period registracije te maksimalno vrijeme *roaminga* za gostujuće mobilne uređaje.

Pristupna točka ima mogućnost slanja zahtjeva za oglašavanjem kojim se agente prisiljava da automatski šalju svoj oglas na mrežu umjesto da na njega čekaju.

Kada priključna točka prepozna strani mobilni uređaj unutar svoje mreže, dodjeljuje mu adresu. Dodijeljena adresa je IP adresa stranog agenta koji ima sučelje spojeno na mrežu unutar koje se trenutno nalazi mobilni uređaj korisnika. Priključna točka dodijeljenu IP adresu može dodjeljivati i drugim uređajima iz razloga što nije jednoznačno dodijeljena jednome uređaju.

Kada se gostujući mobilni uređaj spoji na priključnu točku unutar strane mreže, priključna točka vrši provjeru i komparaciju IP adrese mobilnog uređaja i mrežnih informacija o svojoj podmreži. Analizom priključna točka utvrđuje da je riječ o mobilnom uređaju iz druge mreže. Tom spoznajom, priključna točka započinje proces registracije gostujućeg korisničkog uređaja. Za proces registracije potrebna je IP adresa domaćeg agenta gostujućeg uređaja koju priključna točka iščitava iz tablice podmreže, [21].



Dijagram 4. Otkrivanje agenta u sklopu Proxy Mobile IP procesa

6.3. Ažuriranje tablice podmreže

Svaka pristupna točka unutar PMIP segmenta zadužena je za održavanje tablice podmreže. Tablica podmreže sadrži IP adrese svih domaćih agenata unutar mreža koje podržavaju PMIP protokol.

Tablicu podmreže pristupne točke koriste kako bi utvrdile IP adresu domaćih agenata gostujućih mobilnih uređaja. Pristupna točka saznaje adresu domaćeg agenta prilikom inicijalnog paljenja ili prilikom omogućavanja PMIP protokola unutar svoje podmreže.

Informaciju o domaćem agentu dostavlja autoritativnoj pristupnoj točki koja je zadužena za prosljeđivanje te informacije svim ostalim pristupnim točkama unutar PMIP segmenta. Moguće je konfigurirati do tri autoritativne pristupne točke unutar lokalne odnosno LAN (*eng. Local Area Network*) mreže.

U trenutku spajanja gostujućeg mobilnog uređaja, priključna točka ustvrđuje da je riječ o mobilnom uređaju koji dolazi iz druge podmreže. Priključna točka pretražuje svoju tablicu podmreže te traži IP adresu koja se najviše podudara sa izvornom IP adresom gostujućeg uređaja. Spoznajom IP adrese domaćeg agenta gostujućeg uređaja, može započeti proces njegove registracije, [21].

6.4. Registracija mobilnog uređaja

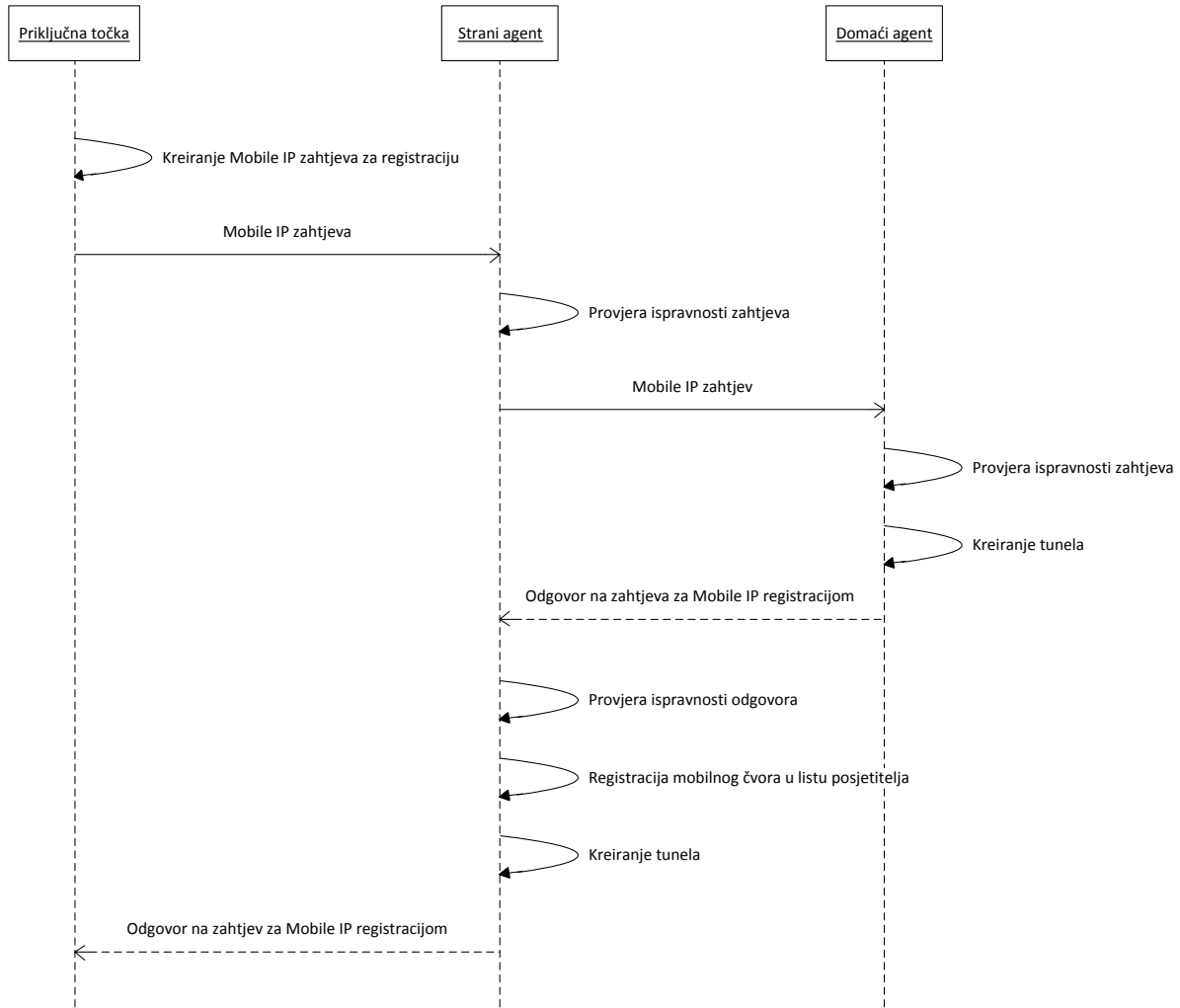
Pristupna točka na domaćoj mreži obavlja proces registracije mobilnih uređaja, prikazanog dijagramom 5., prilikom njihova inicijalnog pojavljivanja unutar njezinog područja prekrivanja. Mobilni uređaj registrira se sa informacijama o njegovoj IP adresi i njegovom domaćem agentu te sigurnosnim informacijama potrebnih za autorizaciju i autentikaciju.

Pristupna točka u stranoj mreži, unutar čijeg područja prekrivanja mobilni uređaj ulazi, koristi sigurnosne informacije, IP adresu gostujućeg mobilnog uređaja te informacije prikupljene od strane stranog agenta prilikom njegovog oglašavanja na mrežu kako bi kreirala MIP registracijski zahtjev. Spomenuti registracijski zahtjev, pristupna točka šalje domaćem agentu uređaja posredstvom stranog agenta. Prije slanja zahtjeva, strani agent obavlja njegovu provjeru te ga prosljeđuje domaćem agentu ukoliko je ispravno kreiran.

Domaći agent također obavlja provjeru zahtjeva kao i strani agent. Ukoliko je zahtjev za registracijom ispravan, domaći agent kreira mobilnu vezu i tunel do IP adrese dodijeljene mobilnom uređaju od strane stranog agenta. Unosi usmjerivačke informacije koje su potrebne za prosljeđivanje IP paketa prema domaćoj adresi uređaja kroz prethodno kreirani tunel.

Domaći agent odgovara na zahtjev za registracijom pristupnoj točki posredstvom stranog agenta koji usputno obavlja verifikaciju odgovora. Ukoliko je ispravan, strani agent dodaje mobilni uređaj u listu gostujućih uređaja te upisuje usmjerivačke informacije za prosljeđivanje paketa prema domaćoj mreži.

Nakon procesa koje su obavili domaći i strani agent, pristupna točka je u mogućnosti ustvrditi da su agenti svjesni mobilnog uređaja koji je u pokretu. Pristupna točka presreće sve pakete od gostujućeg uređaja te ih prosljeđuje stranom agentu. Proces registracije time je kompletiran te je ostvarena veza koja omogućuje komunikaciju uređaju prilikom kretanja, [21].



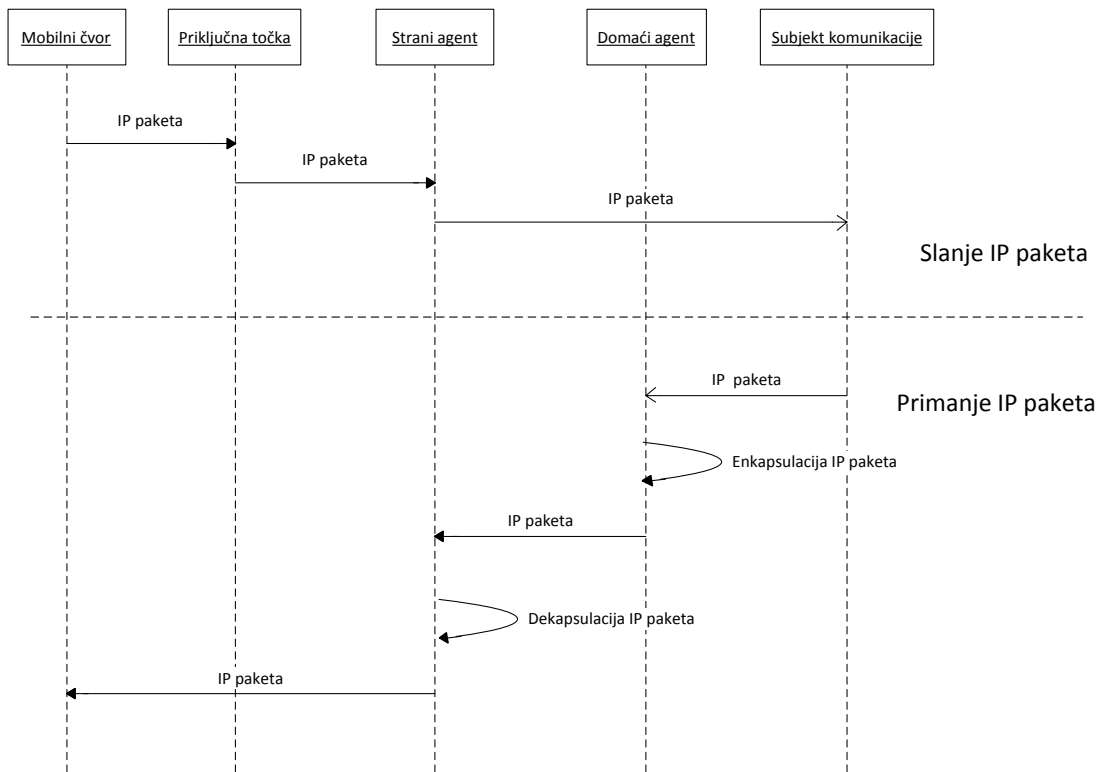
Dijagram 5. Registracija mobilnog uređaja u sklopu Proxy Mobile IP procesa

6.5. Tuneliranje

Mobilni uređaj koji se nalazi unutar strane mreže šalje pakete informacija koristeći svoju inicijalnu IP adresu dobivenu od domaće mreže, čime se postiže dojam da se cijelo vrijeme tijekom konverzacije nalazi stacioniran unutar domaće mreže. Kretanje mobilnog uređaja i njegov prijelaz između stranih mreža cijelo vrijeme su poznate segmentu s kojim komunicira.

Paketi informacija namijenjeni gostujućem mobilnom uređaju, usmjeravaju se prema njegovoj domaćoj mreži gdje je domaći agent zadužen za njihovo presretanje i usmjeravanje odnosno tuneliranje prema adresi koju je mobilni uređaj dobio od strane mreže. Unutar procesa tuneliranja obavlja se enkapsulacija paketa prilikom njihova slanja te njihova dekapulacija prilikom njihovog pristizanja na odredište.

IP paketi koje mobilni uređaj šalje drugome segmentu komunikacije, pristupna točka presreće te ih prosljeđuje stranom agentu. Strani agent zadužen je za njihovo usmjeravanje prema drugom segmentu komunikacije odnosno usmjerava IP pakete prema njihovom odredištu, [21].



Dijagram 6. Tuneliranje IP paketa u sklopu Proxy Mobile IP procesa

6. Zaključak

Korisnički zahtjevi za mobilnošću te kontinuiranom povezanošću i korištenju inovativnih naprednih usluga kreirali su potrebu za razvojem mehanizama i protokola koji su u mogućnosti ostvariti visoke korisničke zahtjeve.

All-IP mreža omogućuje korisnicima pristup uslugama neovisno o pristupnim tehnologijama i mrežama koje koriste za komunikaciju. Time konvergirani koncept korisnicima osigurava kontinuiranu povezanost na servise i usluge sa gotovo svih lokacija, međutim omogućavanje komunikacije prilikom kretanja korisnika nije izvršeno.

Protokoli za upravljanje mobilnošću, kao što su to MIP i PMIP protokol, korisnicima omogućuju kontinuiranu komunikaciju, i u trenucima njihovog kretanja.

Mobile IP protokol predstavlja prvo rješenje takovih zahtjeva koristeći dvije IP adrese. IP adresa, koja je mobilnom čvoru dodijeljena prilikom inicijalnog povezivanja na mrežu od strane domaće mreže, koristi se za jednoznačnu identifikaciju mobilnog uređaja. Druga IP adresa, dodijeljena od strane stranog agenta, koristi se za usmjeravanje IP paketa prema i od mobilnog čvora. Mobilnost korisnika korištenjem MIP protokola postiže se kroz procese otkrivanja domaćeg i stranog agenta, registracije mobilnog uređaja i tuneliranja paketa prema odredištu.

Proxy Mobile IP protokol predstavlja unaprjeđenje Mobile IP protokola uz zadržavanje svih njegovih funkcionalnosti. Također koristi dvije IP adrese koje služe za identifikaciju i usmjeravanje paketa. PMIP protokol omogućuje mobilnost korisnicima provedbom procesa otkrivanja agenta, ažuriranja tablice podmreže, registracije mobilnog uređaja i tuneliranja podataka od i prema mobilnom čvoru.

Nedostatak i mana MIP protokola je primoranost korisnika da koristi specijalizirani softver kako bi mogao ostvariti mobilnost svoje komunikacije. Implementacija softvera povlači sa sobom velike vremenske i financijske troškove iz razloga što svi subjekti MIP komunikacije moraju koristiti spomenuti softver koji zahtjeva operativne zahvate na jezgri operativnog sustava mobilnog uređaja.

Implementacija PMIP protokola moguća je bez redizajniranja operativnog sustava. Omogućuje brže prekapčanje na drugu pristupnu točku te je povećana sigurnost komunikacije u odnosu na MIP rješenje. PMIP mehanizam sa sobom povlači manje troškove, manju potrebu za administracijom i konfiguracijom, a samim time omogućuje bržu implementaciju rješenja za mobilnost terminalnih uređaja.

Literatura

- [1] Poljanšek, I., Fabeta, T.: *Efikasna evolucija prema all-IP mrežama i širokopoljaskom dostupu*, Komunikacije, 2007.
- [2] 3rd Generation Partnership Project: *All-IP Network (AIPN) feasibility study*, 2014.
- [3] Jožipović, S.: *Integracija telefonske i Internet komunikacije (VoIP)*, prezentacija, 2009.
- [4] Hrvatska akademska i istraživačka mreža: *Sigurnosni aspekt VoIP tehnologije*, Zagreb, 2006.
- [5] URL: <http://pcchip.hr/tech/tehnologije-prikaza-televizijskih-programa> (pristupljeno: svibanj 2016.)
- [6] URL: www.ktios.net (pristupljeno: svibanj 2016.)
- [7] Vujović, V., Maksimović, M., Balotić, G., Mlinarević, P.: *Internet stvari – tehnički i ekonomski aspekti primjene*, Univerzitet u Istočnom Sarajevu, 2015.
- [8] Weber, M.: *Regulatorni izazovi Interneta stvari*, Hrvatska regulatorna agencija za mrežne djelatnosti
- [9] Ali-Yahiya, T.: *Understanding LTE and its Performance*, University Paris, 2011.
- [10] Hayashi, T.: *Evolved Packet Core (EPC) Network Equipment for Long Term Evolution (LTE)*, FUJITSU Sci. Tech. J., 2012.
- [11] URL: <http://www.lteandbeyond.com/2012/01/functions-of-main-lte-packet-core.html> (pristupljeno: lipanj 2016.)
- [12] URL: <https://sites.google.com/site/lteencyclopedia/lte-network-infrastructure-and-elements> (pristupljeno: lipanj 2016.)
- [13] URL: <https://sites.google.com/site/lteencyclopedia/lte-network-infrastructure-and-elements> (pristupljeno: lipanj 2016.)
- [14] Medvid, I., Šimić, Ž., Vučić, D.: *IMS i sustav naplate u stvarnom vremenu utemeljen na kvaliteti usluge*
- [15] Palat, S., Godin, P.: *The LTE Network Architecture*, Alcatel Lucent, 2009.

- [16] Johnson, T., Cardozo, E., Prado, R., Zagari, E., Badan, T.: *Mobility in IP Networks: From Link Layer to Application Layer Protocols and Architectures*, University of Sao Paulo, State University of Campinas, Federal University of Goias, 2010.
- [17] Baraković, S.: *Osiguranje kvalitete usluga sljedeće generacije optimizacijom signalizacijskih procedura*, Ministarstvo sigurnosti Bosne i Hercegovine
- [18] Nada, F.: *Performance analysis of Mobile IPv4 and Mobile IPv6*, The International Arab Journal of Information Technology, 2007.
- [19] Perkins, C. E.: *Mobile IP*, Internet Engineering Task Force
- [20] Cisco Systems: *Introduction to Mobile IP*, 3200 Series Mobile Access Router Software Configuration Guide
- [21] Cisco Systems: *Configuring Proxy Mobile IP*, Aironet 1200 Series Access Point Software Configuration Guide
- [22] URL: http://www.eetimes.com/document.asp?doc_id=1272128 (pristupljeno: svibanj 2016.)
- [23] URL: https://www.researchgate.net/figure/259176809_fig1_Fig-1-IoT-A-reference-architecture-functional-view (pristupljeno: svibanj 2016.)
- [24] URL: <http://www.cotsjournalonline.com/articles/view/103742> (pristupljeno: lipanj 2016.)
- [25] URL: <https://www.genband.com/company/glossary/ip-multimedia-subsystem> (pristupljeno: lipanj 2016.)
- [26] URL: https://www.google.hr/search?q=evolved+packet+core&client=firefox-b-ab&source=Inms&tbn=isch&sa=X&ved=0ahUKEwiS-sSM9JjPAhWEtBQKHQfEBEMQ_AUICCGB&biw=1280&bih=689#imgrc=XbilhAxSc-mGhM%3A (pristupljeno: lipanj 2016.)

Popis akronima

IP (eng. Internet protocol)

MIP (eng. Mobile IP Protocol)

PMIP (eng. Proxy Mobile IP Protocol)

QoS (eng. Quality of Service)

VoIP (eng. Voice over IP)

IPTV (eng. Internet Protocol Television)

IoT (eng. Internet of Things)

3GPP (eng. Third Generation Partnership Project)

E-UTRAN (eng. Evolved UMTS Terrestrial Radio Access Network)

EPC (eng. Evolved Packet Core)

LTE/EPC (eng. Long Term Evolution / Evolved packet core)

STM (eng. Synchronous Transfer Mode)

ATM (eng. Asynchronous Transfer Mode)

WiFi (eng. Wireless Fidelity)

CDMA2000 (eng. Code Division Multiple Access)

MME (eng. Mobility Management Entity)

S-GW (eng. Serving Gateway)

PDN-GW (eng. Packet Data Network Gateway)

PCRF (eng. Policy and Charging Rules Function)

NAS (eng. Non Access Stratum protocols)

HSS – (eng. Home subscriber server)

UMTS (eng. Universal Mobile Telecommunications System)

GPRS (eng. General Packet Radio Service)

WLAN (eng. Wireless Local Area Network)

ADSL (eng. Asymmetric Digital Subscriber Line)

PSTN (eng. Public Switched Telephone Network)

SIP (eng. Session Initiation Protocol)

SGSN (eng. Serving GPRS Support Node)

GGSN (eng. Gateway GPRS Support Node)

MRFP (eng. Multimedia Resource Function Processor)

IM-MGW (eng. IP Multimedia – Media Gateway)

CSCF (eng. Call Session Control Function)

MGCF (eng. Media Gateway Control Function)

MRFC (eng. Media Resource Function Controller)

E-UTRAN (eng. Evolved UMTS Terrestrial Radio Access Network)

HSDPA (eng. High Speed Downlink Packet Access)

HSUPA (eng. High Speed Downlink Packet Access)

OFDMA (eng. Orthonogal Frequency Division Multiple Access)

SC-FDMA (eng. Single Carrier Frequency Division Multiple Access)

eNB (eng. Evolved Node B)

IPSec (eng. Internet Protocol Security)

IRDP (eng. ICMP Router Discovery Protocol)

AAP (eng. Authoritative Access Point)

AAA server (eng. Authentication Authorization and Accounting server)

LAN (eng. Local Area Network)

Popis slika

Slika 1. Mrežna arhitektura IPTV usluge	12
Slika 2. IoT-A referentni model	16
Slika 3. Arhitektura evoluirane paketske jezgrene mreže	23
Slika 4. Prikaz arhitekture IP višemedijskog podsustava	30
Slika 5. Arhitektura E-UTRAN pristupne mreže	33
Slika 6. Prikaz funkcionalnih komponenata MIP protokola	43
Slika 7. Funkcionalne komponente Proxy Mobile IP mreže	52

Popis dijagrama

Dijagram 1. Otkrivanje agenta u sklopu Mobile IP procesa	46
Dijagram 2. Registracija mobilnog čvora unutar Mobile IP procesa	48
Dijagram 3. Tuneliranje IP paketa u sklopu Mobile IP procesa	50
Dijagram 4. Otkrivanje agenta u sklopu Proxy Mobile IP procesa	56
Dijagram 5. Registracija mobilnog uređaja u sklopu Proxy Mobile IP procesa	59
Dijagram 6. Tuneliranje IP paketa u sklopu Proxy Mobile IP procesa	61

METAPODACI

Naslov rada: Upravljanje mobilnošću u All-IP mrežama

Student: Augustin Anić

Mentor: izv. prof. dr. sc. Štefica Mrvelj

Naslov na drugom jeziku (engleski): Mobility management in All-IP networks

Povjerenstvo za obranu:

- prof. dr. sc. Zvonko Kavran predsjednik
- izv. prof. dr. sc. Štefica Mrvelj mentor
- dr. sc. Marko Matulin član
- doc. dr. sc. Niko Jelušić zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko-komunikacijski promet

Vrsta studija: diplomski studij

Studij: Promet

Datum obrane diplomskog rada: 27. rujna 2016.

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj _____ diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu _____ diplomskog rada pod

naslovom **Upravljanje mobilnošću u All-IP mrežama** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom

repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, _____ 27. rujna 2016.

(potpis)