

PROJEKTOVANJE VoIP MREŽE

Projekat : Nacionalne banke

Beograd,
Septembar 2007.

Petar Bojović

Sadržaj

<i>Uvod</i>	3
<i>VoIP</i>	4
<i>Centralno-distribuirani sistem za IP telefoniju</i>	12
<i>QoS</i>	13
<i>DSCP</i>	15
<i>Bandwith menadžment</i>	17
<i>Kontrola poziva</i>	18
<i>Dial Plan</i>	20
<i>Oprema</i>	22

➤ Uvod

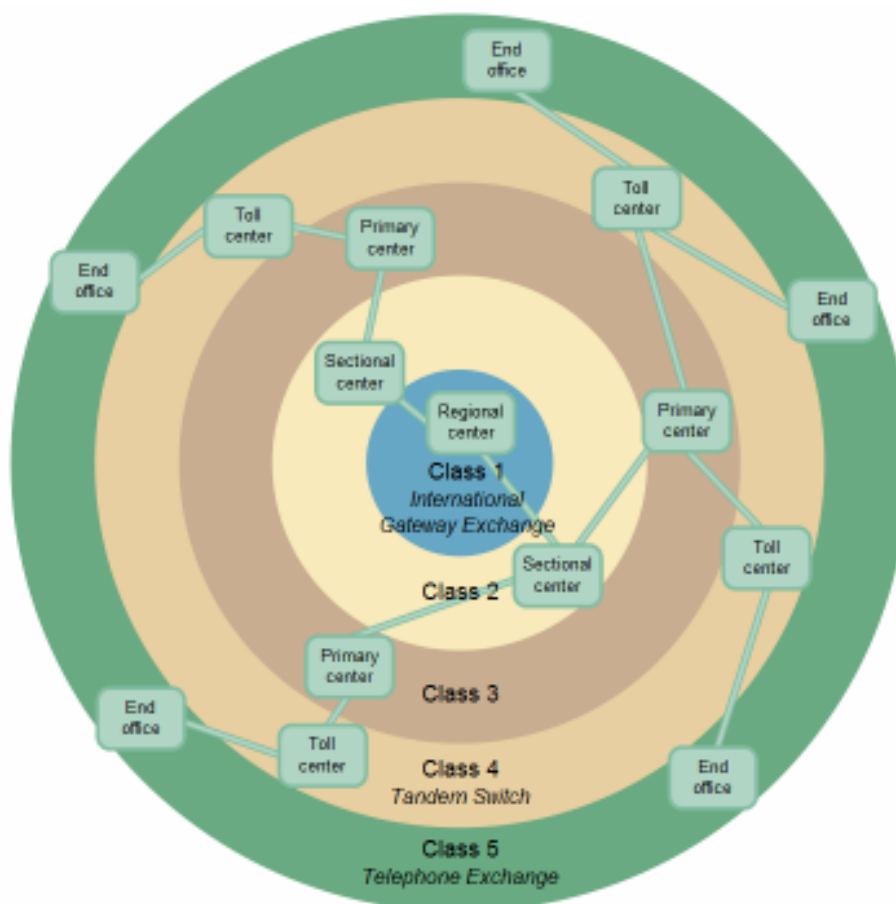
Telefonija predstavlja glavni vid komunikacije ljudi elektronskim putem. Aktuelna tehnologija prenosa glasa – fiksna telefonija – sad već predstavlja zastareo sistem prenosa glasa.

Fiksna telefonija – telefonija koju Telekom već dugo nudi kao uslugu, funkcioniše po principu (circuit switched) komutiranih kola. Tako, kada želimo da uspostavimo vezu sa udaljenom lokacijom, zazimalo ceo link do telefonske centrale, zatim rezervišemo sve linkove do krajnje centrale, i do korisnika kog pozivamo. Kako smo zauzeli po jedan link između svih centrala koje koristimo, drugi korisnici ne mogu koristiti taj link za svoje potrebe.

Analizom se došlo do rezultata da u razgovoru, preko 60 % vremena postoji ćutanje (tišina, ne prenosi se glas), došlo se do zaključka da je iskoristljivost takvog linka maksimum do 40 %.

Zbog nemogućnosti da isti link koriste više korisnika, korišćenje zauzetog linka, njegova cena, pada na pojedinca koji koristi link. To je glavni razlog za visoku cenu razgovora između dve udaljene lokacije.

Ako saberemo ova dva parametra; visoka cena korišćenja linka, i mala efektivna iskoristljivost; dolazimo do zaključka da je ova tehnologija prenosa glasa, vrlo nepovoljna, kako za kranje korisnike, zbog visoke cene korišćenja, tako i za pružaoce ove usluge, zbog skupe opreme.



Primer hijerarhije telefonskih centrala u fiksnoj telefoniji

➤ VoIP

Prihvatanjem TCP/IP protokola kao standard računarskih mreža sposoban da povezuje velike i male mreže u jednu celinu, popularno nazvanu internet, otvarala se nova mogućnost korišćenja postojećih linkova i drugih resursa.

Američki provajder ARPANET, začetnik Internet mreže, je prvi provajder koji je počeo eksperimente na polju prenošenja glasa preko IP mreža, još 1973. godine.

Korišćenjem TCP/IP protokola, koji je paket switched tehnologija prenosa, mogu se rešiti dva najveća problema koja se javljaju kod tehnologija sa komutiranim kolima. Tehnologija Voice over IP (VoIP), se bazira na TCP/IP modelu prenosa podataka. Glas se prvo digitalizuje različitim metodama, u zavisnosti od potrebe za kvalitetom. Zatim se pakuje naprednim algoritmima za kodiranje, korišćenjem nekih od kodeka.

Tako kodiran paket se secka na dosta malih paketa, veličina paketa zavisi od kodeka i protokola koji se koristi za slanje paketa, (SIP G711 ~ 160 bajta na svakih 20 milisekundi). Mali paketi se korišćenjem RTP (Real-time Transport Protokol) protokola šalju drugoj strani, korišćenjem UDP način prenosa. Prijemna strana može biti krajnji korisnik, ili gateway koji treba da prosledi ili na neki način konvertuje te pakete i uruči glas krajnjem korisniku. Kada paket pristigne, on se momentalno dekodira i reprodukuje.

Glavna prednost VoIP sistema je to što jedan poziv, nikada, ne zauzima ceo link, već se kroz isti link mogu slati paketi više različitih korisnika. Ukoliko pak, samo jedan korisnik ima potrebu za korišćenjem linka, koristiće ga samo onoliko koliko je potrebno ta prenos njegovih paketa.

Uz pomoć novijih tehnologija sada je moguće detektovati situacija kada nastupa tišina (momenti kada nema prenosa glasa), pa u tom momentu, smanjiti ili obustaviti slanje RTP paketa koji ne nose koristan sadržaj. Na ovaj način sigurno se povećava efikasnost skupih linkova. Za vreme tišine, paketi drugih korisnika će biti prenet linkom.

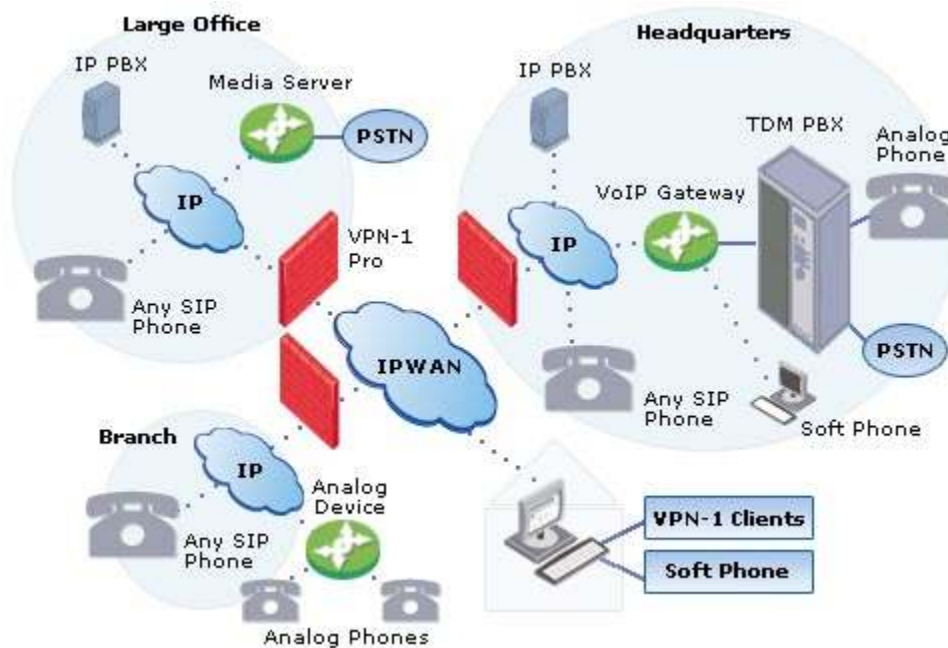
Upoređivanjem dve tehnologije prenosa glasa, VoIP i tehnologija fiksne telefonije, dolazimo do zaključka da se korišćenjem VoIP ostvaruje znatna ušteda, kako od strane korisnika koji neće plaćati punu cenu iznajmljivanja linka, tako i od strane provajdera kojima se investicije u telekomunikacionu opremu zamenjuju investicijama u mrežnu opremu gde postoji znatna razlika u ceni.

Ako postavljamo cenu kao glavni kriterijum, zaključićemo da VoIP nemerljivo bolja tehnologija prenosa glasa od tradicionalne fiksne telefonije. Međutim, korišćenjem mrežnih resursa, VoIP pored pogodnosti donosi i nove probleme, koji su poznati u računarskim mrežama.

Neki od najčešćih problema koje postoje kod upotrebe VoIP tehnologija, dok kod fiksne telefonije ne predstavljaju problem su :

- Raspoloživi propusni opseg (bandwidth) – što direktno utiče kako na broj simultanih poziva, tako i na izbor kvaliteta kodeka za kodiranje glasa
- Kašnjenje – veliki broj malih paketa, zahtevaju minimalno zadržavanje na zagušenim linkovima. To je veoma čest problem i zahteva definisanje QoS (Quality of Service)
- Gubitak paketa – VoIP koristi UDP nepouzdan način prenosa, zbog velikog broja paketa. Zagušeni linkovi odbacuju pakete kako bi regulisali zagušenost. Za VoIP mora se definisati QoS

- Jitter – je nepoželjna varijacija nepredvidivih nepoželjnih efekata kao što su kašnjenja i gubitci paketa. Može se redukovati implementacijom QoS-a.
- Echo – eho je čest problem u hibridnim okruženjima. Uglavnom se stvara kod konverzije A/D – D/A signala i u slučaju nepodešenih impedansi konvertera.
- Zaštita – kod fiksne telefonije to je bilo jednostavno, imaš svoj kabl, svoju liniju koja se fizički štiti. Kod VoIP-a je se na računarskim mrežama pa je potrebno implementirati odgovarajuću zaštitu.
- Pouzdanost – koristi se zajednička infrastruktura sa računarskim mrežama. Za unapređivanje pouzdanosti koriste se iste tehnike kao i kod računarskih mreža. Udvojena, paralelna infrastruktura, rezervni linkovi i sl.
- Prevođenje pulsno pozivanja u DTMF ton – stvar od koje se gotovo odustalo kod VoIP tehnologija.



Arhitektura VoIP mreže

Kao i kod drugih tipova servisa koje koriste TCP/IP model prenosa podataka, i za prenos podataka su definisane različite vrste protokola.

Kako bi se optimizovala putanja između dve udaljene tačke, uveden je koncept koji omogućava da se različitim putem i do različitih destinacija kreće signal za upravljanje pozivom (uspostavljanje i prekid veze, dogovor oko izbora kodeka, registrovanje korisnika i sl.), a različitim paketi koji nose glas. Ovim postupkom se dobija to da centri za pozivanje (signaling call centri), mogu biti na lokacijama bilo gde u svetu, a da ne utiču bitno na kvalitet i brzinu VoIP telefonije. Tako npr. možete iz Srbije osnovati pretplatnički odnos u Americi, pa kada preko VoIP-a zovete Srbiju, paketi signalizacije će otići do call centra u

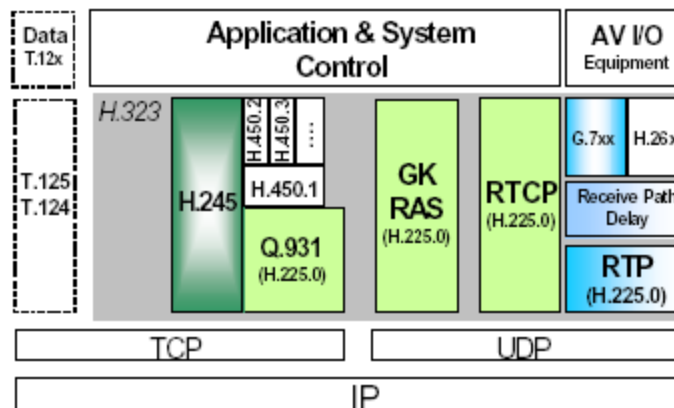
Americi u vratiti se do vas, ali paketi sa glasom će samo putovati od vas do onoga koga pozivate (neće ići do servera u Americi).

Za prenos glasa kroz IP protokol se uglavnom koristi RTP (Real-time Transport Protocol), koji pakuje kodirane pakete u sitne pakete i šalje ih UDP protokolom.

Ono što je nezgodno kod RTP protokola je to što se teško šiti. Razlog je to što mora se obezbediti određeni spektar UDP portova (npr. 10000-20000 UDP), pa je potrebno i ceo spekat propustiti na firewall-u. Ukoliko se propusti manji spektar, manji broj istovremenih poziva može biti uspostavljen. RTP koristi 2 UDP porta po pozivu, jedan za prijem, drugi za slanje VoIP paketa.

Kod signalizacije stanje je vrlo raznoliko.

H.323 protokol je postavljen od strane ITU organizacije i predstavlja prvi signaling protokol koji je komercijalno prestavljen i prihvaćen. U okviru ovog protokola su se razvili drugi podprotokoli koji definišu rad H.323 protokola. Tako npr. H.225.0 definišu konstrukciju paketa za pozivanje, ukazivanje da li je video ili običan poziv i sl.



H.323 koncept

H.323 protokol se kao i većina drugih „usput“ razvijao. Tako brojni nedostaci, prvenstveno zaštita, NAT, i sl., su otklonjeni definisanjem novog protokola u okviru H.323. Početna solucija H.323 protokola nije posedovala nikakvu zaštitu, naime, bilo je dovoljno poznavanje ip adrese call centra kako bi se inicirala veza. Ovaj način ostvarivanja komunikacije se naziva H.323 preko Gateway-a. Uvođenjem standarda H.323 Gatekeeper znatno je podignut kvalitet zaštite preko Call Admission Control mehanizma, i implementiran sistem za prevođenje broja telefona u IP adresu. Implementacijom Gatekeeper mehanizma ostvaruje se potreba kontrola pristupa preko H.323 protokola, sprečava zagušenje mreže, i podiže nivo sigurnosti kroz autentifikaciju.

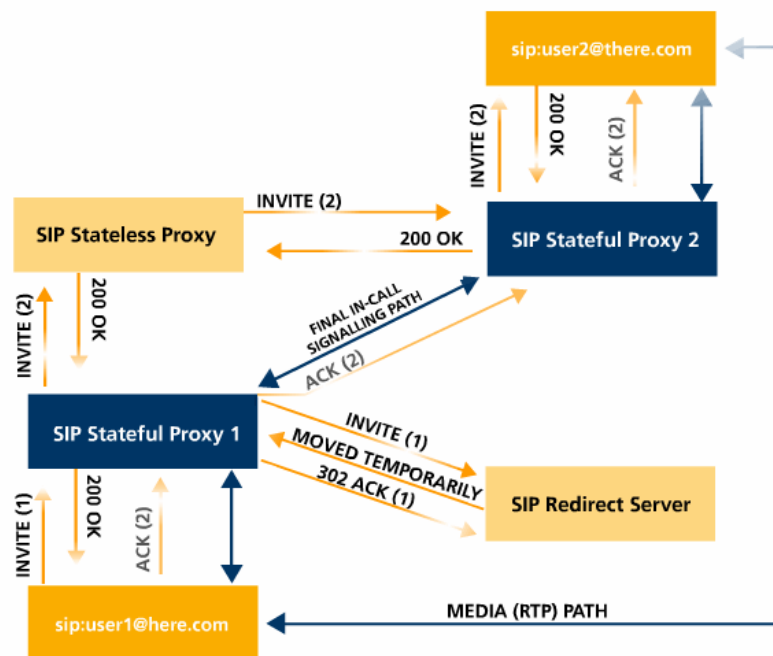
Call Admission Control je mehanizam, često i poseban uređaj, koji ima sledeće zadatke :

- Sprečava preopterećivanje VoIP mreža – odbijajući poziv ukoliko ne postoji dovoljno resursa za njegovo uspostavljanje.
- Kontroliše sav voice saobraćaj obezbeđujući mu potreban kvalitet servisa (QoS) markiranjem.
- Sprečava zagušenja postojećih resursa prosleđivanjem novih poziva na druge linkove.

- Ukoliko se koristi RSVP protokol za rezervaciju resursa duž čitavog puta mreže, vrši kontrolu nad raspolaganjem tih resursa i ne dozvoljava uspostavu veze ako rezervacija nije obavljena.
- Ukoliko zbog bilo kog razloga, procesor preopterećen, problemi na linku i sl., poziv ne može biti kvalitetno uspostavljen, CAC odbija poziv, čime se poziv upućuje drugom putanjom.
- Novije varijante predviđaju napredne sisteme autentifikacije korisnika i zaštite od ranjivosti raznih tipova napada, npr. DOS (Denial-Of-Service)

Zadatak H.323 Gatekeeper mehanizma je da vrši Call Admission Control funkciju u H.323 protokolu. Pored toga vrši prevođenje E.164 identifikacije (broja telefona) u IP adresu.

SIP (Session Initiation Protocol) protokol je protokol definisan od strane IETF organizacije, i po svemu sudeći komercijalno je potisnuo H.323 iz masovne upotrebe. SIP protokol je definisan dokumentom RFC 3261. Može koristiti protokole transportnog sloja: TCP, UDP, SCTP. Počevši sa razvojem 1996. na Kolumbiskom Univerzitetu, u Novembru 2000 je prihvaćen za 3G standard za signalizaciju VoIP paketa.



SIP koncept

SIP je koncipirao sledeće komponente VoIP mreže :

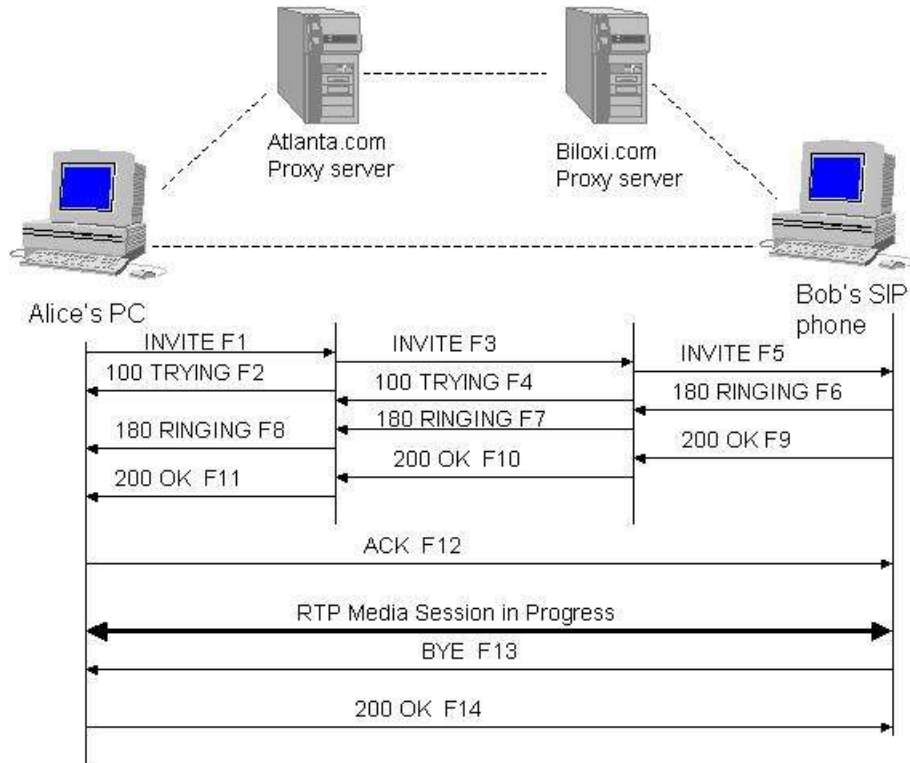
Krajnje tačke – su uređaji ili softwer, koji vrše inicijalizaciju ili prihvatanje poziva tj. vrše interakciju sa korisnikom.

ENUM ili DUNDI - su dve tehnologije za prevođenje broja telefona u ip adresu krajnje tačke ili gateway-a preko kog se može stići do kranje tačke.

SIP Proxy – su sistemi za zaštitu putem autentifikacije kao i Admission Control upravljanje mrežnim resursima. Proxy serveri obavljaju posao rutiranja saobraćaja, tj

usmeravanja signaling paketa ka drugim proxy serverima koji poseduju zahtevane podatke tj. znaju koja ip adresa odgovara pozvanom broju telefona.

Međusobnom signalizacijom SIP Proxy servera, postiže se mogućnost mobilnosti. To znači možete zadržati isti broj telefona a promeniti fizičku lokaciju. SIP protokol je potpuno definisan na logičkom nivou, pa je fizički nezavisno gde se nalazite.



SIP signalizacija

H.323 i SIP protokol zahtevaju neke mrežne predispozicije da bi funkcionisale. Do skoro, ni jedan ni drugi protokol nije mogao da funkcioniše ako se bilo jedna ili druga strana nalaze iza NAT servisa. Razlog je to što bi registratori beležili javnu IP adresu, preko koje se ne može direktno stupiti u kontakt sa krajnjim korisnikom. Pošto veći deo mreža koje imaju pristup internetu koriste NAT kao mehanizam sa prevođenje privatnih u javne ip adrese, SIP je predvideo mogućnost NAT-ovanih adresa što je dugo bila glavna prednost nad H.323 protokolom. Danas i H.323 protokol ima svoje rešenje sa NAT okruženje.

Postoje potrebe u VoIP saobraćaju, kada i RTP i signaling paketi treba da putu istom putanjom i do istog odredišta. To je česta situacija kada se međusobno povezuju call centri i uspostavljaju tzv. Trunk između svojih proxy i gateway servera. U tim situacijama predstavlja komplikaciju to što moramo da vodimo računa u različitim portovima (TCP ili UDP) za SIP, RTP, ili H.323 protokol. Da bi preneli glas od tačke A do tačke B moramo otvoriti portove na firewall-u: od 10000-20000 UDP za RTP, 5060 za SIP, ili 1720 UDP za

H.323, u svakom slučaju to je već širok spektar portova, plus što mora da se vodi računa o NAT konfiguraciji (da se poznaje javna IP ako se koristi privatna na serveru).

Kao rešenje za ovaj problem definisan je IAX (Inter Asterisk eXchange) protokol od strane OpenSource udruženja koja razvija Asterisk VoIP platformu. IAX tj. IAX2 protokol istim kanalom prenosi i signaling i voice podatke. Cilj je da se ekonomičnije rasporedi bandwidth tako što se i signali i voice podaci šalju istim paketom, pa ne postoji zahlavljje za dva paketa (kao kod SIP i H.323). IAX2 koristi jedan UDP port 4569, pa kako ne koristi posredno RDP protokol, sve što je potrebno konfigurirati na firewall-u je da pravilno prosleđuje pomenuti port. Kao rešenje za NAT problem IAX2 koristi STUN javni server na internetu koji služi da automatski sazna koja je javna ip adresa na NAT-u i konfigurira polaznu adresu na javnu IP adresu.

Još jedno bitna prednost IAX-a u odnosu na SIP je to što je uveden mogućnost buferisanja jittera čime je unapređen kvalitet prenosa glasa u tehnologijama sa velikom jitterom kao što je ADSL.

Prednosti IAX-a naspram SIP protokola :

- IAX dosta efikasnije prenosi glasovne pakete nego RTP protokol. Ovo su pokazali testovi čak i prilikom velikog broja istovremenih poziva i korišćenjem različitih kodeka
- IAX je kompletno strukturalno postavljen, za razliku od SIP-a koji je ASCII baziran. Napad je znatno otežan zbog teže sinteze paketa.
- IAX zaštevava prosleđivanje samo jedno UDP porta na firewall-u
- IAX podržava prosleđivanje kanala kako direktno sa korisnika na korisnika, tako i preko servera posrednika
- IAX razdvaja CallerID od autentifikacije
- IAX podržava parcijalno biranje (biranje dela telefonskog broja, dok se čeka ostatak)
- IAX uvek šalje DTMF preko signala, nema zabune da li se nalazi i u voice paketima

Za sada mali broj uređaja podržava IAX2 ekstenziju. Sve češće vidamo na internetu da je izašao novi model telefona koji podržava IAX2 i SIP paralelno. IAX2 softphone aplikacije su znatno traženije u poslednje vreme baš iz razloga što od klijenta ne zahteva nikakvo znanje i konfigurisanje.

Još od uvođenja ISDN digitalnih linija, tema korišćenja različitih algoritama za kodiranje i pakovanje glasa, je bila često glavna tema na telekomunikacionim seminarima.

G.711 (PCM) kodek je standard propisan od strane ITU već 1972. godine. G.711 predstavlja algoritam za pusno-kodnu modulaciju signala frekvencije glasa, koji se (odmerava) sampluje 8000 puta u sekundi. Ovaj standard je definisan iz dva dela. μ -law koji se koristi u Severnoj Americi i Japanu i A-law koji se koristi u ostatku sveta.

G.711 A-law je standard definisan sa kodiranje glasa u računarske potrebe. U algoritmu se uzimaju 13 bita sempla i konvertuje u 8 bita. Karakteristike A-law kodeka su sledeće :

- Frekvencija semplovanja : 8 kHz
- 64 kb/s bitrate (8 kHz x 8 bita po samplu)

- Za izvršavanje algoritma potrebno je oko 0,125 ms
- Zadržava talasastu formu signala
- Sadrži algoritme za oporavak izgubljenih paketa
- Mehanizmi za detektovanje tišine ili generisanje udobnog šuma

Algoritmi za kodiranje, kodeci, su ocenjivani od strane ITU na osnovu postavljenih kriterijuma. Kao rezultat dobija se PSQM (Perceptual Speech Quality Measure) ocena. Za G.711 (PCMA) A-law kodek ocena je 4.45 u idealnim uslovima a 4.11 u realnim uslovima.

GSM kodek tipa Adaptive Multi-Rate (AMR) je kodek koji je prihvaćen na 3G algoritam za kodiranje glasa Oktobra 1998. godine. GSM (AMR) kodek koristi 160 semplova dužine 20 milisekundi. Koristi sledeće tehnike prilikom kodiranja :

- Algebraic Code Excited Linear Prediction (ACELP)
- Discontinuous Transmission (DTX)
- Voice activity detection (VAD)
- Comfort Noise Generation (CNG)

Kod GSM (AMR) kodeka koristi se AMR_12.20 mod koji ima bitrate 12.20 kbit/s. Kako bi otporniji na kvalitet mreže, GSM je smanjio kvalitet glasa.

Generalne karakteristike GSM kodeka su :

- Frekvencija smplovanja 8 kHz/13-bita, filtrirano na između 200-3400Hz
- Bitrate 12.20 kbit/s
- Veličina okvira ~ 244 bita
- Vreme izvršavanja algoritma 20 ms
- Kompleksnost algoritma je 5, u donosu na to da je G.711=1 a G.729=15
- PSQM=4.14 za idealno i 3.79 za realno okruženje

G.729 kodek postoji u različitim varijetama, skoro sve su komercijalnog i zatvorenog tipa, pa je neophodno platiti licencu za korišćenje.

G.729a je kodek koji koristi kompleksne matematičke funkcije kako bi našao što bolji koder za pakovanje glasa. Pravno korišćenja ovog kodeka reguliše firma SIPRO.

Karakteristike kodeka su sledeće :

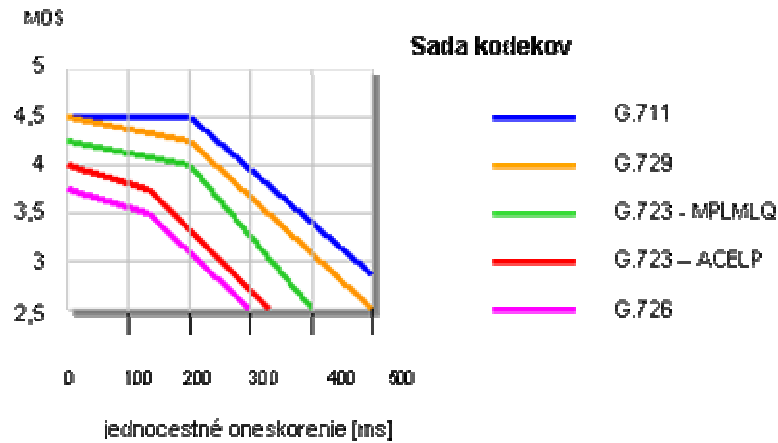
- Frekvencija smplovanja 8 kHz/16 bita (80 semplova sa 10 ms)
- Fiksirani bit rate na 8 kbit/s 10 ms okvir
- Veličina okvira 10 bajta po 10 ms
- Vreme izvršavanja 15 ms po okviru
- G.729 koristi kompleksni oblik ACELP-a
- Kompleksnost se ocenjuje ocenom 15
- PSQM=4.04 za idelano i 3.51 za realno okruženje

Kriterijum izbora kodeka za pakovanje glasa je raspoloživ bandwidth. Ako se radi o LAN okruženju, gde postoji 100 mbps ili jača mreža, bez razmišljanja se treba opredeliti za najkvalitetniji G.711 A-law kodek. U nedoumici možemo biti samo ako postoje WAN linkovi koji trpe određena zagušenja. Tad treba izabrati optimalan kodek koji daje zadovoljavajući kvalitet uz manju konzumaciju propusnog opsega od G.711. U

realnosti, za ove slučajeve, najbolje se pokazao G.729 kodek koji ne smanjuje drastično kvalitet zvuka, za razliku od GSM kodeka. Problem je to što u nekim zemljama da bi se koristio mora da se plati licenca.

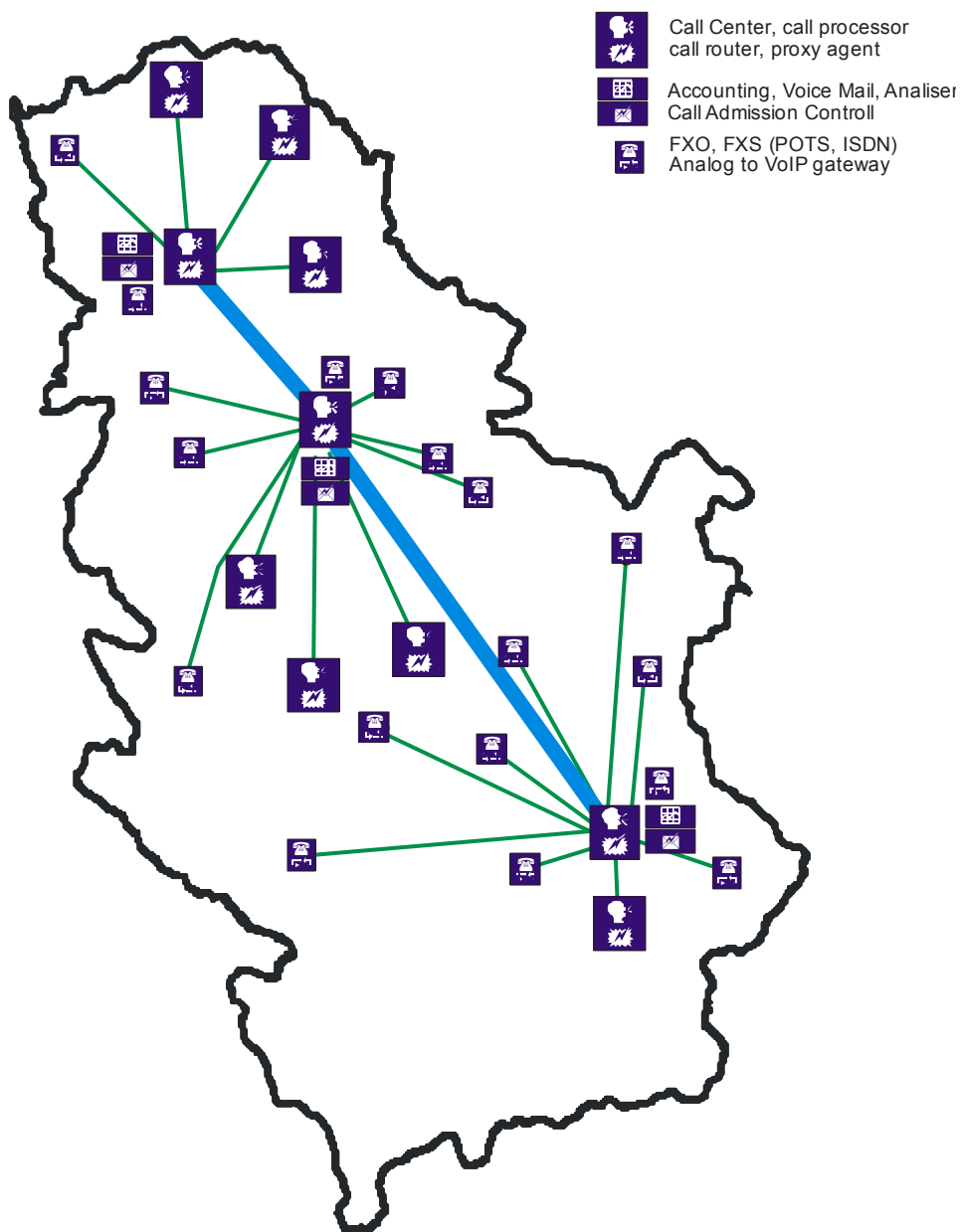
Zaključak :

- LAN okruženjima koristiti SIP ili IAX sa G.711 a-law kodekom
- WAN potencijalno zagušenim okruženjima koristiti IAX sa G.729 kodekom



Prikaz kvaliteta prenesenog glasa različitim kodecima

➤ Centralno-distribuirani sistem za IP telefoniju



Organizacija centralizovano-distribuiranog sistema za IP telefoniju

➤ QoS

Korišćenjem postojećih resursa, istim linkom prenose se paketi različitih tipova podataka. Mrežni uređaji, po defaultu, ne raspoznaju tipove paketa, niti znaju koje su važnosti paketi koje prenose.

Različite aplikacije imaju različite potrebe korišćenja mrežnih resursa. Tako recimo do skoro je važno da HTTP služi za prenos sajtova, zahteva brz odziv, prenos malih fajlova, i vrlo kratko opterećuje linkove. Sa druge strane, FTP i Peer-to-peer programi zahtevaju veliki propusni opseg i imaju znatno veće vreme opterećenja linka (duže se prenose podaci), dok brzina odziva je skoro nebitan faktor. Potrebe svih aplikacija možemo klasifikovati na sledeći način :

- Potreba za propusnim opsegom (bandwith) – kako bi se napravila optimalna organizacija i raspodela mrežnih resursa, potrebno je odraditi proračun zahtevanog propusnog opsega. Ukoliko se zakupi manji propusni opseg nego što je potrebno, moglo bi da dođe do degradiranja performansi mrežnog saobraćaja, što se prikazuje lošijim rezultatima sledećih stavki.
- Količina odbačenih paketa (dropped packets) – usled velikog broja, znatno utiče na TCP konekcije zahtevajući da se paket ponovo pošalje, čime se povećava kašnjenje. Kod UDP konekcije može a ne mora da se primeti. Najčešće se javlja usled „zagušenosti“ linka, tj. kada je potreban veći propusni opseg nego što je zakupljen.
- Kašnjenje (delay) – uvek postoji, makar zbog potrebe mrežnih uređaja da prebace bitove sa port-a na port. Velika kašnjenja prouzrokuju efekat „sporosti“ mreže. Kašnjenje se prikazuje u milisekundama (ms). Velika kašnjenja između ostalog nastaju kada je link zagušen, usled ponavljanja paketa, ako se primenjuje neadekvatan algoritam za redove i sl. Prilikom pregledanja sajtova, ako je odziv 1000ms (1 sekund) stičemo utisak da internet radi veoma sporo.
- Jitter (Džiter) – predstavlja nepredvidivu nepravilnu promenu u kašnjenju. Izražava se u procentima promena kašnjenja. Usled velikog jittera dolazi do istog efekta kao kod velikih kašnjenja.
- Pristizanje paketa bez pravilnog rasporeda – kako na internetu postupak preusmeravanja paketa je potpuno automatizovan, tako ne možemo predvideti kojim putem će naši paketi proći do kranje destinacije. Kod slanja većih podataka, šalju se više manjih paketa. Ne mora da znači da će ti paketi putovati istim putem, i da će stići u rasporedu kojim su poslani. Zbog ovog efekta, može doći do velikog kašnjenja ili gubitka nekog od paketa, što bi kod TCP prouzrogovalo ponovnim slanjem tog ili grupe paketa.
- Greške – se dešavaju zbog ne savršenosti, kako fizičkih linkova, tako i samih uređaja. Dešava se da se u prenosu paket minimalno izmeni, promeni jedan bit, zbog čega se taj paket smatra sa greškom i odbacuje na sledećem uređaju. O odbacivanju se obaveštava pošaljilac kako bi paket poslao ponovo. Ovaj efekat povećava kašnjenje zbog potrebe ponovnog slanja paketa.

Zadatak tehnologije Quality of Service (QoS) je da uvede red, raspored, sprovede plan u organizaciji mrežnog sobračaja. Time ćemo postići bolju iskoristljivost veoma skupih linkova, bez zakupa većeg i skupljeg propusnog opsega. Pravilnom planskom organizacijom mrežnog sobračaja postići ćemo to da aplikacijama sa različitim potrebama mrežnih resursa, pružimo ono što je potrebno za efikasan rad. Primer je to da ne moramo da se odrekemo Peer-to-peer programa, koji uvek maksimalno opterećuju propusni opseg, ako hoćemo brz odziv HTTP strana. Dovoljno je samo definisati QoS na pravi način.

Prvi korak kod postavljanja QoS politike je određivanje potreba različitih aplikacija.

Sledeća tabela prikazuje zahteve nekih aplikacija :

	Bandwith	Odbačeni paketi	Kašnjenje	Jitter	Ne pravilni raspored paketa	Greške
HTTP	>128 kbps	< 10 %	< 500 ms	< 1000	-	-
P2P	Max	-	-	-	-	-
VoIP	> 64 kbps	< 1 %	< 150 ms	< 100	utiče na kašnjenje	- -
Video	> 300 kbps	< 1 %	< 100 ms	< 100	- -	- -
Mission Critical	~ 45 kbps	< 1 %	< 50 ms	< 10	- -	- -

Drugi korak za uspostavljanje QoS politike je markiranje različitih tipova saobraćaja, i svrstavanje u odgovarajuće grupe.

Pakete možemo razvrstati na osnovu više kriterijuma :

- Odredišna IP adresa
- Izvorišna IP adresa
- Odredišni port
- Izvorišni port
- Tip protokola
- Vrednost DSCP ili TOS bitova
- MAC adresa

Korišćenjem nekog od pomenutih parametara raspoznavanja tipa paketa, na ulazu u router (ili switch), vršimo markiranje konekcije, tj. paketa. Time postizemo to da uređaj razaznaje različite vrste aplikacija čije pakete prenosi.

Ukoliko ne postoji relacija poverenja između routera i drugog mrežnog uređaja, onda ne možemo očekivati da će markiranje DSCP vrednosti biti odrađeno na tom drugom uređaju, već se remarkacija DSCP vrednosti vrši na samom routeru uz pomoć drugih pomenutih kriterijuma razlikovanja paketa aplikacija.

➤ DSCP

Differentiated services ili DiffServ je polje u okviru TOS bitova unutar IP hedera koje služi da odredi klasu servisa, tj. obeležava zahteve određene aplikacije, kako bi mrežni uređaji, kroz koji plaket prolazi, pokušali da pruže servis kakav se očekuje. (malo kašnjenje, što manje gubitka paketa i sl.)

Za određivanje klase servisa koriste se 6 bitova u okviru IP hedera. Prva 3 bita se koriste od određivanje prioriteta saobraćaja (IP Precedence), tj. definiše grupe klasa zahteva za uslugom. Svaka od te tri grupe sadrži više različitih nivoa klasa.

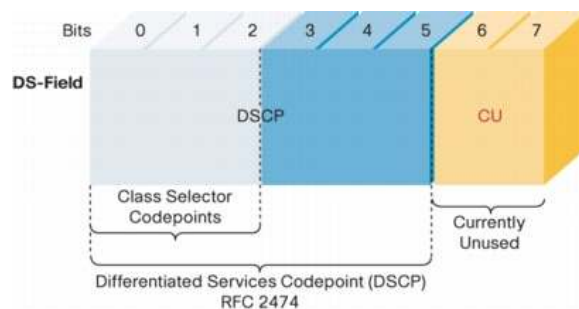
Sve obuhvatno gledajući DSCP vrednosti možemo podeliti u tri posebne klase:

- Best-effort (BE) – klasa DSCP=0 gde se ne obezbeđuje nikakva garancija u transportu, ovo je ujedno i default klasa
- Expedited Forwarding (EF) – namenjena za saobraćaj koji zahteva minimalno kašnjenje i minimalan broj izgubljenih paketa
- Assured Forwarding (AF) – namenjen za sve druge klasifikacije saobraćaja

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010	010010	011010	100010
	AF11	AF21	AF31	AF41
	DSCP 10	DSCP 18	DSCP 26	DSCP 34
Medium	001100	010100	011100	100100
	AF12	AF 22	AF32	AF42
	DSCP 12	DSCP 20	DSCP 28	DSCP 36
High	001110	010110	011110	100110
	AF13	AF23	AF33	AF43
	DSCP 14	DSCP 22	DSCP 30	DSCP 38

Assured Forwarding (AF) – tabela ponašanja

Veća klasa treba da ima veći prioritet i manje kašnjenje. Kombinacijom različitih klasa i minimalnim odbacivanjem paketa, dobijamo 12 različitih klasa u okviru AF klasifikacije. Tako recimo klasa AF43 treba da ima minimalno kašnjenje ali nije bitno ako se izgubi veći broj paketa.



DSCP vrednost u okviru IP hedera

Da bi mrežni uređaj, router, izvršio markiranje VoIP saobraćaja potrebno je samo analizirati DSCP vrednost bitova. Ukoliko postoji DSCP markiranje od strane ostalih uređaja koji prenose VoIP pakete, DSCP vrednost tih paketa treba da bude postavljeno na vrednost EF (Expedited Forwarding) klasu saobraćaja.

Tabela markiranja i dodele DSCP vrednosti različitim tipovima saobraćaja :

	DSCP Klasa	DSCP Vrednost
Mission Critical	AF42	36
VoIP	EF	46
Video	EF	46
Mail	AF12	12
HTTP	AF12	12
NTP	AF41	34
OSPF	AF41	34
Ostalo	BE	0

DSCP vrednosti za različite aplikacije

U našem slučaju Mission Critical aplikacija je finansijska aplikacija koja zahteva brz odziv i nije mnogo osetljiva na gubitke paketa.

Network Time Protocol zbog preciznosti podešavanja sata zahteva visok prioritet tj. minimalno kašnjenje, a pošto se radi o UDP protokolu, neophodan je što manji procenat odbačenih paketa.

OSPF routing protokol treba što brže da dovede routere u konzistentno stanje kako bi se očuvala puna konektivnost u mreži.

Klasifikacija saobraća je mora izvršiti na prvom routeru do krajnje tačke i to na sledeći način :

- Mission critical – finansijska aplikacija uvek gađa fiksnu destinacionu adresu, tako da paketi čija je destinaciona adresa adresa servera za finansisku aplikaciju, treba da se markiraju sa DSCP vrednošću 36
- VoIP i Video paketi moraju biti već markirani kada napuštaju uređaj. Ukoliko nisu već markirani treba izvršiti markiranje na osnovu destinacionog porta IAX protokola tj. UDP port 4569 za VoIP na DSCP vrednost 46.

- Mail paketi treba da se markiraju na osnovu destinacionog porta IMAP protokola TCP 143, POP TCP 110, SMTP TCP 25, IMAPS port TCP 993, SMTPS port TCP 465. DSCP vrednost se postavlja na 12.
- HTTP paketi treba da se markiraju na osnovu destinacionog porta TCP 80, HTTPS port TCP 443. DSCP vrednost se postavlja na 12.
- NTP se markira na osnovu destinacionog porta UDP 123 na DSCP vrednost 34.
- OSPF se markira preko destinacione multicast adresa 224.0.0.5 i 224.0.0.6 na DSCP vrednost 34.

➤ Bandwith menadžment

Treći korak u postavljanju QoS politike je određivanje algoritma za raspoređivanje i distribuiranje paketa sa različitim DSCP vrednostima.

Bandwith menadžment (menadžment propusnog opsega) je neophodan u situacijama kada ne možemo obezbediti odgovarajući propusni opseg za sve željene aplikacije. Idealno bi bilo kad bi bili u mogućnosti iznajmiti ili postaviti link onolikog propusnog opsega koliko će nam u trenutku najvećeg opterećenja trebati. Pošto je postavljanje ili iznajmljivanje ovakvog linka, veoma skupo i ne efikasno, to nije situacija koju ćemo vidati u praksi. Zbog toga gotovo uvek je neophodno definisati bandwith menadžment u okviru QoS politike.

Za uređivanje propusnog opsega koriste se sledeće tehnologije :

- Oblikovanje saobraćaja (limitiranje saobraćaja) – kojim se vrši ograničenje maksimalnog propusnog opsega određene aplikacije. Samim tim ne dozvoljava se da aplikacija uzima veći propusni opseg nego što je definisano i time ugrožava druge aplikacije.
- Algoritmi za raspoređivanje – služe da omoguće prioritizaciju određenog saobraćaja kako bi omogućili kako fer transport paketa, tako i manje kašnjenje za pakete koji imaju veći prioritet.
- Algoritmi za izbegavanje zagušenja – koriste se na interfejsima gde može doći do zagušenja. Najčešće je to kod prelaska sa brzih LAN linkova na spor WAN linkove.

Pravilan izbor algoritma za raspoređivanje prilično utiče na kvalitet postavljenog QoS-a. Neki od algoritama su :

- Weighted fair queuing (WFQ) – je algoritam koji je vrlo sličan FIFO algoritmu, koji raspoređuje po pravilu koji paket prvi stigne na ulaz, prvi će izaći na izlaz. Jedina je razlika to što za različite DSCP vrednosti može postaviti posebne FIFO redove. Uvek se pošalje predefinisani broj prioritetnijih paketa, pa tek onda oni sa manjim prioritetom.
- Class based weighted fair queuing (CBWFQ) – algoritam funkcioniše slično kao WFQ što redovi dele ukupan propusni opseg ravnomerno.

- Weighted round robin (WRR) – algoritam koji se, pred FIFO koristi, za Best-effort usluživanje. Algoritam jednostavno propušta po jedan paket iz svake grupe.
- Low Latency Queueing (LLQ) – algoritam je nadgradnja na CBWFQ donošenjem striktnog prioriteta. Naime, postoje dve klase koje se obrađuju po sistemu striktnog prioriteta, kada nešto dođe u taj red, odmah se propusti na izlaz, i nekoliko klasa sa CBWFQ. Ova nadogradnja predstavlja idealno rešenje za VoIP i 3Play mreže. Kada paket sa EF markicom dođe u prioritetan red, biva odmah propušten na izlazni interfejs. Ostali paketi za to vreme čekaju.

Izebegavanje zagušenja linka se po defaultu radi odbacivanjem novo-pristiglih paketa. To je tehnologija tail-drop. Međutim, ovakav pristup ima prilično nedostataka, posebno prilikom korišćenja TCP konekcija. Alternativa ovom metodu je :

- (Weight) Random Early Detect (RED, WRED) – čime se već od X procenata opterećenosti linka počinje odbacivanje paketa, ali ne onih koji su poslednji u redu, već neki koji se određuju slučajnom metodom. WRED ima različito definisan prag odbacivanja X za različite klase saboraćaja tj. DSCP vrednosti.
- Dozvola određenog burst rate tolerancije pre odbacivanja (ili markiranja za odbacivanje)
- Markiranje paketa za odbacivanje (bez odbacivanja) – je tehnika kojom se klijentu i serveru stavlja do znanja da na linkovima postoji zagušenje te da treba da smanje brzinu slanja podataka.

Za naše potrebe koristićemo LLQ algoritam sa apsolutnim prioritetom za DSCP vrednost EF, dok će u okviru LLQ, druge DSCP vrednosti biti raspoređene CBWFQ tehnikom. Ukoliko ne postoji mogućnost korišćenja LLQ mehanizma, algoritam WFQ bi nam pružio zadovoljavajuće rezultate.

Na zagušenim interfejsima treba koristiti WRED mehanizam odbacivanja paketa.

Kao poslednja, ali veoma važna stvar kod implementacije QoS politke je stalno praćenje, monitoring protoka paketa, njihovog raspoređivanja, performanse i sl.

➤ Kontrola poziva

SIP, IAX, pa i H.323 u kombinaciji sa Gatekeeper tehnologijom zahtevaju da onaj ko želi da koristi resurse VoIP komunikacionih cenara, bude u svakom momentu autentifikovan, i poseduje određena autorizaciona prava.

Autentifikacija se vrši korišćenjem UserID parametra, koji je često broj telefona ili ime korisnika, i šifrom. Šifra se, za sada, često šalje kao deo autorizacione sekvence, što je ozbiljan sigurnosni problem. Postoje rešenja koja doprinose bezbednoj autentifikaciji upotrebom MD5 heširanih šifara i nekog od poznatih sigurnih sistema autentifikacije kao što je CHAP autentifikacija.

Autorizacija predstavlja postupak dodele prava određenom autentifikovanom korisniku, kao što su npr.: pozivanje trocifrenih brojeva, pozivanje višecifrenih brojeva, pozivanje brojeva koji počinju sa 0, primanje poziva i sl.

Prijavom korisnika (nakon autentifikacije i autorizacije), komunikacioni centar poseduje dovoljno informacija o tom korisniku. Pored ostalog poseduje i IP adresu preko koje se korisnik prijavio.

Korisnik ne mora da bude čovek (uglavnom i nije), već VoIP telefon, VoIP gateway, softverski telefon, i sl.

Call Admission Control – vrši kontrolu mrežnih resursa koji se tiču VoIP komunikacija. Ovaj sistem je zadužen da se postara da se QoS sprovede efikasno. Setuje DSCP vrednost paketa, ne dozvoljava veći broj konkurentnih kanala nego što link može da propusti, vrši prosleđivanje na alternativne linkove ako je potrebno.

Telefonija dugo poznaje koncept centralizovanog i decentralizovanog sistema telefoniranja. Naime, prvi telefoni su svi bili povezani na jedinstvenu centralnu lokaciju zvanu „centrala“. Odatle bi operater izvršio uspostavljanje veze sa drugom stranom. Odatle je potekao centralizovan sistem telefonije, gde postoji jedna, glavna centrala, preko koje se spajaju tačke A i B. Naglim rastom broja korisnika, više nije bilo moguće zadržati centralizovan koncept pozivanja, već su se veće centrale razbile na više malih.

Decentralizovani koncept je ono što se danas koristi u fiksnoj telefoniji. Postoji veliki broj manjih centrala, na različitim fizičkim lokacijama. Te centrale su povezane sa više srednjih centrala, koje se nalaze na većim lokacijama. Tako kroz nekoliko nivoa. Ukoliko jedan korisnik želi da uspostavi vezu sa fizički dalekim korisnikom, njegov poziv prolazi kroz nekoliko decentralizovanih centrala da bi došla do traženog korisnika. Ovaj koncept se pokazao prilično jeftinijim i logičnijim, nego koncept centralizovanog pozivanja, ali je održavanje postalo komplikovanije.

Ista stvar je i kod VoIP centrala i telefonije.

Da bi centralizovan sistem mogao da postoji, on mora da ima veoma jake linkove, i visoku pouzdanost. Sa druge strane, distribuirani sistem skida opterećenje glavne centrale, ali komplikuje održavanje.

Naj efikasnije rešenje se postiže kombinovanjem ova dva sistema. Distribuirano-centralizovan sistem, koji poseduje nekoliko centralnih lokacija – centrala, međusobno se pokrivaju, kako linkovima, tako i opremom, dok kod srednjih lokacija postoji nezavistan sistem omogućujući lokalni rad i u slučaju pada velikih centrala.

Na velikim lokacijama, Beograd, Novi Sad, Niš nalaze se glavne centrale, koje pružaju srednjim i malim lokacijama. Međusobno su povezane i rezervnim linkovima, kako bi se problem otkaza sveo na minimum. Sve sadrže kompletne baze korisnika i autorizacionih prava, koje međusobno sinhronizuju nakon svake promene.

Srednje lokacije poseduju distribuiranu telefonsku centralu, koja sadrži bazu korisnika i autorizacionih prava onih korisnika koji su planiranti tom fizičkom centru. Srednje lokacije uspostavljaju Trunk kroz linkove, prema svim drugim velikim centralama.

Male lokacije ne poseduju distribuirane centrale, zbog cene postavljanja i održavanja takve centrale. One poseduju samo VoIP gateway uređaje za spajanje na neki od glavnih centrala.

FXS moduli na VoIP gateway uređajima služe da poveži standardan fiksni telefon, na koji smo navili u fiksnoj mreži, sa VoIP centralom. FXO moduli na VoIP gateway uređaju služe omogućće jeftiniji lokalni poziv ka lokaciji u regionu. Npr. iz Novog Sada zovu nekog u Negotinu, umesto da koristimo Telekomovu mrežu iz Novog Sada, koristićemo svoju mrežu do Negotina, pa tek onda Telekomovu mrežu iz Negotina do onoga koga želimo pozvati.

Centralne lokacije su zadužene da stalno vrše testiranje i monitoring Trunk linijama kako do srednjih i malih lokacija tako i do FXO modula gateway uređaja.

➤ Dial Plan

Smisao Distribuirano-centralizovanog sistema se dobija tak pravilnim određivanjem i numeracijom lokalizacija.

Koliko je važno da se na pravi način odredi numeracija lokalizacija vidi se tak kada dođe vreme da se odredi dial plan i rute ka različitim lokacijama.

Uvek treba ostaviti mogućnost za nadogradnju prilikom dodele numeracija talafonskom sistemu. Za potrebe numeracije naše VoIP mreže, dovoljan je broj od 4 cifre.

Podela je izvršena po glavnim, centralnim lokacijama.

Za svaku centralnu lokaciju dodljenje su 2000 brojeva. U tim brojevima je za svaku srednju lokaciju određeno 300 brojeva, a za malu 100 brojeva.

Za numerisanje same centralne lokacije rezervisano je 500 brojeva.

Tabela nemeracije izgleda ovako :

Grad	Prefiks broj
Beograd	10XX
	11XX
	12XX
	13XX
	14XX
Novi Sad	30XX
	31XX
	32XX
	33XX
	34XX
Niš	50XX
	51XX
	52XX
	53XX
	54XX
Valjevo	15XX
	16XX

	17XX
Čačak	18XX 19XX 20XX
Kragujevac	21XX 22XX 23XX
Leskovac	55XX 56XX 57XX
Zrenjanin	35XX 36XX 37XX
Kikinda	38XX 39XX 40XX
Subotica	41XX 42XX 43XX
Užice	23XX
Novi Pazar	58XX
Kraljevo	59XX
Prokuplje	60XX
Kruševac	61XX
Jagodina	62XX
Pirot	63XX
Zaječar	64XX
Bor	65XX
Požarevac	24XX
Smederevo	25XX
Šabac	26XX
Sremska Mitrovica	27XX
Pančevo	28XX
Sombor	44XX

Numeracija gradova je izvršena na taj način da prefiksi određeni prefiksi tačno ukazuju preko kog glavnog centra treba da se rutira poziv.

Dial plan u Beogradu :

Prefiks 3XXX i 4XXX poslati na Trunk prema Novom Sadu

Prefiks 5XXX i 6XXX poslati na Trunk prema Nišu

Prefiks 15XX, 16XX, 17XX prema Valjevu

Prefiks 18XX, 19XX, 20XX prema Čačku

Prefiks 21XX, 22XX, 23XX prema Kragujevcu

Prefiks 24XX prema Požarevcu

Prefiks 25XX prema Smederevu

Prefiks 26XX prema Šabcu
Prefiks 27XX prema Sremskoj Mitrovici
Prefiks 28XX prema Pančevu
Prefikse 10XX, 11XX, 12XX, 13XX, 14XX rutiranje na interne lokale

Dial plan Novi Sad :
Prefiks 1XXX i 2XXX poslati na Trunk prema Beogradu
Prefiks 5XXX i 6XXX poslati na Trunk prema Nišu
Prefiks 35XX, 36XX i 37XX poslati ka Zrenjaninu
Prefiks 37XX, 39XX i 40XX poslati ka Kikindi
Prefiks 41XX, 42XX i 43XX poslati ka Subotici
Prefiks 44XX poslati ka Somboru
Prefikse 30XX, 31XX, 32XX, 33XX, 34XX rutiranje na interne lokale

Dial plan za Niš :
Prefiks 1XXX i 2XXX poslati na Trunk prema Beogradu
Prefiks 3XXX i 4XXX poslati na Trunk prema Nišu
Prefiks 55XX, 56XX i 57XX poslati ka Leskovcu
Prefiks 58XX poslati ka Novom Pazaru
Prefiks 59XX poslati ka Kraljevu
Prefiks 60XX poslati ka Prokuplju
Prefiks 61XX poslati ka Kruševcu
Prefiks 62XX poslati ka Jagodini
Prefiks 63XX poslati ka Pirotu
Prefiks 64XX poslati ka Zaječaru
Prefiks 65XX poslati ka Boru
Prefikse 50XX, 51XX, 52XX, 53XX, 54XX rotiranje na interne lokale

Centrale na srednjim lokalizacijama treba da imaju sledeći dial plan :
Prefiks 1XXX i 2XXX poslati na Trunk prema Beogradu
Prefiks 3XXX i 4XXX poslati na Trunk prema Novom Sadu
Prefiks 5XXX i 6XXX poslati na Trunk prema Nišu
Lokalne prefiksne treba da pošalju na interne lokale

➤ Oprema

Communication Control Center (C³) je VoIP PBX (Private branch exchange) (telefonska centrala) rešenje firme Sky Communications (www.skycommunications.co.yu).

C³ je rešenje koje sadrži integraciju svih neophodnih činilaca jedne proširive VoIP mreže.

Unutar C³ komunikacionog servera nalaze se call procesor, call admission control, call proxy, agent, baza korisnika, CDR (Call Detail Recorder), Voice mail, Voice Recorder, Trafic Analyzer, i još mnogo drugih tehnologija koje se mogu prepoznati na najskupljim telefonskim centralama.

Najveća prednost C³ sistema je njegova proširivnost i inter-operabilnost sa bilo kojom drugom telefonskom centralom (koja poštuje neki od propisanih standarda).

Pored mogućnosti za integracijom sa drugim velikim telefonskim sistemama i mrežama, C³ nudi mogućnost kompletne integracije sa računarskom mrežom i računarskom infrastrukturom. Tako npr. pruža nam mogućnost da postavimo aplikaciju koja će nam preko telefona čitati mail, izgovoriti kurs eura na današnji dan direktno pročitajući informaciju sa sajta Narodne Banke Srbije. Inegracija i sa ne računarskim sistemima, kao što je mogućnost otvaranja, zatvaranja, otključavanja vrata ili kapija, je još jedna od mogućnosti ove proširivog sistema.

C³ podržava gotovo sve stadarde za VoIP komunikaciju. Najveća podrška je posvećena SIP i IAX protokolima. Podržani su svi ne licencirani algoritmi za kodiranje glasa, kao i neki od plaćenih npr. G.729.

Izuzetna proširivost i nadogradnja ovog sistema dozvoljava nam da postavimo sistem sa distribuiranim korisničkim bazama. Tako u slučaju otkaza jednog od centara, drugi veliki centar preuzima kompletan posao.

Posebno replikacionom metodom postignuto je to da udvajanjem centralnih jedinica C³ sistema dobijamo veoma visoku pouzdanost. U slučaju otkaza jednog od tih jedinica na centralnoj lokaciji, drugi uređaj preuzima kompletnu ulogu za samo nekoliko sekundi.

C³ komunikacioni centar poseduje određeni broj FXO ISDN portova. Mogu biti baznog ili primarnog tipa u zavisnosti od potreba. Na taj način ostvaruje se veza sa fiksnom telefonijom preko Telekomovih priključaka.

VoIP telefoni, koji koriste SIP ili IAX protokol za komunikaciju, priključuju se na sistem korišćenjem odgovarajućeg VLAN broja koji ima postavljen QoS duž cele mreže. Telefonima treba podesiti IP adrese C³ centara kao i autentifikacione parametre, kako bi bili deo VoIP mreže.

Ukoliko postoji potreba za starim analognim telefonima, dokupljuje se FXS na VoIP gateway. Ovaj uređaj vrši konverziju paketne komunikacije VoIP-a na standardnu telefoniju.

Na velikim lokacijama treba postaviti udvojene jedinice C³ sistema kako bi se dobila odgovarajuća puzdanost. Svaki takav sistem sadrži sve potrebne napredne funkcije VoIP telefonije i vrši replikaciju podataka na druge paralelne jedinice kako bi se u bilo kom slučaju sačuvali različiti podaci komunikacionog centra (npr. CDR).

Na srednjim lokacijama dovoljno je postaviti po jednu jedinicu C³ sistema koja sadrži trunk linkove kao ostalim velikim lokacijama.

Na malim lokacijama potrebno je postaviti samo FXO i FXS module gateway uređaja koji se povezuju na neku od centralnih lokacija. Sa FXS modulma ćemo povezati analogne telefone na maloj lokaciji, a sa FXO modulima napraviti telefoniranje u tom regionu jeftinijim jer ćemo sve pozive ka tom regionu slati preko FXO porta na tom lokalitetu.