Arhitektura VoIP mreže

Flanjak, Zvonimir

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Zvonimir Flanjak

ARHITEKTURA VoIP mreže

ZAVRŠNI RAD

Zagreb, 2018.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

ARHITEKTURA VoIP mreže

ARCHITECTURE OF VoIP NETWORK

Mentor: dr. sc. Ivan Forenbacher

Student: Zvonimir Flanjak

JMBAG: 0135234139

Zagreb, kolovoz 2018.

Arhitektura VoIP mreže

Sažetak

Porastom potrebe za razmjenom sadržaja te proširenjem spektra mogućnosti mreže nastala je problematika vezana uz komunikaciju mreža različitih tehnologija. Rješenje je pronađeno u protokolima i standardima koji su omogućili interoperabilnost različith tipova mreža. Konvergencija je korak prema savladavanju trenutnih problema u prijenosu podataka različitih tipova mreža.

Voice over IP nudi se kao jedno od prihvatljivih rješenja za zamjenu postojeće PSTN (eng. *Public Switched Telephone Network*) mreže koja omogućuje glasovnu komunikaciju. Također, proširenjem spektra mogućnosti komunikacijske mreže nastaju potencijalni sigurnosni problemi, stoga je potrebno voditi računa o stupnju integriteta podataka u mreži. Cilj ovog rada je opisati osnovne elemente VoIP mreže, definirati potrebne protokole za rad VoIP-a, interoperabilnost s drugim tehnologijama te mehanizme zaštite VoIP mreže.

KLJUČNE RIJEČI: Voice over IP, protokoli, interoperabilnost

Architecture of VoIP Network

Summary

Human need to exchange information on a greater distance brings the development of communication networks to such quality where average user can’t experience any delays or losses in transmission. However,increased need to exchange the content and network possibilities resulted with interoperability issues of networks based on different technologies. The solution was found in protocols and standards that enabled the interoperability of differenty types of networks. Convergence is a step towards in overcoming the current problems in data transmission of different types of networks.*Voice over* IP is offered as one of the most affordable solutions for replacing an existing PSTN (eng. *Public Switched Telephone Network*) network that provides voice communication. Also, by expanding the spectrum of communication network capabilities, potential security problems arise, so it is necessary to take into account the level of data integrity in the network. Therefore, the aim of this paper is to describe the basic elements of the VoIP network, define the necessary VoIP protocol protocols, interoperability with other network technologies, and VoIP network security.

KEYWORDS: Voice over IP, protocols, interoperability

Sadržaj

1 Uvod 1
2 Evolucija mreža za prijenos govora 2
3 Arhitektura VoIP mreže 4
4 Protokoli i standardi korišteni za VoIP 6
4.1 Protokoli za prijenos audio signala 6
4.1.1 Real-time Transport Protocol (RTP) 7
4.1.2 Real-Time Streaming Protocol (RTSP) 7
4.1.3 Real-time Control Protocol (RTCP) 8
4.1.4 Resource Reservation Protocol (RSVP) 9
4.2 Signalizacijski protokoli 9
4.2.1 H.323 10
4.2.2 Session Initiation Protocol (SIP) 13
4.2.3 Media Gateway Control Protocol (MGCP) 15
4.3 Session Description Protocol (SDP) 15
4.4 Session Announcement Protocol (SAP) 16
5 Značajke VoIP mreže 17
5.1 Quality of service 17
5.2 Sigurnosne prijetnje (značajke) VoIP mreže 18
5.3 Načini zaštite VoIP mreže 20
5.3.1 Fizička zaštita 20
5.3.2 Odvajanje IP adresa 21
5.3.3 Virtualni LAN-ovi 21
5.3.4 Vatrozidi 21
5.3.5 Enkripcija 22
5.4 Prednosti i nedostatci 23
6 Interoperabilnost VoIP s ostalim mrežama 24
6.1 Interoperabilnost s nepokretnom mrežom 26
6.2 Interoperabilnost s pokretnom mrežom 28
7 Zaključak 30
Popis kratica 31
Literatura 32
Popis fotografija 34
Popis tablica 35

1 Uvod

Razvoj tehnologije imao je veliki doprinos u načinu komuniciranja i razmjene informacija. Prve su mreže omogućavale prijenos samo jedne vrste informacija, a današnjom tehnologijom moguće je ostvariti istovremeni prijenos više vrsta informacija. Sve te tehnologije bilo je potrebno nekako umrežiti kako bi mogle međusobno komunicirati. Stoga su definirani različiti standardi i protokoli koji su omogućili interoperabilnost između različitih tehnologija.

Novim komunikacijskim tehnologijama omogućeno je prenošenje veće količine podataka putem iste mreže uz djelomičnu izmjenu arhitekture. Evolucija mreže donijela je veću kvalitetu u prijenosu informacija. Primarni je cilj daljnjeg razvoja povezati sve tehnologije kako bi djelovale kao homogena cjelina koja bi pojednostavila prijenos informacija između različitih tehnologija i mreža. Prvi je rezultat toga razvoj VoIP mreža koje su omogućile glasovnu komunikaciju i multimedijske sjednice korištenjem Internet-protokola.

Cilj je ovoga završnog rada objasniti što je VoIP, na koji način funkcionira i navesti njegove značajke te grafički prikazati arhitekturu VoIP mreže, objasniti njezine dijelove i protokole koji se koriste, kroz 7 poglavlja:

1. Uvod
2. Evolucija mreža za prijenos govora
3. Arhitektura VoIP mreže
4. Korišteni protokoli u VoIP mrežama
5. Značajke VoIP mreže
6. Interoperabilnost VoIP s ostalim mrežama
7. Zaključak

U drugom će poglavlju biti opisan povijesni razvoj mreže koji počinje pojavom NMT-a i sve do pojave prve VoIP mreže, koji su omogućile prijenos govora korištenjem Internet-protokola.

Treće se poglavlje odnosi na arhitekturu VoIP mreže. Navest će se njezini osnovni dijelovi koji su potrebni za implementaciju VoIP-a. Objasnit će se uloga svakog dijela arhitekture i konačno način rada same VoIP mreže.

U četvrtom će poglavlju biti navedeni osnovni protokoli potrebni za rad VoIP mreže. Protokoli će biti razvrstani u skupine s obzirom na njihovu primjenu te će se objasniti njihova uloga.

Kroz peto poglavlje bit će definirane karakteristike VoIP mreže, parametri kao što su packet jitter, kašnjenje, gubitak paketa, *echo* i drugi, koji utječu na kvalitetu VoIP usluge. Također, bit će objašnjena pouzdanost i sigurnost VoIP mreže koja je vrlo važna za integritet informacija.

U posljednjem će poglavlju biti objašnjeni potrebni čimbenici koji omogućuju nesmetanu komunikaciju VoIP mreže s ostalim mrežama.

2 Evolucija mreža za prijenos govora

Početak telekomunikacije i prvih prijenosa glasa na veće udaljenosti započeo je izumitelj Alexander Graham Bell koji je izumio prvi telefon 1876. godine. Sljedeće godine uspio je ostvariti dvosmjernu vezu na dionici udaljenoj 16 km. Time su telefon i telefonski sustav revolucionirali način komunikacije. Za razvoj telefona je važna 1878. godina kada je Hunnings izumio ugljeni mikrofon i time znatno povećao doseg veze između dva telefona. Rastom broja telefonskih linija pojavljuje se problem povezivanja različitih telefonskih linija te zato nastaju prvu telefonske centrale. Prve telefonske centrale nisu bile automatizirane, već su zaposlenici u centralama morali ručno prospajati pozive prema odredištu. Prva telefonska centrala izgrađena je 1878. godine u New Havenu, [18].

Almon B Strowger 1889. godine patentirao je prvu automatsku centralu, a 1892. godine u suradnji s Joseph B. Harrisom i Moses A. Mayerom formira kompaniju Strowger Automatic Telephone Exchange i pušta u rad prvu telefonsku centralu. Automatizacijom telefonskih centrala uvedeno je pulsno biranje, tako da svaki pretplatnik može izravno pozvati drugog pretplatnika, no međugradski pozivi su i dalje zahtijevali ručno prospajanje operatera. Kasnijom pojavom adresne signalizacije, uključujući metode višestruke frekvencije, omogućilo je pretplatnicima izravno pozivanje na veće udaljenosti. Već do kraja 20. stoljeća kontrolu poziva je vršio signalni sustav 7 (eng. *Signalling System No. 7*). To je bio početak globalnog PSTN-a. Revolucijom tranzistora telefonske tvrtke počele su prebacivati vlastite mreže u digitalan način rada. Digitalna mreža za integrirane usluge (eng. *Integrated Services Digital Network* - ISDN) prvi je komunikacijski standarda za istovremeni digitalni prijenos glasa, video, podataka i drugih usluga preko tradicionalne PSTN bakrene mreže, što rezultira boljom kvalitetom poziva od analogne linije. Dizajniran je za pružanje jedinstvenog sučelja (u smislu hardvera i komunikacijskih protokola) za povezivanje telefona, faks uređaja, računala. Prvi ISDN bio je prikaz kako će u budućnosti telefonske mreže izgledati, [18].

Prva generacija mobilnih mreži, poznata kao 1G sagrađena je početkom osamdesetih godina prošlog stoljeća i koristila je analogne signale za prijenos govora pomoću FDMA (eng. *Frequency-Division Multiple Access*) tehnologije. Druga generacija mobilne mreže je prva digitalna implementacija bežične govorne mreže. Njom je pokrenut GSM (eng. *Global System for Mobile Communications*) standard koji je omogućio *roaming*, isporuku poruka SMS (eng. *Short Message Service*), multimedijske poruke MMS (eng. *Multimedia Messaging Service*). Razvoj 2.5 G je promatran kao korak prema 3G, što je potaknuto potražnjom za boljom podatkovnom uslugom i pristupom internetu. Brzine od 64-144 kbps omogućile su mobilnim telefonima Internet pretraživanje, navigaciju, faks, glasovnu poštu i sl. Početkom 2000.-te godine kompanije su razvile 3G mrežu. Značajke 3G sustava su da podržavaju mnogo veće brzine prijenosa podataka i nude veći kapacitet, što ih čini prikladnim za aplikacije velikih brzina kao i za tradicionalne glasovne pozive. Ali

ljudska potreba za još većim brzinama potaknula je razvoj trenutno primarne mobilne telekomunikacijske mreže (4G). Koja pruža još veće brzine nego 3G.

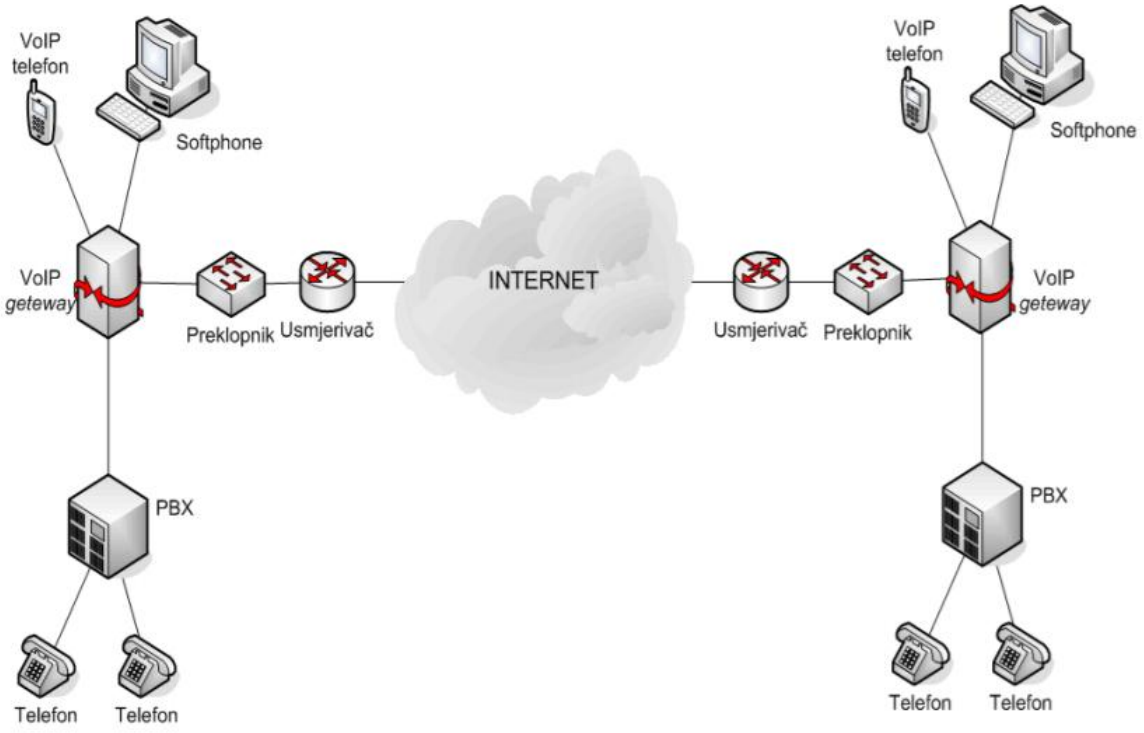
3 Arhitektura VoIP mreže

Voice over IP tehnologija je koja omogućuje korištenje IP mreže za glasovne aplikacije kao što su telefonija, glasovne poruke i telekonferencija. VoIP definira način prijenosa glasovnih poziva putem IP mreže, uključujući digitalizaciju i paketizaciju glasovnih tokova. VoIP sustavi pretvaraju naš glas u digitalan signal koji je pogodan za prijenos IP mrežom. Ako korisnik poziva tradicionalni telefonski broj, signal se pretvara u tradicionalni telefonski signal prije nego stigne do odredišta. VoIP omogućuje upućivanje poziva izravno s računala, VoIP telefona ili tradicionalnih analognih telefona povezanih posebnim adapterom, [19].

Osnovna komponente vidljive na slici 1. koje su potrebne za stvarnu implementaciju VoIP-a, prema [2] jesu:

- MREŽNA INFRASTRUKTURA - podržava VoIP tehnologiju i može se gledati kao jedna logička glasovna mreža distribuirana preko IP okosnice koja pruža konekciju i prijenos glasovnih paketa preko mreže. Ta IP infrastruktura mora omogućiti prijenos glasovnih paketa bez ikakvih poteškoća.
- PROCESORI (KONTROLERI) POZIVA - moduli potrebni za uspostavljanje i nadziranje poziva, autorizacije korisnika, pružanja osnovnih telefonskih usluga i kontroliranje brzine prijenosa (eng. *bandwidth*) za svaki link.
- PREVODIOCI (eng. *MEDIA/SIGNALING GATEWAYS*) - potrebni su za nastajanje poziva, detekciju poziva, pretvorbu glasa iz analognog u digitalni oblik (stvaranje glasovnih digitalnih paketa). Ujedno to su komponente koje omogućuju prelazak između različitih tehnologija (npr. prelazak između IP i ISDN tehnologija).
- KORISNIČKI VoIP TERMINALI - Potražnja za VoIP uslugama je uzrokovala široki asortiman korisničkih tzv. "*end-user*" proizvoda kao što su:
    - VoIP terminali– obično ti proizvodi imaju ekstra dodatne mogućnosti koje nadilaze obične telefone. Neki od takvih proizvoda imaju osnovne funkcionalnosti koje pružaju iste mogućnosti kao i konvencionalni telefoni.
    - Konferencijski VoIP terminali – pružaju istu vrstu usluge kao i obični konferencijski telefoni, ali pošto se komunikacija provodi preko Interneta korisniku je dozvoljeno koordiniranje tradicionalnih podatkovnih usluga (npr. što se prikazuje na monitorima na oba kraja razgovora).
    - Mobilni VoIP terminali – bežične VoIP jedinice postaju sve više i više popularne, pogotovo što organizacije već imaju ugrađene osnovne 802.11Q mrežne komponente. Bežični VoIP predstavlja veliki sigurnosni problem, pogotovo zbog naširoko poznatih nedostataka 802.11Q protokola.
- OSOBNA RAČUNALA tzv. *Soft Phone* sustavi – sa slušalicama, aplikacijom (npr. Skype,

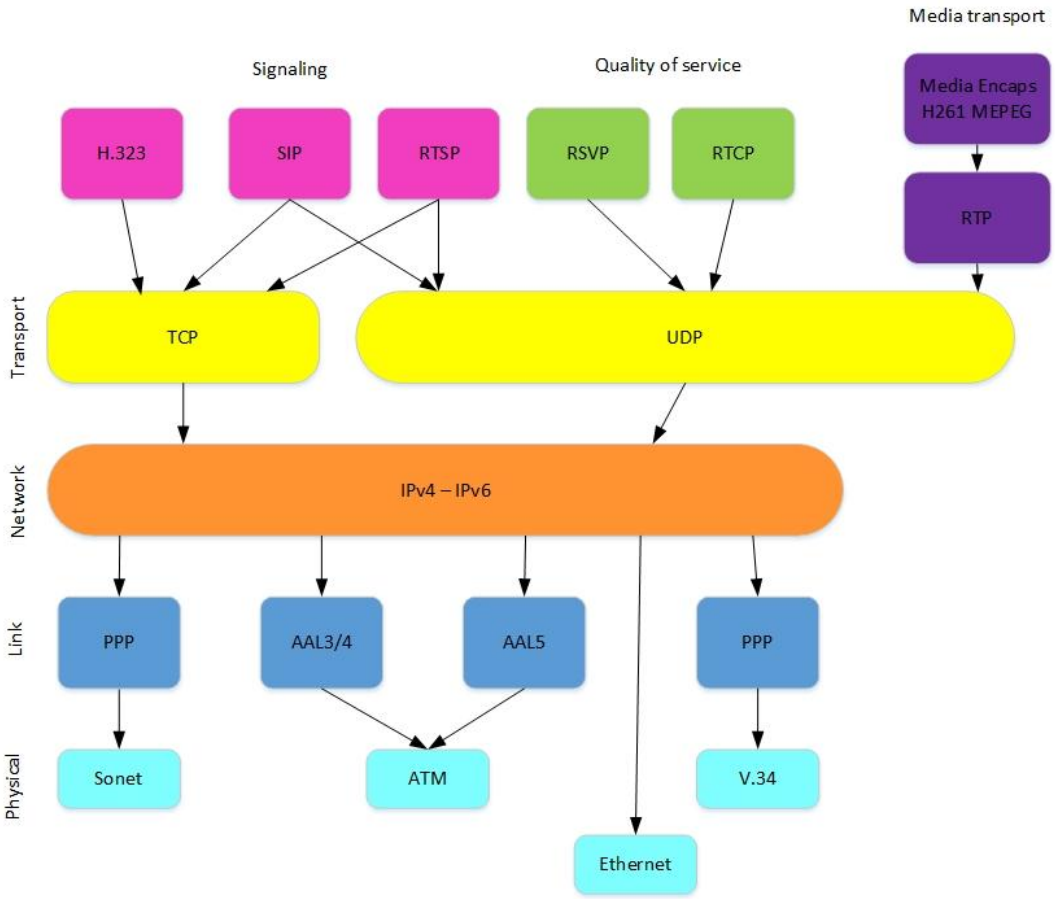
Microsoft NetMeeting) i jeftinom konekcijom na Internet, svaki PC ili radna stanica mogu biti iskorišteni kao VoIP komponenta.



Slika 1. VoIP arhitektura, [2]

4 Protokoli i standardi korišteni za VoIP

Protokole potrebne za rad današnjih VoIP sustava mogu se podijeliti na protokole za prijenos multimedijskog i signalizacijskog sadržaja. Protokolarna arhitektura vidljiva na slici 2., a protokoli za prijenos audio signala i signalizacijski protokoli bit će razrađeni u nastavku.



Slika 2. Protokolarna arhitektura VoIP-a

Izvor: [16]

4.1 Protokoli za prijenos audio signala

Protokoli za prijenos audio signala zaduženi su za isporuku audiosadržaja i videosadržaja, kontrolu *media* servera koji uspostavlja i kontrolira medijsku sesiju, nadzor prijenosa podataka i rezervaciju resursa potrebnim aplikacijama. U nastavku bit će definirani sljedeći protokoli: RTP (eng. *Real-time Transport Protocol),* RTSP (eng. *Real-Time Streaming Protocol)*, RTCP (eng. *Real-time Control Protocol*) i RSVP (eng. *Resource Reservation Protocol*) protokoli.

4.1.1 Real-time Transport Protocol (RTP)

Real-time Transport Protocol (RTP) je protokol mrežnog sloja OSI modela. Zadaća je RTP protokola isporuka audiosadržaja i videosadržaja putem mreže. Najčešće se primjenjuje u sustavima za komunikaciju i zabavu koji uključuju streaming-medije kao što su telefonija, videokonferencija, TV-usluge itd. RTP određuje način na koji programi upravljaju prijenosom multimedijskog sadržaja u realnom vremenu preko unicast i multicast usluga. Ovaj protokol ne garantira trenutnu dostavu multimedijskih podataka jer ovisi o karakteristikama mreže, [4].

RTP je jedan od temelja VoIP-a i koristi se zajedno sa SIP-om koji pomaže u postavljanju veza preko mreže. Također se koristi u kombinaciji s RTCP-om. RTP nosi medijske tokove, a RTCP služi za praćenje statističkih podataka o prijenosu i kvaliteti usluge te pomaže u sinkronizaciji više streamova. Nadgledanje prijenosa omogućuje primatelju detektiranje gubitaka podataka i nadoknađivanje bilo kakvih nedostataka uzrokovanih kašnjenjem ili varijacijom kašnjenja. Informacije u zaglavlju RTP-a omogućuju primatelju rekonstrukciju podataka i a također sadrži informacije koje navode kako se bitovi kodeka raspadaju u pakete. RTP protokol, prema hijerarhiji, izvršava se iznad UDP protokola, [12].

Funkcije RTP protokola prema [7]:

- Sekvenciranje: Broj sekvence u RTP paketu koristi se za otkrivanje izgubljenih paketa.
- Identifikacija opterećenja: na Internetu je često potrebno dinamički mijenjati kodiranje medija kako bi se prilagodila promjeni dostupnosti propusnosti. Kako bi se osigurala ova funkcionalnost, u svakom RTP paketu uključen je identifikacijski broj opterećenja za opisivanje kodiranja medija.
- Indikator okvira: Video i audio šalju su u logičkim jedinicama zvanim okviri. Početak i kraj okvira označava se„frame marker“ bitom.
- Identifikacija izvora: U multicast sesiji imamo mnogo sudionika. Dakle, identifikacija je potrebna za određivanje pokretača okvira. Za identifikaciju se koristi SSRC (eng. *Synchronization Source*).
- Intramedia sinkronizacija: Kako bi nadoknadili različite odgode zagušenja za pakete u istom streamu, RTP nudi vremenske oznake.

4.1.2 Real-Time Streaming Protocol (RTSP)

Real Time Streaming Protocol (RTSP) protokol je koji djeluje na aplikacijskom sloju OSI modela. Koristi se u komunikacijskim sustavim za kontolu stremaing media servera. On uspostavlja i kontrolira medijsku sesiju od jednoga kraja do drugoga kraja pružajući „network-remote-control“ za jedan ili više vremenski sinkroniziranih streamova s kontinuiranim prijenosom medijskog sadržaja. Koristi se kao „network remote control“ u multimedijskim serverima. RTSP nije zadužen za prijenos samih podatak. RTSP serveri najčešće za prijenos koriste RTP protokol zajedno s RCTP za prijenos medijskog sadržaja. Funkcije RTSP protokola prema [12]:

- Dohvaćanje multimedijskog sadržajas medijskog poslužitelja: Klijent može zatražiti opis prezentacije i zatražiti od poslužitelja postavljanje sesije za slanje traženih podataka. Poslužitelj može slati prezentaciju na više točaka *multicastom* ili ju poslati klijentu koristeći *unicast*.
- Poziv medijskog poslužitelja na konferenciju: Medijski poslužitelj može biti "pozvan" da se pridruži postojećim konferencijama, za reprodukciju medija ili snimanje prezentacije. Ovaj način je koristan za distribuirane poduke. Nekoliko stranke na konferenciji mogu se preokrenuti "guranje daljinskog upravljača kontrolne tipke. "
- Dodavanje medija na postojeću prezentaciju: Poslužitelj ili klijent mogu se međusobno obavijestiti o svim dodatnim medijima koji su postali dostupni.

4.1.3 Real-time Control Protocol (RTCP)

Real-Time Transport Control Protocol (RTCP) protokol je koji nadzire prijenos podataka na velikim multicast mrežama. Time pripomaže radu RTP protokola. RTCP se koristi u VoIP-u, IPTV-u, *streaming* medijima i videokonferencijama. RTCP prenosi statističke i kontrolne podatke, RTP prenosi sadržaj. Neke su od informacija koje RTCP prenosi količina *byteova* za prijenos, količina poslanih i izgubljenih paketa te *round-trip delay* između krajnjih točaka. Također sadrži CNAME (eng. *Canomical Name*) koji jednoznačno označava sudionike tijekom uspostavljanja sesije, [7].

RTCP koristi pet različitih vrsta paketa (poruka) za prijenos različitih kontrolnih informacija prema [7]:

- RR (Receiver report) – za statistiku prijema od sudionika koji nisu aktivni pošiljatelji
- SR (sender report) – za statistiku prijenosa i prijema od sudionika koji su aktivni pošiljatelji
- SDES – stavke za opis izvora, uključujući CNAME
- BYE – ukazuje na kraj sudjelovanja
- i APP – funkcije specifične za aplikaciju

Prema [7] dodatne usluge koje RTCP pruža sudionicima jesu:

• QoS povratna informacija: RTCP se koristi za prijavljivanje kvalitete usluge. Navedene informacije sadrže broj izgubljenih paketa, vrijeme kružnog putovanja, podrhtavanje, a izvori te podatke koriste za prilagodbu brzine prijenosa podataka.
• Kontrola sesije: Pomoću BYE paketa RTCP omogućuje sudionicima da naznače da napuštaju sesiju.
• Identifikacija: Informacije poput adrese e-pošte, imena i telefonskog broja uključene su u pakete RTCP-a tako da svi korisnici mogu znati identitet drugih korisnika za tu sesiju.

• Intermedijska sinkronizacija: Iako se video i audio obično šalju preko različitih streamova, potrebno ih je sinkronizirati na prijamniku kako bi se zajedno reproducirali. RTCP pruža informacije potrebne za usklađivanje tokova.

4.1.4 Resource Reservation Protocol (RSVP)

Resource Reservation Protocol (RSVP) predstavlja skup pravila koja definiraju komunikacijske kanale koji će se koristiti za *multicast* (jedan izvor – više odredišta) prijenos videozapisa i drugih poruka. RSVP je dio modela Internet Integrated Services (IIS) koji osigurava najbolju uslugu u stvarnom vremenu i kontrolirano dijeljenje veza. Također, omogućuje aplikacijama rezervaciju i odustajanje od rezerviranih resursa nakon prestanka potreba za njima. Rad RSVP-a rezultira rezerviranjem resursa u svakom čvoru duž cijelog puta, [14].

Temeljna filozofija usmjeravanja na Internetu je *„best effort“* koji služi većem broju korisnika dovoljno dobro, ali nije prikladan za prijenos videosadržaja i audiosadržaja. Ako korisnik želi određeni internetski program, RSVP tom korisniku omogućuje rezervaciju dijela frekvencijskog pojasa za prijem programa, samim time i veće brzine prijenosa i pouzdaniji protok. Osim multicasta, RSVP također podržava i unicast (jedan izvor – jedno odredište) prijenos, [14].

Prema [15] postoje dvije glavne vrste poruka:

- *path messages* (path)

Path messages šalje se od domaćina pošiljatelja duž putanje podataka i pohranjuje stanje puta u svakom čvoru duž staze. Stanje puta sadrži IP-adresu prethodnog čvora, a neki podatkovni objekti jesu:

1. predložak pošiljatelja za opisivanje formata podataka pošiljatelja u obliku *Filterspec* [2]
2. pošiljatelj *tspec* za opis prometne karakteristike protoka podataka
3. *adspec* koji nosi reklamne podatke (više pojedinosti potražite u RFC 2210).

- reservation messages (*resv*)

Resv-poruka šalje se od prijamnika do pošiljatelja uz obrnuti put podataka. Na svakom čvoru IP adresa odredišta resv-poruke će se promijeniti na adresu sljedećeg čvora na obrnutom putu i IP adresa izvora na adresu prethodne adrese čvora na obrnutom putu. *Resv*-poruka sadrži podatkovni objekt flowpec koji identificira resurse potrebne za protok.

4.2 Signalizacijski protokoli

Signalizacija je sposobnost generiranja i razmjene kontrolnih informacija koje će se koristiti za upravljanje, praćenje i otpuštanje veza između krajnjih točaka. Glasovno signaliziranje traži sposobnost pružanja funkcije nadzora, adresiranja i upozororavanja između čvorova, [11].

Tradicionalna PSTN mreža koristi se signalnim sustavom 7 (SS7) za prijenos kontrolnih poruka. Danas tri najpopularnija signalizacijska protokola koji se koriste u današnjim VoIP sustavima jesu H.323, SIP (eng. *Session Initiation Protocol*) koji se koriste za uspostavu poziva te MGCP (eng. *Media Gateway Contol Protocol*) protokol za kontrolu pretvornika medija.

VoIP signalizacijski protokoli mogu se podijeliti u dvije skupine prema [17]:

- procesi kontrole sesije (eng. *Session Control Protocol* - SCP)
- medijski kontrolni protokoli (eng. *Medica Control protocol* - MCP).

Protokoli za kontrolu sesije (SCP) odgovorni su za uspostavljanje, očuvanje i prekidanje poziva. Oni su također odgovorni za pregovore o parametrima sesija kao što su kodeksi, tonovi, mogućnosti širine pojasa i drugo. Primjeri takvih protokola jesu: H.323 i SIP (eng. *Session Initiation Protocol*), [17].

Protokoli kontrole medija (MCP) odgovorni su za stvaranje i uklanjanje medijskih veza. Koriste se za otvaranje i zatvaranje medijskih veza na VoIP *gateway-ima* i za obradu obavijesit koje dolaze od tih pristupnika. *Media Gateway* je VoIP komponenta koja prenosi medije između IP i PSTN mreže. Njime upravlja MGC. Dva glavna protokola za kontrolu medija jesu: MGCP i Megaco (H.248), [17].

4.2.1 H.323

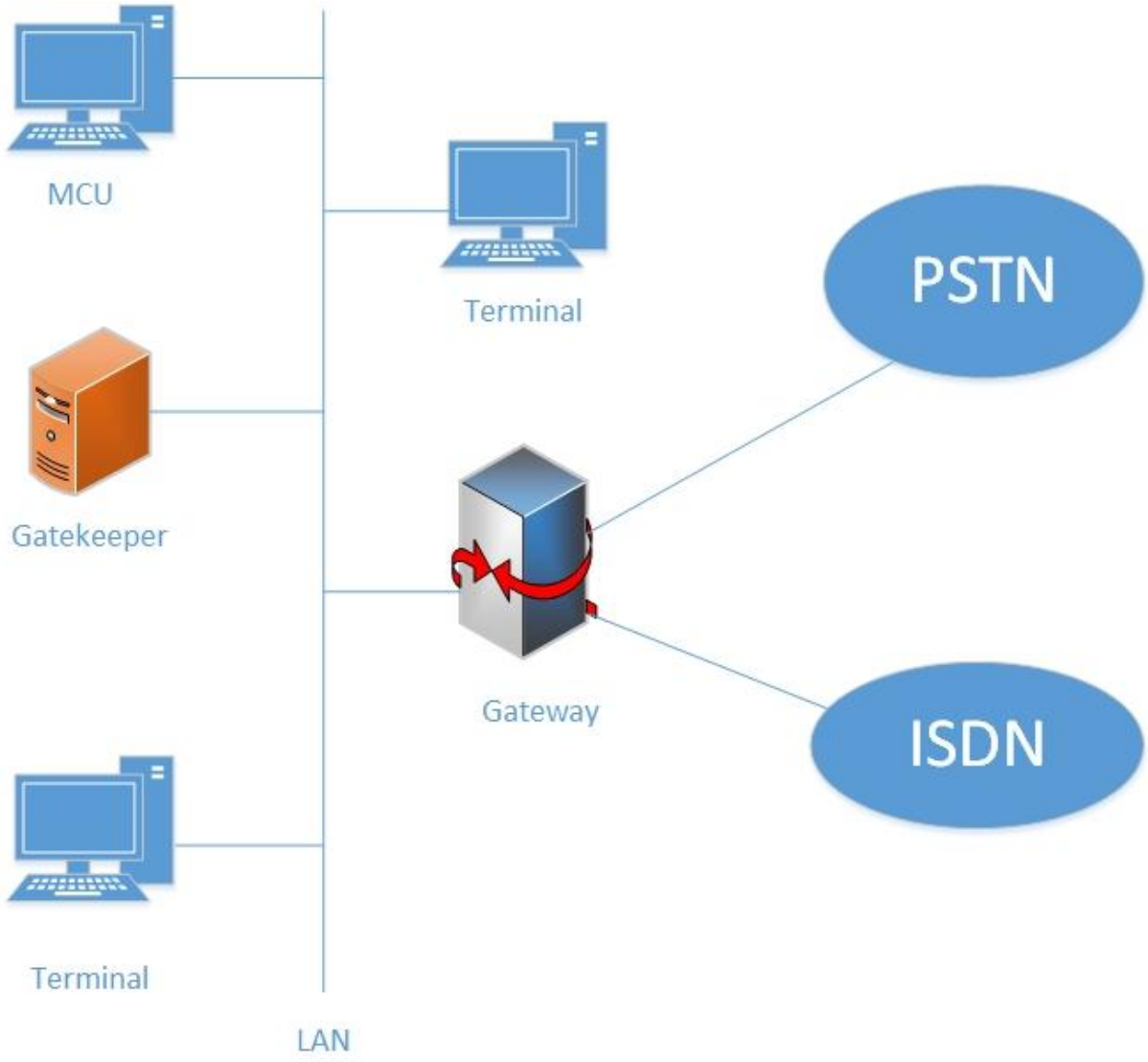
H.323 je standard međunarodne telekomunikacijske unije (ITU – *International telecomunication union)* koji definira kako terminalni uređaji, oprema i multimedijalne usluge komuniciraju putem mreže koja ne pruža jamstvo kvalitete usluge (npr. Internet). H.323 terminali i oprema mogu prenositi video u realnom vremenu, isto kao i glasovni razgovor, podatke ili neku kombinaciju tih elemenata. Proizvodi koji se koriste standardom H.323 za zvuk i sliku omogućavaju spajanje i komunikaciju s drugim korisnicima putem interneta, isto kao što korisnici s različitim telefonima mogu međusobno komunicirati, [3]

Prema [10] svojstva H.323 standarda jesu:

- standardna kompresija/dekompresija
- povezivanje različite opreme
- neovisnost o mreži
- neovisnost o opremi i aplikaciji
- podrška za konferencijsku vezu
- nadzor mreže i
- podrška za komunikaciju s više krajnjih točaka.

Prema [2] H.323 definiran je pomoću četiriju logičkih komponenata kao što je vidljivo na slici 3.:

- terminal - osnovni element svake H.323 zone. Tipičan predstavnik H.323 terminala je Microsoft-ov NetMeeting.
- prevodilac protokola (eng. *gateway*) - komponenta koja omogućava prelazak između različitih tehnologija, tzv. most između H.323 zone i neke druge mreže. (npr. H.323/H.320 *gateway* osigurava prelazak između IP i ISDN tehnologija).
- *gatekeeper* - komponenta koja nadgleda rad svih ostalih komponenti u H.323 zoni (može se poistovjetiti s telefonskom centralom u klasičnoj telefoniji). Njegova je uloga:
    - preslikavanje pozivanih telefonskih brojeva u IP adrese odredišnih VoIP *gateway*-a, tj. pohranjivanje plana numeracije čitave mreže i
    - zaštita mrežnih resursa odnosno kontrola broja uspostavljenih VoIP poziva kroz mrežu (čime se eliminira pojava zagušenja u mreži uslijed prevelikog istovremenog broja VoIP poziva).
- MCU (eng. *Multi-point Control Unit*) - zadužen za kontrolu *multi-point* konferencija (dvije ili više točaka “spojenih“ u konferenciju). MCU sadrži Multi-*point* kontroler (MC) koji nadgleda pozive, a po potrebi ima i *Multi-point* procesor (MP) kako bi mogao upravljati medijima (prebacivanje između medija ili neki drugi proces, …).



Slika 3. H.323 komponente

Izvor: [12]

4.2.2 Session Initiation Protocol (SIP)

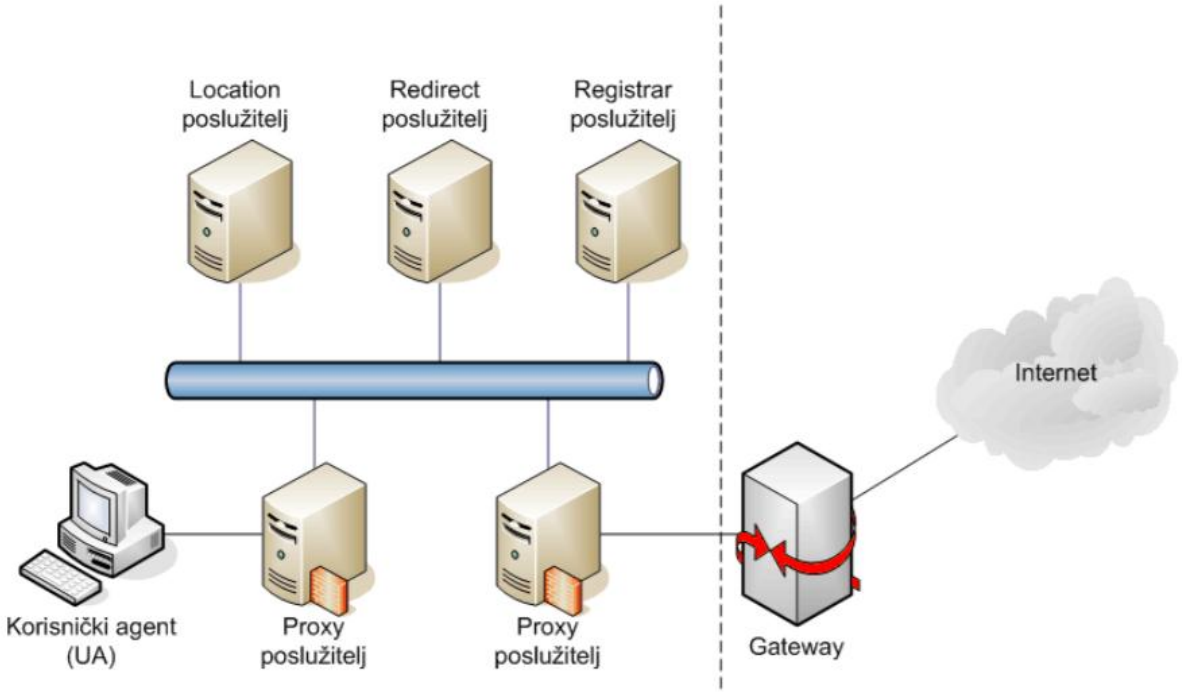
Sesijski inicijacijski protokol (SIP) signalni je protokol koji se koristi pri uspostavljanju VoIP veze. SIP je dizajniran kao alternativa H.323 signalizaciji. Najčešće se SIP koristi za uspostavljanje i raskidanje glasovnih te videopoziva, ali također se može koristiti za modifikaciju već postojećih poziva, na primjer za dodavanje ili uklanjanje sudionika u pozivu. SIP koristi upit-odgovor model tako da se pojedina SIP transakcija sastoji od klijentskog upita, praćena s minimalno jednim odgovorom od strane poslužitelja. SIP ne prenosi zvuk od izvora do destinacije. Korisnik ili pozivatelj je identificiran pomoću URI (*eng. Uniform Resource Identifier*), [9]

Sesija se može inicirati na dva načina, prema [21]:

1. Ako je poznata SIP odredišna adresa, (1) pozivatelj šalje destinacija invite poruku u sklopu lokalnog proxy poslužitelja (IP PBX centrala).
2. Ako nije poznata SIP odredišna adresa, tada matični proxy poslužitelj šalje zahtjev prema (2) redirect poslužitelju koji šalje upit (3) location poslužitelju. (4) Redirect poslužitelj šalje informaciju prema matičnom proxy poslužitelj pozivatelja koji tada šalje (5) invite poruku na odredišni proxy poslužitelj prema dobivenoj SIP adresi. Odredišni proxy poslužitelj može konzultirati (6) location poslužitelja ako ne zna odmah lokaciju odredišta. Nakon toga, (7) prosljeđuje invite poruku prema odredištu.

Na slici 4. vidljivi su elementi SIP arhitekture, [2].

- Korisnički agenti (*eng. User Agents*) – bilo koji klijent ili uređaj koji inicira SIP povezivanje poput IP telefona, računalnog *instant messaging* klijenta, ili mobilnog uređaja. Taj korisnički agent također može biti *gateway* koji je u interakciji s PSTN-om
- Posredni (eng. *proxy*) poslužitelj - najvažnija funkcija *proxy* poslužitelja je pronalaženja korisnika i prevođenje adresa. Tijekom svog rada *proxy* poslužitelj može generirati zahtjeve drugim poslužiteljima ili klijentima.
- Identifikacijski (eng. *registrar*) poslužitelj - prihvaća identifikacijske zahtjeve i najčešće se postavlja skupa s *redirect* ili *proxy* poslužiteljem.
- Preusmjerivački (eng. *redirect*) poslužitelj - prihvaća zahtjeve i na njih odgovara s 0 ili više mogućih adresa za uspostavljanje veze. Za razliku od *proxy* poslužitelja on ne može poslati zahtjev niti kao korisnički agent klijent uspostaviti vezu.
- Locirajući (eng. *location*) poslužitelj - služi za pronalaženje trenutne korisnikove lokacije (IP adrese).



Slika 4. SIP komponente, [2]

Tablica 1.H.323 i SIP usporedba

Usporedba H.323 i SIP-a		
Naziv	H.323	SIP
Kreiran od	ITU	IETF
Kompatibilnost s PSTN-om	Da	Da
Kompatibilnost s Internetom	Ne	Da
Arhitektura	Monolitna	Modularna
Kompleksnost	Cijeli stog protokola	SIP upravlja postavljanjem
Pregovaranje oko parametara	Da	Da
Signaliziranje poziva	Q.931 preko TCP-a	SIP preko TCP-a / UDP-a
Format poruka	Binarni	ASCII
Transport medija	RTP/RTCP	RTP/RTCP
Poziv s više od dva člana	Da	Da
Multimedijske koncerencije	Da	Ne
Adresiranje	Telefonski broj	URL
Prekid poziva	Izričito ili TCP otpuštanje	Izričito ili *Timeout*
Instant poruke	Ne	Da
Enkripcija	Ne	Da
Veličina standarda	1400 stranica	250 stranica
Implementacija	Velika i kompleksna	Umjerena
Status	Široko rasprostranjen	Perspektivna zamjena

Izvor: [13]

4.2.3 Media Gateway Control Protocol (MGCP)

U početku *gateway-i* su bili promatrani kao uređaji koji su imali kontrolu na pozivima, koristeći protokole poput H.323 i SIP i *hardware* potreban za kontrolu PSTN sučelja. Pojavom VoIP mreže bilo je potrebno nekako povezati ju s PSTN mrežom. Zbog potrebne konverzije multimedijskog sadržaja i signalizacije, *gateway* se dijeli na dva logička dijela. Prvi dio naziva se kontroler medijskog pristupnika (eng. *Media Gateway Controller* – MGC) i on sadrži samu logiku kontrole poziva. Drugi logički dio naziva se medijski pristupnik (eng. *Media Gateway*) i on služi za povezivanje VoIP mreže s PSTN-om. Tom podjelom nastalo je novo sučelje između MGC-a i MG-a, stoga je bilo potrebno definirati protokol koji bi definirao komunikaciju između ta dva logička dijela, [24].

Media Gateway Control Protocol (MGCP) standardni je protokol za rukovanje signalizacijom i upravljačkim sesijama tijekom multimedijske konferencije. Protokol definira značenje komunikacije između medijskih mrežnih pristupnika koji pretvaraju podatke iz formata koji je potreban za *circuit-switched* mreže u onaj koji je potreban za *packet-siwtched* mrežu te kontrolere medijskog mrežnog pristupnika. MGCP se može koristiti za uspostavu, održavanje i raskid poziva između više krajnjih točaka. MGCP je kreiran iz dva protokola- *Internet Protocol Device Control* (IPDC) i *Simple Gateway Control Protocol* (SGCP).

Karakteristike MGCP, [8]:

- Master / slave protokol:
  - preuzima ograničenu inteligenciju na rubu (krajnje točke) i inteligenciju u jezgri (agent poziva)
  - koristi se između call agenata i medijskih pristupnika
  - razlikuje se od SIP i H.323 koji su *peer-to-peer* protokoli.
- Surađuje s SIP-om i H.323.

4.3 Session Description Protocol (SDP)

Svrha SDP-a je prenijeti informacije o medijskom strujanju u multimedijskim sesijama kako bi primatelji sesije dobili pristup istoj. SDP se primarno koristi u *internetwork*, iako generalno gledano može opisati konferencije u drugim mrežnim okruženjima. SDP je isključivo format za opis sesije – ne uključuje transportni protokol, ali namijenjen je korištenju različitih transportnih protokola kao što su SAP, SIP, RTSP i drugi. Multimedijska je sesija definirana kao set medijskih strujanja koji postoje određeno vrijeme. Medijsko strujanje može biti s više točaka na više točaka, za vrijeme kojih sesija, koja je aktivna, ne treba biti nastavljena. *Multicast* bazirane sesije na Internetu razlikuju se od drugih formi konferencija u kojima se svi koji primaju promet mogu uključiti u sesiju (osim kad je promet sesije enkriptiran). U takvom okruženju SDP ima dvije svrhe: komunikaciju u postojećim sesijama te prijenos potrebnih informacija kako bi se omogućilo pristupanje i sudjelovanje u sesiji, [6].

SDP potreban za opisivanje multimedijskih sesija za najavu istih ili poziva u sesiju sadrži sljedeće informacije, [6]:

- naziv i svrhu sesije
- adresu i broj priključnice (eng. p*ort*)
- vrijeme početka i kraja
- informacije za zaprimanje medija
- Informacije o širini pojasa koje se koriste u konferenciji
- kontaktne informacije o osobi koja je odgovorna za sesiju.

4.4 Session Announcement Protocol (SAP)

Session Announcement Protocol (SAP) protokol je koji služi za objavljivanje nadolazećih višesmjernih konferencija i drugih multicast sesija. Koristi za definiranje formata i opisivanje informacija koje će se razmjenjivati tijekom sesije u kojoj sudjeluje više korisnika.

SAP periodički šalje obavještajni paket na poznatu multicast-adresu i port. Broj porta koji se koristi za slanje obavijesti je 9875. Da bi se objavila multicast sesija, kreator sesije šalje multicast-paket na poznatu multicast-grupu koristeći se SDP protokolom za opisivanje paketa. Općenito je implementiran u lokalne mreže. SAP sadrži mehanizme za osiguravanje integriteta najave sesije, za autentikaciju podrijetla najave i za šifriranje takvih obavijesti, [12].

5 Značajke VoIP mreže

Korisnici kako u ostalim uslugama tako i kod VoIP-a zahtijevaju određen stupanj kvalitete usluge. Neki od tih zahtjeva su: kontinuirana usluga bez gubitaka i kašnjenja te jedna od jako bitnih stavki je i sigurnost samog korisnika i njegovih informacija. U nastavku će se kroz poglavlja opisati kvaliteta usluge VoIP mreže, moguće sigurnosne prijetnje, metode zaštite od mogućih prijetnji te prednosti i nedostatci VoIP tehnologije.

5.1 Quality of service

QoS(Quality of Service) glavni je problem u implementiranju VoIP-a. Postavlja se pitanje kako jamčiti da paket za glasovnu ili drugu medijsku vezu neće zakasniti ili biti izgubljen zbog smetnji drugog prometa koji ima manji prioritet. Neki od parametara koje treba uzeti u obziru kod QoS-a jesu:

- latencija: vrijeme potrebno da se paket dostavi
- jitter: varijacije u kašnjenju isporuke paketa
- gubitak paketa: zagušenje uzrokuje odbacivanje paketa u mreži

VoIP može jamčiti visokokvalitetni prijenos govora samo ako se glasovnim paketima da prioritet nad ostalim vrstama mrežnog prometa. Da bi se VoIP implementirao tako da korisnici dobivaju prihvatljivu razinu kvalitete glasa, VoIP prometu se mora zajamčiti određena pojasna širina, latencija i *jitter*. Općenito, QoS pruža bolju mrežnu uslugu sljedećim značajkama, [21]:

- podrška namjenske širine pojasa
- poboljšanje karakteristika gubitaka
- izbjegavanje i upravljanje zagušenjima mreže
- oblikovanje mrežnog prometa
- postavljanje prioriteta prometa preko mreže.

Glasovni pozivi, bilo jedan na jedan ili konferencija, traže sljedeće, [4]:

- ≤ 150 ms jednosmjernu latenciju od usta do uha (po ITU G.114 standardu)
- Jitter od 30 ms
- ≤ 1 posto gubitak paketa
- od 17 do 106 kbps zajamčene prioritetne širine pojasa po pozivu (ovisno o brzini uzorkovanja, kodecima i *overhead-ima* drugog sloja)
- 150 bps (plus *overhead-i* drugog sloja) po telefonu zajamčene širine pojasa za glasovni promet.

Zahtjevi za videokonferenciju mogu se primijeniti kao sposobnost jedan-na-jedan ili kao konferencija s više točaka, [4]:

- ≤ 150 ms jednosmjernog kašnjenja od usta do uha (prema ITU G.114 standardu).
- Jitter od 30 ms.

- ≤ 1 posto gubitak paketa.
- garancija minimalne širine pojasa - sjednica videokonferencija plus 20 %. Na primjer, sesija videokonferencije od 384 kbps traži 460 kbps zajamčenu prioritetnu širinu pojasa.

5.2 Sigurnosne prijetnje (značajke) VoIP mreže

Voice over IP sustavi oslanjaju se na podatkovnu mrežu, što znači sigurnosne slabosti i različite vrste napada povezani s IP mrežom mogući su i u VoIP sustavima. Osiguravanje VoIP-a ima mnoge izazove koji ne postoje u javnoj telefonskoj mreži. VoIP je aplikacija koja se izvodi preko podatkovne mreže, time poprima i sve sigurnosne slabosti i mogućnosti različitih vrsta napada povezane s podatkovnom mrežom.

VoIP isto koristi IP adresiranje za lociranje ostalih korisnika na glasovnim komunikacijskim mrežama. Stoga je IP sigurnost veoma važna stavka za osiguravanje VoIP mreža, za koje se očekuje da postane okosnica svih glasovnih komunikacija u svijetu, [2].

U nastavku će se navesti neke od prijetnji koje su zajedničke IP i VoIP mrežama. Prema [2], u nastavku navest će se neke vrste mogućih prijetnji prema VoIP mrežama:

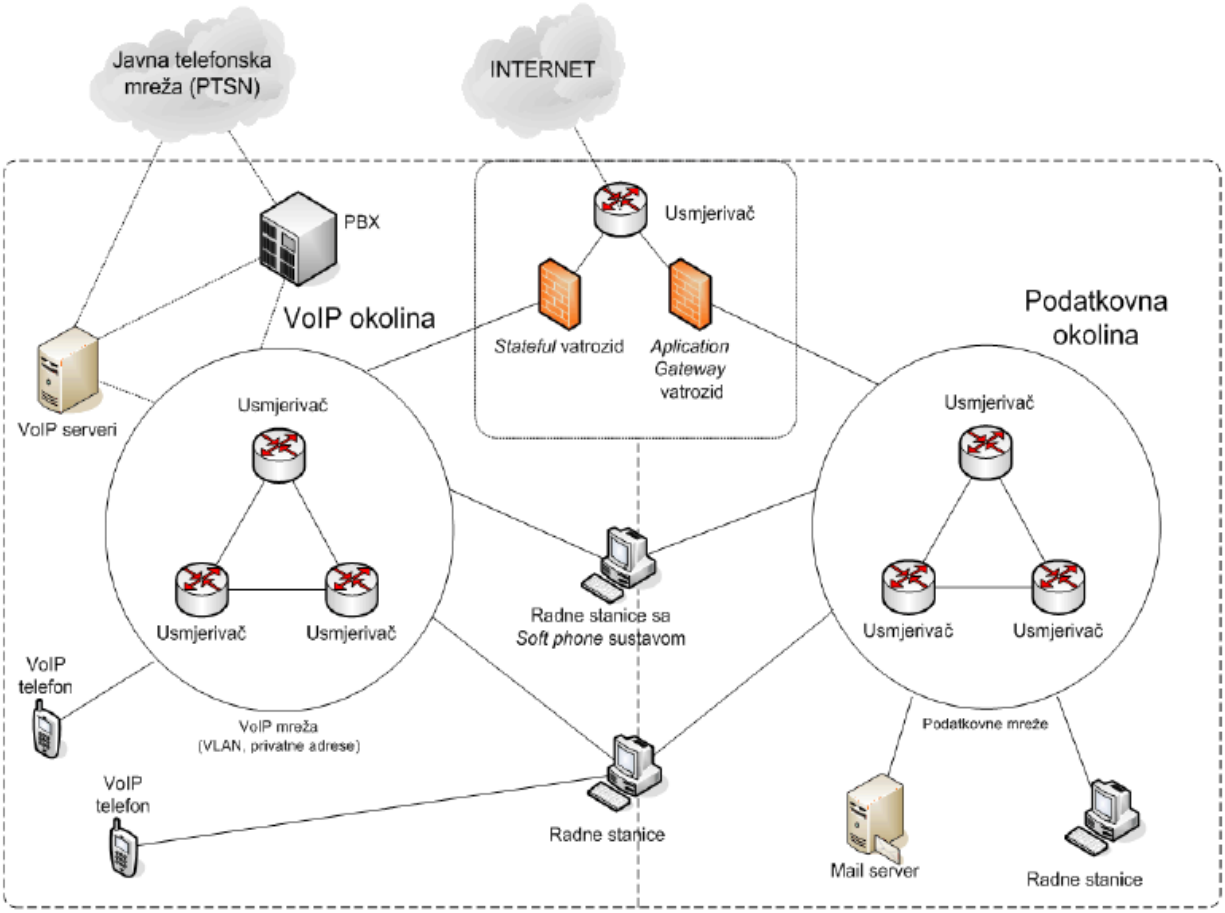
- **Neovlašteno praćenje i analiza prometa** - Neovlašteno praćenje i prisluškivanje mrežnog prometa (eng. Sniffing/Eavesdropping) može rezultirati otkrivanjem povjerljivih ili nezaštićenih korisničkih informacija, a u najgorem slučaju i krađom identiteta korisnika. Iskorištavanjem ovog propusta sofisticiranim malicioznim korisnicima omogućeno je prikupljanje informacija o VoIP mreži koje se mogu iskoristiti za napade na druge dijelove mreže (podatkovna, nadzorna …).
- **Uskraćivanje računalnih resursa** - Napadi uskraćivanja računalnih resursa (eng. Denial of Service – DoS) mogu biti zasnovani na okupiranju računalnih mreža s nepotrebnim podacima ili na rušenju pojedinih komponenti mreže. Ukoliko organizacija koristi tradicionalne komunikacijske kanale za razgovor (javna telefonska mreža) tada čak i u slučajevima kada je podatkovna mreža srušena, organizacija i dalje može komunicirati i obavljati telefonske razgovore. Ali ukoliko organizacija bazira svoje poslovanje na VoIP mreži, tada DoS napadi mogu biti veoma efikasni protiv tih organizacija. To je prvenstveno rezultat činjenice da DoS napadi ili prekidaju uslugu ili smanjuju kvalitetu postojeće usluge (eng. Quality of Sevice - QoS) za koju je nužno da bude visoka kako bi VoIP bio funkcionalan. Zbog opasnosti koju DoS napadi predstavljaju za VoIP mreže, proizvođači VoIP opreme sve češće ugrađuju u svoje proizvode različite metode zaštita od DoS napada.
- **Distribuirano uskraćivanje računalnih resursa** - Distribuirani napadi uskraćivanja računalnih resursa (eng. Distributed Denial of Service – DDoS) slični su prethodno opisanim napadima uz tu razliku što se ovi napadi ne

izvršavaju s jednog nego s većeg broja računala. Da bi maliciozni korisnik izvršio DDoS napad potrebno je da na određeni način utječe na veću skupinu računala. To se može izvesti ukoliko napadač preuzme kontrolu nad tim računalima. Ta računala mogu biti upravljana preko različitih virusa i trojanaca koji napadaču omogućavaju upravljanje računalima i zagušivanje mreže hrpom nepotrebnih podataka koji uzrokuju uskraćivanje resursa na napadnutom računalu ili mreži

- **Presretanje poziva** - Presretanje poziva (eng. call interception) omogućava nedozvoljeno nadgledanje i snimanje poziva te glasovnih poruka. Presretanjem i prisluškivanjem poziva unutar organizacija moguće je ukrasti tajne i povjerljive poslovne podatke. VoIP pozivi se mogu presretati tako da se preusmjere na neki posredni poslužitelj koji prema svojoj konfiguraciji nadzire VoIP pozive - tzv. „Man in the middle“ napad. VoIP pozivi se mogu na jednostavan način skupljati i dekodirati ukoliko napadač ima fizički pristup lokalnoj računalnoj mreži preko koje VoIP paketi putuju. Kao protumjere za ovakve napade potrebno je zaštititi fizičke pristupe mreži te implementirati enkripciju s nekom od raspoloživih metoda.
- **Krađa identiteta** - Krađom tuđeg identiteta napadač može doći do informacija potrebnih za stjecanje kontrole nad tuđim IP telefonom te preusmjeriti promet na drugu lokaciju. I ukoliko legitimni korisnik nije svjestan preusmjeravanja poziva tada on može odavati povjerljiva informacije, a da nije ni svjestan toga.
- **Financijska zlouporaba VoIP infrastrukture (eng. Call Fraud)** - Call fraud je specifičan napad za VoIP mreže koji se sastoji od nezakonitog korištenja VoIP infrastrukture za obavljanje telefonskih poziva. Takvi telefonski pozivi izgledaju kao da su pokrenuti od legitimnih korisnika unutar napadnute mreže pa se njima i naplaćuju.
- **VoIP neželjena pošta (eng. Spam over Internet Telephony - SPIT)** - Iako se nekima čini da je zatrpavanje IP telefona neželjenim SPAM porukama i informacijama samo neugodna nuspojava konekcije na Internet, većina korisnika gubi korisno vrijeme na čišćenje telefona od istih te tijekom tog vremena nisu u mogućnosti ispunjavati svoje poslovne zadatke. Kako se sve više poslovnih korisnika odlučuje za VoIP komunikacije, VoIP neželjena pošta ima sve veću i veću tendenciju širenja i sve veću populaciju kojoj je namijenjena.

5.3 Načini zaštite VoIP mreže

Kako bi se VoIP sustavi zaštitili od mogućih napada, potrebno je stalno raditi na sigurnosti. U nastavku, prema prijedlozima CARNet-a, navedeni su načini zaštite kojima se minimaliziraju sigurnosni rizici i prijetnje unutar VoIP mreža. Na slici 5. može se vidjeti logička shema VoIP sigurnosne arhitekture.



Slika 5. Logička shema VoIP sigurnosne arhitekture, [2]

Prema [2] preporučene metode zaštite VoIP mreže od različitih prijetnji razrađene su u sljedećim poglavljima.

5.3.1 Fizička zaštita

Preporuke za fizičku sigurnost i konfiguraciju VoIP aplikacija - Promatrano s aspekta fizičke sigurnosti i konfiguriranja samih VoIP aplikacija preporučaju se sljedeće metode, [2]:

- sve kritične VoIP mrežne i poslužiteljske komponente trebalo bi locirati u zaštićene i sigurne lokacije odvojene od neovlaštenog pristupa;
- IP telefone bi trebalo konfigurirati tako da ne prikazuju svoje mrežne konfiguracijske informacije;

- tzv. *Soft Phone* sustavi, koji provode VoIP komunikaciju pomoću običnog računala, slušalicai specijalnog programa, trebalo bi izbjegavati.

5.3.2 Odvajanje IP adresa

Preporuke za VoIP komponente - sve VoIP komponente bi trebalo postaviti na odvojene privatne mreže, koristile bi se privatne IP adrese za odvajanje IP telefonije od podatkovnih mreža. Kada su potrebne mrežne konekcije između VoIP i ostalih podatkovnih mreža potrebno je implementirati NAT koji prevodi javne IP adrese u privatne te time interna računala odvaja od vanjske mreže. NAT bi trebalo implementirati na dodirnim točkama VoIP i ostalih mreža. Tako je pružena dodatna sigurnost od malicioznih korisnika koji neće biti u mogućnosti skeniranja VoIP mreža u potrazi za mogućim sigurnosnim propustima, osim kada NAT nije pravilno konfiguriran, [2].

5.3.3 Virtualni LAN-ovi

Preporuča se odvajanje VoIP-a od ostalih podatkovnih mreža korištenjem virtualnih lokalnih mreža (eng. *Virtual Local Area Networks - VLAN*). Tehnologija virtualnih LAN-ova omogućuje logičko grupiranje korisnika, neovisno o njihovoj fizičkoj lokaciji, u manje logičke cjeline, tzv. Virtualne lokalne računalne mreže (VLAN). Ovakvim pristupom moguće je unutar jednog fizičkog LAN-a kreirati nekoliko manjih, međusobno odvojenih virtualnih LAN-ova, od kojih svaki zadržava svojstva klasične računalne mreže.

Grupiranje korisnika moguće je realizirati prema različitim kriterijima kao što su MAC adrese mrežnih kartica, IP adrese, portovi preklopnika, itd. Svaki virtualni LAN predstavlja jednu *broadcast* domenu, a komunikaciju između pojedinih VLAN-ova moguće je kontrolirati. U preklapanim mrežama VLAN-ovi ostvaruju logičko segmentiranje i odvajanje i time dodatno povećavaju performanse i sigurnost mreže.

Odvajanje VoIP mreža od ostalih podatkovnih mreža služi za umanjivanje opasnosti od DoS napada i prisluškivanje paketa iz podatkovnih mreža. Uz to, odvajanjem podatkovnih i VoIP mreža smanjuje se “natjecanje“ za mrežnim resursima i samim time smanjuje se vrijeme kašnjenja za prijenosne servise. Kako je VoIP jako osjetljiv na vrijeme kašnjenja, ovakav segmentni pristup je jedan od najjeftinijih načina poboljšavanja performans postojeće mrežne infrastrukture, [2].

5.3.4 Vatrozidi

Najbolji način za osiguravanje VoIP usluge jest filtriranje prometa između VoIP mreža i podatkovnih mreža korištenjem vatrozida (eng. firewalls). Vatrozid je sustav (programski ili sklopovski) čija je osnovna uloga filtriranje dolaznog i odlaznog mrežnog prometa organizacije. Svoju osnovnu zadaću vatrozid obavlja putem sigurnosnih pravila koja definiraju koji je promet dopušten, a koji zabranjen u skladu

sa sigurnosnom politikom organizacije. Jedan od nedostataka vatozidne zaštite je taj što se nakon definicije pravila filtriranja ona više ne mijenjaju, ili se moraju mijenjati ručno. Nažalost, zbog specifičnosti VoIP-a koji za normalan rad zahtjeva korištenje velikog raspona otvorenih portova (protokol koji se koristi za prijenos VoIP podataka koristi raspon portova od 10024 do 65535 za transportiranje paketa), potrebno je koristiti vatrozide koji direktno podržavaju SIP i H.323 protokole, [2].

5.3.5 Enkripcija

Gdje god je moguće i gdje je izvedivo trebala bi se implementirati enkripcija VoIP prometa korištenjem VPN-ova (eng. Virtual Private Networks) ili bilo kojom metodom trenutno dostupnom. Virtualne privatne mreže (tzv. enkripcijski tuneli) omogućavaju sigurno spajanje dvije fizički odvojene mreže preko Interneta bez izlaganja podataka neautoriziranim korisnicima. Nakon što je jednom uspješno uspostavljena, virtualna privatna mreža je zaštićena od neovlaštenih iskorištenja sve dok su enkripcijske tehnike sigurne.

Koncept VPN-a omogućava udaljenim korisnicima na nezaštićenoj strani direktno adresiranje računala unutar lokalne mreže, što drugim korisnicima nije moguće zbog NAT-a i filtriranja paketa. Kako bi udaljeni korisnici uspješno prošli fazu spajanja na lokalnu mrežu potrebno je uspješno obaviti autentifikaciju istih. Ta autentifikacija mora biti kriptirana u svrhu sprečavanja krađe podataka od strane napadača i iskorištenja istih. Za svaki udaljeni nadzor i udaljeni pristup VoIP komponentama preporuča se korištenje IPsec ili SSH (eng. Secure Shell) protokola. Također, svugdje gdje je moguće, preporuča se korištenje IPsec tuneliranja umjesto IPsec transporta iz razloga što tuneliranje maskira odredišnu i izvorišnu IP adresu, [2].

5.4 Prednosti i nedostatci

Prednosti:

- Jedna od najvažnijih prednosti su smanjeni troškovi u odnosu na tradicionalne telefonske usluge. Korištenjem besplatnih *software-a* cijena je ograničena na cijenu lokalnog davatelja internetskih usluga.
- Mogućnost integriranja s postojećom telefonskom vezom.
- Obično dolazi s besplatnim značajkama kao što ID pozivatelja s imenom, poziv na čekanje, konferencijski pozivi, prosljeđivanje poziva, koje se kod tradicionalnih dodatno naplaćuje.
- VoIP uslugu je moguće koristiti bilo gdje ukoliko postoji širokopojasna veza bez obzira na lokaciju i udaljenost.
- Tradicionalni pozivi imaju tek nekoliko dodatnih funkcija koje se obično dodatno plaćaju. Dok VoIP ima veliki izbor dodatnih funkcija kao što su: prosljeđivanje poziva, govorna pošta, ID pozivatelja, mogućnost više sudionika u pozivu
- Mogućnost slanja dokumenata, slika i ostalog sadržaja tijekom poziva.

Nedostatci:

- Potrebna je internetska veza za rad.
- U slučaju nestanka struje nije moguće uspostaviti poziv.
- Na kvalitetu poziva utječe kvaliteta širokopojasne veze i performanse vašeg računala. Loša internetska veza i zagušenje mogu rezultirati lošom kvalitetom usluge.
- Sigurnost je glavni problem za VoIP. Najznačanija sigurnosna pitanja vezana uz VoIP su krađa identiteta, virusi, uskraćivanje usluga, *spam* i drugi.

6 Interoperabilnost VoIP s ostalim mrežama

Uvođenje VoIP-a traži hibridnu integraciju PSTN-a i Interneta. Postoje tri ključna okruženja. Općenito se navode kao VoIP okruženja i mogu se navesti kao:

- okruženje u kojem je poziv započeo i završio u PSTN-u koji koristi IP mrežu i njene protokole
- okruženje u kojem je poziv započeo u PSTN mreži i završava na internetu, i obrnuto.

Uzevši u obzir navedena okruženja, rješenje interoperabilnosti nalazi se u adresiranju. Na primjer, dvije ključne sheme adresiranja E.164 za PSTN i IPv4 za Internet moraju na neki način komunicirati. Zbog opsežne implementacije SS7 za PSTN, SS7 (eng. Sygnaling System no. 7) adresiranje i protokoli moraju također komunicirati. Prijenos broja još jedan je važan čimbenik koji treba uzeti u obzir. Sve ovo mora funkcionirati bez prekida funkcionalnosti usluge i prekomjernog utjecaja na zahtjeve za kvalitetu usluge (QoS).

Razvoj privatnog IP adresiranja u rezidencijalnom i poslovnom poduzeću gdje se koristi NAT (eng. Network Address Translation)/NAPT(eng. Network Address and Port Translation) funkcionalnost, donosi praktičnu nužnost za rad VoIP sustava, u takvom okruženju VoIP uređaji iza privatnog IP adresnog sučelja i javne Internet mreže mogu međusobno komunicirati. Prelaskom na „all-IP“ mrežu za VoIP i Internet usluge mogli bi se riješiti ili smanjiti brojni problemi vezani uz interoperabilnost.

Za usmjeravanja poziva za POTS usluge (eng. Plain old telephone Service), gdje je Internet dio poziva, potrebno je poznavati osnove funkcioniranja usmjeravanja poziva. UNI (eng. User-To-Network Interface) u slučaju telefonske usluge pruža sljedeće funkcije: kada korisnik podigne slušalicu, telefonska centrala prepoznaje da je slušalica podignuta i šalje korisniku ton kojim mu daje do znanja da može birati broj za uspostavu; ako centrala uspješno postavi poziv, korisnik će čuti zvuk zvonjenja; kada osoba na drugoj strani podigne slušalicu, poziv se uspostavlja i UNI prenosi glasovni analogni signal u telefonsku centralu gdje se pretvara u oblik pogodan za prijenos mrežom. Spuštanjem slušalice od bilo koje strane završava poziv. Za zamjenu analognog UNI segmenta s različitim tehnologijama potrebno je uzeti u obzir sljedeće aspekte:

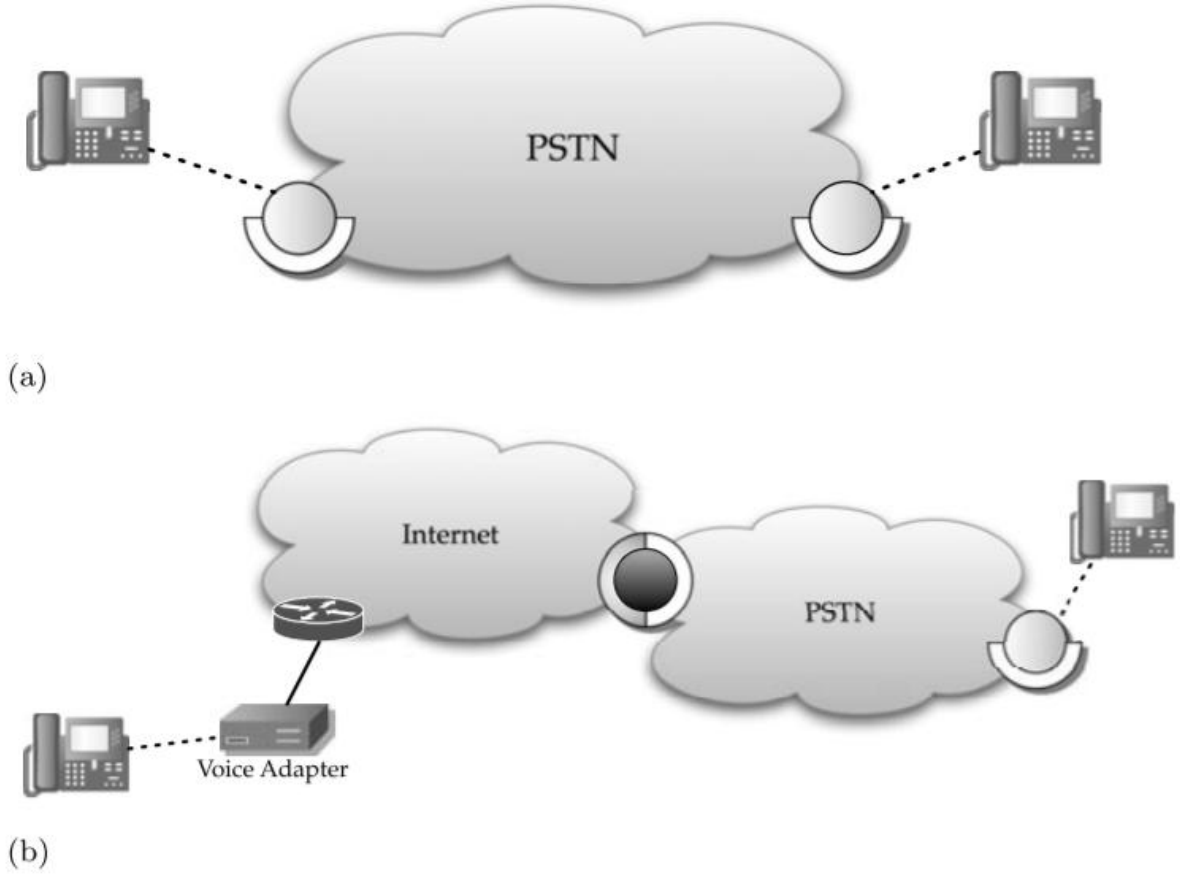
- zamjena direktne linije s indirektnim modom mrežnog povezivanja
- prelazak komunikacijskog moda u oblik paketnog prijenosa informacija.

Da bi se to omogućilo, nužno je da krajnji korisnik i telefonska centrala imaju odgovarajuće adaptere kako bi osnovne i dodatne funkcije za UNI i dalje bile moguće. Uz pretpostavku da se koristi ITU-T Q.931 protokol, koji pruža osnovnu kontrolu poziva za pristup signalizaciji, PSTN će i dalje koristiti SS7 za signalizaciju unutar PSTN mreže.[1]

[1] D. Medhi; K. Ramasamy: Network Routing Algorithms Protocols and Architectures; Str 663.-664.

Ako UNI postaje IP mreža i ako se za UNI signaliziranje poziva želi koristiti Q.931, onda VoIP adapteri moraju podržavati funkcionalnost kreiranja Q.931 paketa koji se prenose preko IP mreže.

Da bi se povezala PSTN mreža s UNI-jem, središnji ured mora imati medijsko-signalizacijski gateway koji ima sposobnost komunikacije s VoIP adapterima za razmjenu glasovnih poruka i paketizirane glasovne pakete. Ova funkcija gatewaya može biti fizički integrirana s centralnim uredskim preklopnikom ili može biti odvojeni poslužitelj koji koristi mod komutacije kanala za komunikaciju s telefonskom centralom. U ovom okruženju upravljanje pozivima ostvaruje se putem telefonske centrale kroz *gateway*. Treba uzeti u obzir da *gateway* treba imati sučelje bazirano na IP-u kako bi mogao primati i tumačiti pakirane poruke Q.931. Mora imati sučelje koje može razgovarati s telefonskom centralom za korištenje SS7 poruka. Zauzvrat *gateway* bi trebao generirati Q.931 poruke za slanje prema VoIP adapterima preko IP mreže. Ovo sve omogućuje telefonima spajanje na PSTN.[2]

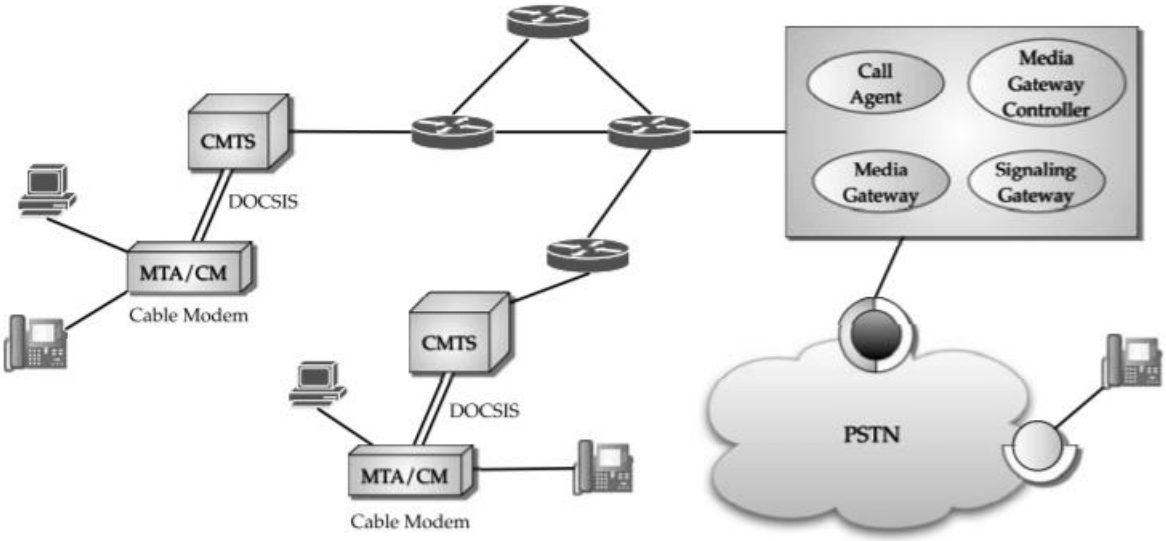


Slika 6. Promjena u pristupnoj tehnologiji (UNI) u telefoniji: (a) tradicionalni (b) ugradnja IP mreže, [1]

[2] D. Medhi; K. Ramasamy: Network Routing Algorithms Protocols and Architectures; Str 665

6.1 Interoperabilnost s nepokretnom mrežom

U slučaju interoperabilnosti s nepokretnom mrežom, onda davatelj usluge daje pretplatniku adapter, ali je potrebno korisnika prvo locirati po poštanskoj adresi. Povezivanje VoIP telefona pomoću RJ-11 priključka i RJ-45 priključak za povezivanje računala omogućeno je pomoću ugrađenog eMTA (eng. Embedded Multimedia Terminal Adapter).



Slika 7. Konceptualna arhitektura za kabelsku IP mrežu za telefoniranje, [1]

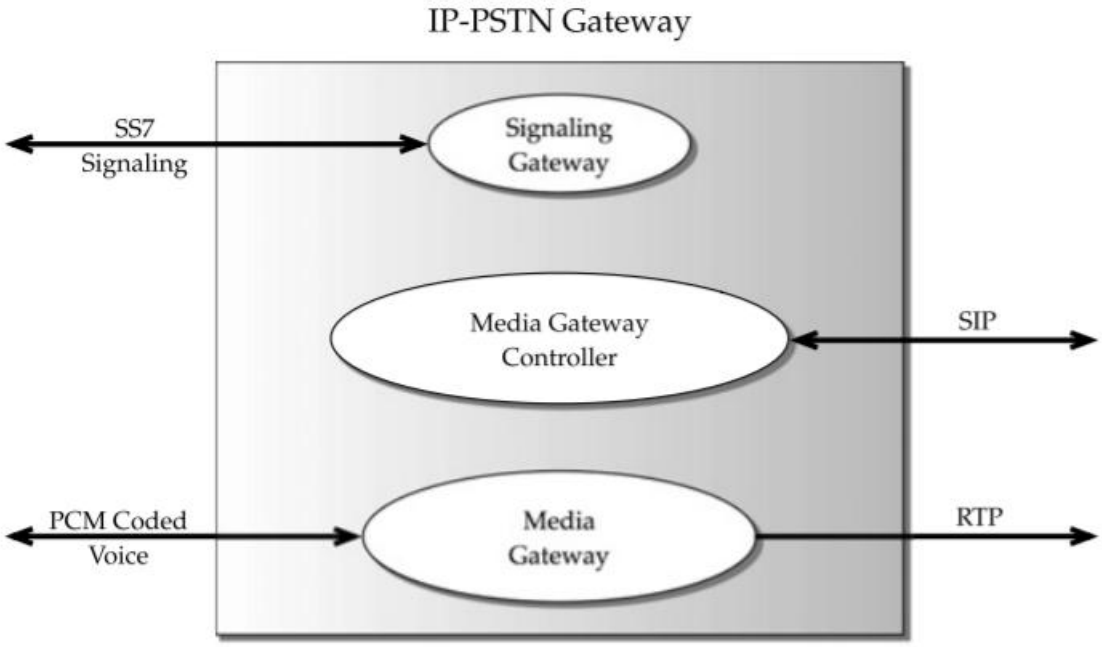
U slučaju kao na slici 3. IP umrežavanje na korisnikovoj strani koristi infrastrukturu koja pripada pružatelju usluge putem modemske usluge. Korisnik preko modema ima IP pristup, što znači da je eMTA spojena na kabelsku liniju. Kabelski modem vidljiv je CMTS-u (eng. *Cable Modem Termination System*) uz korištenje DOCSIS protokola (eng. *Data over cable service Interface Specification*). CMTS je primarno slojni uređaj koji se može integrirati s ruterom na trećem sloju za IP komunikaciju. Od eMTA-e na korisnikovoj strani do call manager servera cijelo je IP umrežavanje u nadležnosti davatelja usluge, što formira upravljivi IP backbone. PacketCable specifikacija traži da svaka krajnja točka ima potpuno kvalificiranu domenu. S obzirom da mobilnost nije moguće, zaključuje se, da se svaki telefonski broj povezuje sa statičnom IP adresom.

Stvarna mrežna arhitektura može biti sasvim drugačija ovisno o fizičkoj domeni pružatelja CNP-a (eng*. Cable Network Provider*). Na primjer, ako je usluga pružatelja CNP-a ograničena na geografsku lokaciju, kao što je gradsko područje, izlazna točka na PSTN može biti na jednom mjestu. Treba uzeti u obzir opciju usmjeravanja poziva iz jednog geografskog područja do drugog geografskog područja, ulazak u PSTN mrežu pa izlaska u drugu lokaciju te natrag u kabelsku mrežu. To bi bilo poželjno radi smanjenja troškova i ostalih poslovnih razloga. U ovom scenariju pružatelj usluga imat će funkcije upravljanja pozivima u različitim geografskim lokacijama, ovisno o broju koji je pretplatnik zvao. Stvarna izlazna točka iz mreže može biti drugačija. U tom bi slučaju pružatelj kabelske usluge trebao

pružati *high-bandwidth* krugove kao što su OC-3 (eng. *Optical Carrier Level*) za konekciju između različitih MAN mreža kako bi se uspostavila IP mreža.

Za scenarij u kojem poziv započinje u PSTN mreži i završava u IP mreži, gdje nisu oba krajnja uređaja analogni telefoni, za stvarnovremene *Two-way* aplikacije za multimediju i telefoniju razvijen je SIP protokol u IP okruženju. SIP protokol upravlja samo aspektom kontrole sesije poziva, dok je medij za poziv paketiziran i obrađen korištenjem RTP-a (eng. *Real-Time Transport Protocol*). SIP protokol se može koristiti u *end-to-end* metodi od jednog krajnjeg uređaja do drugog te ne traži zasebne protokole za mrežni dio.[3]

Vrlo važnu ulogu u radu ima *gateway* koji se sastoji od triju komponenata: MGC (eng. *Media Gateway Controller*), SG (eng. *Signaling Gateway*) i MG (eng. *Media Gateway*). SG prima SS7 ISUP poruke od PSTN-a i prosljeđuje ih MGC-u te se poruke zatim pretvaraju u SIP ekvivalentne poruke i za prijenos IP mrežom. Slično radi i MGC koji prima SIP poruke te se one prenose prema SG-u za generiranje ekvivalentnih SS7 ISUP poruka za odašiljanje preko PSTN-a. Uloga je MGC-a kontrola *audiostreamova* preko pulsno kodne modulacije na strani PSTN-a i pomoću RTP-a na IP strani. *Gateway* mora djelovati i obavijestiti pristupnika medija u vezi s rukovanjem medijem, ovisno o statusu poziva, kao što je uspostavljanje ili otpuštanje. *Gateway* je mozak u ovom sustavu i potreban je za održavanje stanja i prijevoda za različite veze.[4]



Slika 8. Gateway između PSTN i IP mreže, [1]

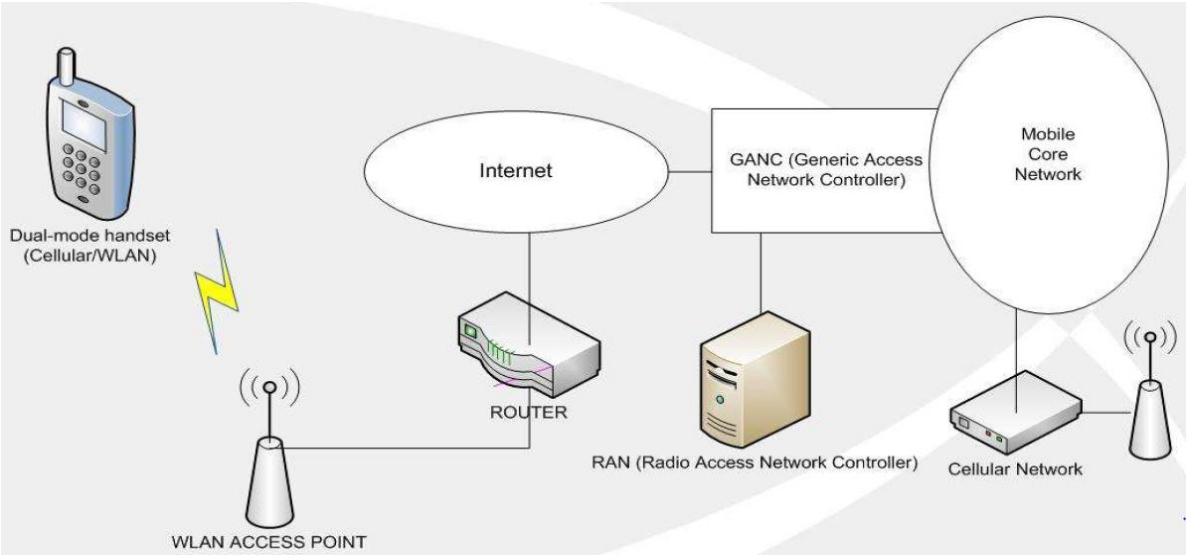
[3] Ibid, Str 675.
[4] Ibid, Str 676.

6.2 Interoperabilnost s pokretnom mrežom

Fiksna mobilna konvergencija (eng. *Fixed-Mobile Convergence* - FMC*)* predstavlja prijelazno razdolje u telekomunikacijskoj industriji kojom će se ukloniti razlika između fiksnih i mobilnih mreža. 3GPP prvi je standard koji je podržavao FMC.

IP multimedijski sustav (eng. *IP Multimedia Subsystem* – IMS) i multimedijska domena (eng. Multimedia Domain) su 3GPP i 3GPP2 verzije istih stvari, tj. IP i SIP standardi definirani za obradu multimedijskih signala u bežičnoj domeni. IMS podržava komunikaciju između SIP korisničkih agenata koji pristupaju IP mreži i različitih SIP poslužitelja unutar mreže, koristeći pristupne usluge 3GPP i 3GPP2 sustava podatkovne mreže temeljene na paketnom prijenosu, [22].

FMC rješenja koja omogućuju rad preko Wi-Fi i mobilne pristupne mreže nazivaju se *dual-mode* rješenja. *Dual-mode* rješenje mogu se temeljiti na različitim tehnologijama. Najistaknutija su dva standardna pristupa: jedan se temelji na IMS-u; drugi se temelji na UMA/GAN, koji je definiran za GSM stanične sustave (eng. GSM cellular systems). Oba pristupa učinkovito konvergiraju zičani i mobilni VoIP preko Wi-Fi/širokopojasne mreže „skrivanjem“ Wi-Fi access media i signaliziranjem iz jezgre čelijske mreže (eng. Cellular core network). IMS omogućuje konvergenciju u višim slojevima. Za razliku od IMS-a, UMA/GAN standard omogućuje podršku Wi-FI infrastrukture na način da izgleda kao skup GSM baznih stanica, čime se Wi-Fi prikazuje kao još jedno 3GPP radijsko sučelje i zahtijeva da sav promet prođe kroz jezgu 3GPP-a, [22]. Slika 9. prikazuje pojednostavljen prikaz arhitekture za podržavanje fiksne mobilne konvergencije.



Slika 9. Ahitektura za podržavanje fiksne mobilne konvergencije, [23]

Osnovni elemetni koji su potrebni za interoperabilnost VoIP mreže s mobilnom mrežom jesu: *dual-mode handset, Radio Access Network Controller i Generic Access Network Controller* te će isti biti ukratko objašnjeni u nastavku.

Dual-mode handset su mobilni uređaji koji koriste više tehnika za prijenos i preuzimanje glasovnih i podatkovnih informacija. Ovi *dual-mode* mobilni uređaji kompatibilni su s GSM i CDMA mrežama te koriste sofisticiranu tehnologiju za prijenos poziva između tenologija.

Radio Access Network Controller (RAN) predstavlja uređaj koji se nalazi između uređaja kao što su mobilni telefoni i računala te omogućuje povezivanje tih uređaja na jezgrenu mrežu. Neke vrste RAN: GSM *radio access network*, UMTS *radio access network*.

Generic Access Network (GAN) proširuje mobilne glasovne, podatkovne i multimedijske aplikacije preko IP mreže. GAN omogućuje paketima prosljeđivanje na mrežnu pristupnu točku preko interneta, a ne preko GSM-a, UMTS-a i sl. GAN se koristi kako bi se omogućilo mobilnih telefonima za povezivanje poziva putem Wi-Fi mreže. Zasebni uređaj GAN kontroler (eng. GAN controller) prima podatke s interneta i šalje ih u mobilnu mrežu telefona kao da dolaze iz mobilne antene, [25].

7 Zaključak

U posljednjem desetljeću tehnologija se jako brzo razvijala, pogotovo u telekomunikacijama. Potreba za komunikacijom dovela je do razvoja prvih telefonskih sustava. Prvi telefonski sustavi bili su vrlo ograničeni. Same centrale nisu bile automatizirane, već su zaposlenici bili zaduženi za prospajanje poziva.

Kasnijim dolaskom modernijih telefonskih sustava i pojavom interneta, ljudi su htjeli osim glasa prenositi i različite vrste informacija kao što su tekst, slike, video zapisa i dr. No svi ti sustavi su bili posebne cjeline, te ih je bilo potrebno nekako povezati da bi različite tehnologije mogle međusobno komunicirati.

VoIP je tehnologija koja omogućuje prijenos glasa korištenjem IP mreže. Međutim, VoIP sustavi ne bi postojali bez tri jako bitne inovacije: telefona, Interneta i najbitnijeg IP protokola (eng. *Internet Protocol*). Za razliku od tradicionalne mreže, kod VoIP-a glas se prenosi u digitalnom obliku u IP paketima kroz IP mrežu. Za kvalitetu usluge brinu se protokoli za prijenos glasa, a za upravljanje pozivima, uspostavom i prekidanjem zaduženi su signalizacijski protokoli.

Kvalitetu usluge koju VoIP mora pužiti korisnicima mora biti jednaka ili bolja od one koju pruža telefonska mreža da bi postao dostojna zamjena tradicionalnim telefonima. Zbog povezanosti s IP mrežom, VoIP je podložan raznim prijetnjama i napadima. Stoga je osim fizičke zaštite VoIP mrežnih komponenti, potrebno provesti i metode zaštite kojima bi se korisnici VoIP usluga zaštitili od zlonamjernih djelovanja koji im mogu osobno naštetiti ili onemogućiti pristup usluzi.

Interoperabilnost je omogućila komunikaciju između različitih komunikacijskih tehnologija, time danas zastarjele tehnologije nije bilo potrebno uklanjati nego se nadogradnjom postojeće infrastrukture postigao željeni cilj.

Popis kratica

CNAME	Canonical Name
CNP	Cable Network Provider
eMTA	Embedded Multimedia Terminal Adapter
FMC	Fixed-Mobile Convergence
GAN	Generic Access Network
GANC	Generic Access Network Controller
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet protocol
ITU-T	ITU Telecommunication Standardization Sector
NAT	Network Address Translation
NAPT	Network Address and Port Translation
MC	Multi-point Controler
MCU	Multi-point Control Unit
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
POTS	Plain old telephone Service
RAN	Radio Access Network Controller
RR	Receiver report
RSVP	Resource reservation Protocol
RTC	Real-Time Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real-Time Streaming Protocol
SDES	Source description items
SG	Signaling Gateway
SR	Sender report
UNI	User-To-Network Interface
VoIP	Voice over Internet Protocol

Literatura

[1] Medhi D, Ramasamy K. Network Routing Algorithms Protocols and Architectures, Elsevier Inc ., San Francisco, California, 2007. [Pristupljeno: kolovoz 2018.]

[2] Sigurnosni aspekti VoIP tehnologije. Preuzeto sa: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-03-151.pdf [Pristupljeno: kolovoz 2018.]

[3] Security Issues and Countermeasure for VoIP. [Online]: https://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701 [Pristupljeno: kolovoz 2018.]

[4] Implementing Quality of Service Over Cisco MPLS VPNs. [Online]: http://www.ciscopress.com/articles/article.asp?p=471096&seqNum=6 [Pristupljeno: kolovoz 2018.]

[5] Quality of Service Design Overview. [Online]: http://www.ciscopress.com/articles/article.asp?p=357102 [Pristupljeno: kolovoz 2018.]

[6] SDP: Session Description Protocol. [Online]: http://www.rfc-editor.org/in-notes/rfc2327.txt [Pristupljeno: kolovoz 2018.]

[7] RTP: A Transport Protocol for Real-Time Applications. [Online]: https://tools.ietf.org/html/rfc3550 [Pristupljeno: lipanj 2018.]

[8] Media Gateway Control Protocol (MGCP). [Online]: https://tools.ietf.org/html/rfc3435 [Pristupljeno: rujan 2018.]

[9] VoIP Security Vulnerabilities. Preuzeto sa: https://www.sans.org/reading-room/whitepapers/voip/voip-security vulnerabilities-2036 [Pristupljeno: kolovoz 2018.]

[10] The H.323 Sandard. [Online]: https://msdn.microsoft.com/en-us/library/ms709083(v=vs.85).aspx [Pristupljeno: kolovoz 2018.]

[11] VoIP Fundamentals (Introducing Voice over IP Networks) Part 1. [Online]: http://what-when-how.com/cisco-voice-over-ip-cvoice/voip-fundamentals-introducing-voice-over-ip-networks-part-1/ [Pristupljeno: kolovoz 2018.]

[12] Voice over IP: Protocols and Standards. [Online]: https://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/ [Pristupljeno: lipanj 2018.]

[13] Integrate VoIP with your existing network. Preuzeto sa: https://telephone-systems.com.au/images/pdf/voip.pdf [Pristupljeno: kolovoz 2018.]

[14] The Use of RSVP with IETF Integrated Services. [Online]: https://tools.ietf.org/html/rfc2210 [Pristupljeno: lipanj 2018.]

[15] Resource ReSerVation Protocol (RSVP). [Online]: https://tools.ietf.org/html/rfc2205 [Pristupljeno: lipanj 2018.]

[16] http://www.ericsson.hr/etk/revija/Br_1_2001/govor_slike/3.jpg [Pristupljeno: kolovoz 2018.]

[17] VoIP Signaling Protocols. [Online]: https://www.pluralsight.com/blog/it-ops/voip-signaling-protocols [Pristupljeno: kolovoz 2018.]
[18] Evolucija telefonskih sustava. Preuzeto sa: http://arhiva.ericsson.hr:8080/etk/revija/Br_2_2004/evolucija_tel_sustava.pdf [Pristupljeno: kolovoz 2018.]
[19] Top Ten Security Issues Voice over IP (VoIP). Preuzeto sa: https://www.scribd.com/document/246746404/Top-Ten-Voip-Security-Issue [Pristupljeno: kolovoz 2018.]
[20] Quality of Service for Voice over IP. Preuzeto sa: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.pdf [Pristupljeno: kolovoz 2018.]
[21] Peraković D, Periša M, Šraić S, Forenbacher I,: Autorizirana predavanja iz kolegija Arhitektura telekomunikacijske mreže: Arhitektura multimedijskih mreža. [Online]: http://estudent.fpz.hr/Predmeti/A/Arhitektura_telekomunikacijske_mreze/Materijali/6_Arhitektura_multimedijskih_mreza_-_10112016.pdf [Pristupljeno: rujan 2018.]
[22] Fixed mobile convergence technology. [Online]: fundamentalshttps://searchunifiedcommunications.techtarget.com/feature/Fixed-mobile-convergence-technology-fundamentals#B [Pristupljeno: rujan 2018.]
[23] Wireless Local Area Networks in Fixed Mobile Convergence. [Online]: http://trends-in-telecoms.blogspot.com/2011/06/wireless-local-area-networks-in-fixed.html [Pristupljeno: rujan 2018.]
[24] Use of MEGACO vis-à-vis MGCP to build a Gateway Solution. [Online]: https://hive1.hive.packetizer.com/users/packetizer/papers/ipmc/MEGACOvsMGCP_v3.pdf [Pristupljeno: rujan 2018.]
[25] Fixed-Mobile Convergence. [Online]: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR07/discussion_papers/fixedmobileconvergence.pdf [Pristupljeno: rujan 2018.]

Popis fotografija

Slika 1. VoIP arhitektura 5
Slika 2. Protokolarna arhitektura VoIP-a 6
Slika 3. H.323 komponente 12
Slika 4. SIP komponente 14
Slika 5. Logička shema VoIP sigurnosne arhitekture 20
Slika 6. Promjena u pristupnoj tehnologiji (UNI) u telefoniji: (a) tradicionalni (b) ugradnja IP mreže 25
Slika 7. Konceptualna arhitektura za kabelsku IP mrežu za telefoniranje 26
Slika 8. Gateway između PSTN i IP mreže 27
Slika *9*. Ahitektura za podržavanje fiksne mobilne konvergencije 28

Popis tablica

Tablica 1.H.323 i SIP usporedba 14