KOMUTACIONI SISTEMI
– Poglavlje 10 –

10 Signalizacija u paketskim mrežama

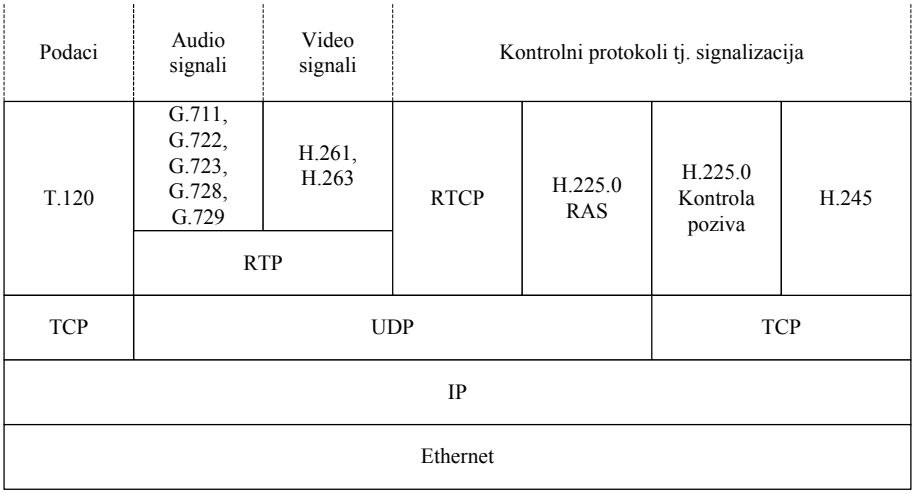
U okviru ovog poglavlja ćemo pod signalizacijom podrazumevati signalizaciju koja se odnosi na telefoniju u paketskim mrežama. Paketske mreže imaju drugačiji model komunikacije od mreža baziranih na komutaciji kola. Kada se formira paketska telefonija u okviru neke paketske mreže, cilj je ostvariti funkcionalnosti koje nudi i klasična (fiksna) telefonija. Stoga je potreban uređaj koji će vršiti ulogu telefonske centrale, ali postoje i razlike u tome šta od funkcija telefonske centrale treba taj uređaj da poseduje. U paketskim mrežama prosleđivanje tj. komutaciju vrše mrežni čvorovi poput rutera i svičeva, pri čemu se prosleđivanje vrši na nivou paketa (sem u izuzecima poput komutacije burstova sačinjenih od grupe paketa). Pretvarati ove uređaje u telefonske centrale ne bi imalo smisla jer većina saobraćaja koji oni komutiraju tipično nije telefonski saobraćaj. Ono što treba da izvršava uređaj u paketskoj mreži koji je ekvivalent telefonske centrale jesu pre svega funkcije administracije i signalizacije koje se odnose na tarifiranje i imenik (adresar) korisnika iz grupe administrativnih funkcija, odnosno na osnovnu signalizaciju neophodnu za uspostavu i raskid telefonske veze. Naime, čim pozivajući korisnik dobije mrežnu adresu (u paketskoj mreži) traženog korisnika, on može preći na direktnu komunikaciju sa traženim korisnikom tako što će slati pakete adresirane na njegovu mrežnu adresu, a mrežni čvorovi će se postarati da ti paketi dođu do traženog korisnika (što uostalom čine za sve pakete nezavisno od informacije koju ti paketi prenose). Time se omogućava da se najveći deo telefonske signalizacije obavi direktno između dva korisnika u komunikaciji. Naravno, u slučaju složenijih telefonskih poziva koji traže i dodatne usluge moguće je dodatno angažovati uređaj koji obavlja ulogu telefonske centrale, poput preusmeravanja poziva u slučaju zauzetosti traženog korisnika ili automatskog poziva traženog korisnika kada on postane slobodan. U najjednostavnijim slučajevima za paketsku telefonsku komunikaciju čak nisu ni potrebni uređaji sa ulogom telefonske centrale, odnosno korisnici mogu da obave svu telefonsku signalizaciju između sebe (slučaj kada korisnik ima kod sebe adresnu informaciju traženog korisnika). Prednost ovakvog pristupa, gde su odgovarajući hostovi/serveri logički deo paketske telefonske mreže i koji koriste usluge mrežnih čvorova za funkcije usmeravanja i komutacije, je velika fleksibilnost u formiranju telefonije u paketskim mrežama, pri čemu mrežna infrastruktura ne mora da se menja već se samo dodaju uređaji koji sa stanovišta paketske mreže predstavljaju hostove/servere čime je veoma jednostavno prilagođavati implementaciju paketske telefonije svojim potrebama.

Paketska telefonija u slučaju IP mreža se naziva VoIP (*Voice over IP*) telefonija i ona je najpoznatija paketska telefonija iz prostog razloga što IP tehnologija predstavlja najpoznatiju i najraširenuju paketsku tehnologiju. Međutim, paketska telefonija se može kreirati i na drugim paketskim mrežama, poput ATM mreže. Postoje dva osnovna pristupa za kreiranje paketske telefonije, H.323 i SIP sistemi signalizacije za paketsku telefoniju. H.323 predstavlja skup protokola koji je razvila ITU-T organizacija i koja pokriva ne samo signalizaciju, već i druge aspekte telefonske komunikacije poput audio i video kodeka (koder/dekoder). SIP protokol predstavlja protokol namenjen za telefonsku signalizaciju u IP mrežama i ovaj protokol je razvilo IETF telo. Razlike ova dva sistema signalizacije dobrim delom potiču od toga ko je razvio dotični sistem. ITU-T organizacija je inertnija i sporije donosi standarde, ali standardi prolaze kroz veoma rigorozne analize i testiranja, i kao rezultat se dobijaju pouzdani, zreli i veoma precizno napisani standardi, ali i često preterano kompleksni standardi koji pokrivaju više aspekata nego što bi možda trebali za veliki broj praktičnih primena. S druge strane, IETF je

znatno dinamičnije telo koje brže donosi preporuke, ali su donete preporuke ponekad manje zrele od onih koje donosi ITU-T i češće zahtevaju dodatne preporuke (dopune) ili ispravke radi otklanjanja naknadno uočenih nedostataka. Međutim, IETF preporuke (preciznije RFC preporuke) prate znatno brže dešavanja u praksi i brže odgovaraju na potrebe korisnika, a uglavnom su i veoma dobro prilagođene filozofiji IP tehnologije pa se lako usvajaju u IP mrežama. U nastavku poglavlja ćemo predstaviti navedena dva sistema signalizacije. Potom će biti izloženi osnovni principi mešovitog rada paketske i fiksne telefonije, sa posebnim osvrtom na probleme koji prate ovaj mešoviti rad.

10.1. H.323 sistem signalizacije

H.323 standard ITU-T organizacije predstavlja opis H.323 infrastrukture (mreže), primere primene u praksi, kao i referencu na standarde koji se koriste u H.323 mrežama, poput H.245 i H.225.0 standarda koji se koriste za signalizaciju prilikom uspostave i raskida poziva. Stoga se može reći da H.323 predstavlja skup standarda koji omogućava paketsku telefoniju u paketskim mrežama koje mogu, ali i ne moraju da obezbeđuju kvalitet servisa. Očigledno, H.323 je predviđen za upotrebu u proizvoljnoj paketskoj tehnologiji, poput IP ili ATM mreža. H.323 ne definiše samo telefonske pozive, već i video pozive, kao i audio i video konferencijske veze (ustvari, originalna svrha definisanja H.323 skupa protokola je bila definisanje podrške za konferencijske veze).



Slika 10.1.1. H.323 protokolski stek

H.323 mreža predstavlja logičku celinu koja fizički koristi paketsku mrežu. Prikaz pozicija protokola u slučaju IP i eternet mreže je prikazan na slici 10.1.1. Kao što se vidi, H.323 omogućava prenos audio i video signala, ali i podataka između korisnika u jednoj interaktivnoj vezi. Za prenos audio signala se mogu koristiti audio kodeci koje smo ranije već opisali poput G.711, G.729, i dr. Pod audio signalom se podrazumeva govorni signal, što se uostalom moglo i zaključiti iz nabrojanih audio kodeka. Za prenos video signala se mogu koristiti video kodeci, poput onih definisanih u ITU-T preporukama H.261 i H.263. U oba slučaja (audio i video signali) se koristi RTP protokol (zajedno sa RTCP kontrolnim protokolom) za prenos audio/video signala, kao i nepouzdani UDP protokol jer je brži od TCP protokola i stoga podesniji za prenos audio/video signala kao što smo ranije već naveli. Napomenimo da se mogu koristiti i drugi proizvoljni audio/video kodeci koji nisu pokriveni ITU-T standardima, pri čemu

je jedino bitno da oba korisnika u komunikaciji mogu da rade sa izabranim proizvoljnim kodekom. U slučaju prenosa podataka mogu se koristiti različiti standardi poput T.120 standarda (koji u suštini predstavlja svojevrsni okvir za skup standarda za prenos različitih tipova podataka poput slika, fajlova i dr.), i svi oni koriste pouzdani TCP protokol jer obezbeđuje pouzdan prenos što je veoma bitno za prenos podataka. Sa slike 10.1.1 možemo videti da postoje tri različite signalizacije (ne računajući RTCP), pri čemu se koriste dva standarda H.225.0 i H.245. H.225.0 se koristi za RAS (*Registration, Admission, and Status*) signalizaciju kojom se između ostalog vrši registracija korisnika na 'centralu', kao i dozvoljavanje započinjanja procesa uspostavljanja veze korisniku od strane 'centrale'. Ova signalizacija je veoma jednostavna i razmena ove signalizacije se sastoji od veoma malog broja poruka pa se stoga koristi UDP protokol jer nije potrebno obezbediti mehanizam pouzdanosti (slično kao i kod drugih protokola sa kratkom komunikacijom poput DHCP ili DNS) na transportnom sloju, već je to efikasnije uraditi na aplikacionom sloju. H.225.0 takođe definiše i signalizaciju za uspostavu i raskid telefonske veze (kontrola poziva) koja je bazirana na ISDN Q.931 signalizaciji. U ovom slučaju se koristi TCP protokol radi neophodne pouzdane razmene signalizacionih poruka, pošto se proces uspostave veze (preciznije proces signalizacije) sastoji od višestruke razmene poruka. H.245 protokol omogućava precizniji dogovor korisnika tj. njihovih terminala o uslovima prenosa, na primer koji audio i/ili video kodek će se koristiti, koja je maksimalna brzina (protok) koji korisnik može primati i sl. Razlog za uvođenje H.245 protokola proističe iz činjenice da postoji velik broj kodeka koje korisnik može koristiti, a takođe korisnici mogu biti priključeni na paketsku mrežu linkovima različite brzine pa je neophodno uskladiti detalje prenosa da bi komunikacija mogla ispravno da se odvija. Ovaj protokol takođe podrazumeva višestruku razmenu poruka pa je neophodno koristiti pouzdan TCP protokol. Naravno, na mrežnom sloju svi koriste IP protokol, odnosno na sloju linka podataka se koriste eternet okviri pošto je u primeru pretpostavljena eternet mreža.

U okviru H.323 standarda se definišu entiteti koji se mogu koristiti u H.323 mreži, pri čemu se pod entitetom podrazumeva određena funkcionalnost. Namerno se ne koristi termin uređaj, jer jedan uređaj može da sadrži više funkcionalnosti i time u suštini predstavlja više entiteta odjednom. Entiteti definisani H.323 standardom su:

- Terminal - Korisnički entitet (host) koji omogućava govornu ili govornu+video ili govornu+podaci ili govornu+video+podaci komunikaciju preko H.323 mreže. Očigledno, svaki H.323 terminal mora da podržava govornu komunikaciju. Primeri H.323 terminala su video telefon, IP telefon (često se ovakav telefon označava kao H.323 telefon da bi se naglasilo da komunicira preko H.323 mreže) ili računar na kome su instalirane odgovarajuće aplikacije za neki od navedenih tipova komunikacija koje terminal može da ostvari.
- Gejtvej - Entitet koji omogućava povezivanje sa ne-H.323 mrežama radi ostvarivanja komunikacije između H.323 terminala i ne-H.323 terminala. Na primer, razgovor između H.323 telefona i telefona iz fiksne (javne) telefonske mreže. Takođe, upotreba gejtveja može da omogući tunelovanje telefonskog saobraćaja kroz H.323 mrežu (na primer, ako su delovi javne telefonske mreže povezani preko IP mreže na kojoj se izvršava H.323 mreža). Gejtvej vrši prevođenje korisničkog saobraćaja (na primer, govornog saobraćaja) iz formata koji se koristi u H.323 mreži (kodek koji koristi dotični H.323 terminal čiji se saobraćaj usmerava ka ne-H.323 mreži kroz gejtvej) u format koji odgovara ne-

H.323 mreži (na primer, govorni odmerci u E1 PCM signalu u fiksnoj telefonskoj mreži), kao i prevođenje u suprotnom smeru. Gejtvej takođe vrši prevođenje signalizacije iz H.323 mreže u format koji se koristi u ne-H.323 mreži (na primer, signalizacija No7 u fiksnoj telefonskoj mreži), kao i prevođenje u suprotnom smeru. Pošto je signalizacija za proces uspostave veze (H.225.0 kontrola poziva) zasnovana na ISDN Q.931 signalizaciji, omogućena je dobra interoperabilnost H.323 mreže sa fiksnom telefonijom i ISDN mrežom. Pošto je QSIG signalizacija takođe zasnovana na ISDN signalizaciji, omogućena je i dobra interoperabilnost u privatnim telefonskim mrežama koje se sastoje iz H.323 delova (paketske mreže) i delova baziranih na komutaciji kola.

- Gejtkiper - Entitet koji najviše odgovara centrali iz klasične telefonije. Gejtkiper omogućava bolje opsluživanje poziva, tako što pruža usluge prevođenja adresa, kontrolu pristupa, kontrolu propusnog opsega. Usluga prevođenja adrese podrazumeva da, na osnovu alijasa traženog korisnika, vrati pozivajućem korisniku mrežnu adresu traženog korisnika koju pozivajući korisnik može koristiti u nastavku procesa uspostave veze i komunikaciji sa traženim korisnikom (u slučaju IP mreža, vraća se IP adresa korisnika). Upotreba alijasa omogućava korisnicima lakše i efikasnije memorisanje adresa drugih korisnika, kao i lakše kreiranje imenika korisnika. Na primer, alijas može biti u URI (*Uniform Resource Identifier*) obliku *h323:petar.petrovic@etf.rs* koji se lako može zapamtiti. Isto tako, alijasi omogućavaju korisniku da menja svoju IP adresu, a da to ne bude vidljivo ostalim korisnicima jer će oni i dalje da koriste alijas koji se nije menjao. Čuvanje imenika sa realnim adresama i alijasima korisnika u gejtkiperu omogućava lakše priključivanje novih korisnika jer se ažuriranje vrši samo u gejtkiperu (isto važi i za ažuriranje podataka o korisnicima, poput promene IP adrese korisnika). Kontrola pristupa predstavlja proces svojevrsne autorizacije korisnika u okviru koje korisnik dobija dozvolu za ostvarivanje veze (ili mu se odbija zahtev). Na ovaj način, gejtkiper u slučaju prevelikog broja razgovora koji su u toku može odbiti zahtev pozivajućeg korisnika za uspostavom nove veze ako smatra da će time biti prekoračen propusni opseg dodeljen telefonskim vezama i time ugroziti kvalitet servisa tekućih razgovora, ili ako je u gejtkiperu podešena vrednost maksimalnog broja istovremenih veza, gejtkiper može odbijati nove veze kada se dosegne ova maksimalna vrednost. Kontrola propusnog opsega omogućava menadžment propusnog opsega u mreži. Gejtkiper prati broj tekućih veza i proračunava koliki propusni opseg one troše, pa u slučaju potencijalnog prekoračenja može da odbije nove zahteve za uspostavom veze. Takođe, kontrola propusnog opsega omogućava dinamičko definisanje propusnog opsega tekućim vezama (može se smanjiti ili povećati propusni opseg tekućih veza). Pored ovih osnovnih funkcionalnosti, gejtkiper može implementirati i druge funkcionalnosti u slučaju potrebe i koje bi omogućile bolju kontrolu i opsluživanje poziva. Na primer, u slučaju implementacije usluge kol-centra, gejtkiper može da izvrši balansiranje poziva ka operaterima tako da ih podjednako optereti.
- Multipoint kontroler - Ovaj entitet se koristi u konferencijskim vezama. Pod konferencijskom vezom se podrazumeva veza između tri ili više korisnika. Pri tome, pod konferencijom se tipično podrazumeva audio (prenose se samo govorni

signali) ili video (prenose se govorni i video signali) konferencija, ali postoje i konferencije u okviru kojih se mogu dodatno prenositi i podaci poput teksta, slike, fajlova i dr. Multipoint kontroler vrši kontrolu konferencijske veze, ali ne vrši procesiranje korisničkih signala, poput miksovanja govornih signala. Pod kontrolom konferencijske veze se podrazumeva pregovaranje zajedničkih parametara komunikacije svih učesnika konferencije, poput audio/video kodeka, protoka i sl. Parametri se podešavaju prema korisniku sa najslabijim tehničkim mogućnostima (u njih pored tehničkih mogućnosti terminala ubrajamo i brzinu linka na koji je spojen korisnik), ali postoji mogućnost i podele korisnika na više grupa sa različitim parametrima tako da neki korisnici, na primer, koriste veći protok od drugih sa slabijim tehničkim mogućnostima. U slučaju video konferencije, multipoint kontroler može da odredi čiji video signal će se puštati učesnicima u konferenciji, pri čemu postoji i mogućnost prikaza više video signala odjednom, ali za tako nešto je potreban multipoint procesor. Takođe, parametri komunikacije se mogu pregovarati i tokom trajanja konferencije, na primer, po uključenju novog korisnika. Multipoint kontroler se može nalaziti u sklopu multipoint kontrolne jedinice, gejtkipera, gejtveja ili terminala.

- Multipoint procesor - Ovaj entitet se koristi takođe u konferencijskim vezama, ali za procesiranje korisničkih signala (govornih signala, video signala i/ili podataka). Na primer, miksovanje govornih signala, selekciju izvora video signala koji će se puštati ostalim korisnicima (tzv. svičovanje izvora video signala), miksovanje video signala kojim se može postići prikaz više video signala na ekranu (na primer, slika u slici, četiri prikaza u 2x2 formatu i dr.), konverzije između različitih kodeka i dr. Multipoint procesor se može nalaziti u sklopu multipoint kontrolne jedinice, gejtkipera ili gejtveja.
- Multipoint kontrolna jedinica - Ovaj entitet sadrži jedan multipoint kontroler i nula ili više multipoint procesora (tj. multipoint procesori su opcioni). Multipoint kontrolna jedinica se koristi za kontrolu konferencijskih veza objedinjujući u sebi funkcionalnosti multipoint kontrolera i multipoint procesora. Razlog za uvođenje ovog entiteta je fleksibilnija implementacija podrške za konferencijske veze jer se ona može realizovati u okviru zasebnog uređaja u slučaju potrebe, i time izbeći opterećivanje gejtveja ili gejtkipera konferencijskim funkcionalnostima.

Sa stanovišta konferencijske veze, razlikujemo centralizovanu i decentralizovanu konferencijsku vezu. U slučaju centralizovane konferencijske veze, svi učesnici (tj. njihovi terminali) se povezuju na multipoint kontrolnu jedinicu po tačka-tačka principu (*point-to-point*). Terminali šalju i kontrolne podatke (signalizacija) i korisne podatke (govor, video, podaci) ka multipoint kontrolnoj jedinici. Multipoint kontroler u kontrolnoj jedinici vrši pregovaranje zajedničkih parametara komunikacije koji će svi učesnici koristiti u komunikaciji (postoji i mogućnost formiranja nekoliko različitih grupa sa različitim parametrima u skladu sa tehničkim mogućnostima učesnika) - kontrolne podatke koji predstavljaju rezultat pregovora se vraćaju od multipoint kontrolera (tj. kontrolne jedinice) ka učesnicima u uspostavljenim tačka-tačka vezama. Multipoint procesor (ako se koristi) u kontrolnoj jedinici vrši procesiranje primljenih korisnih podataka (govor, video i/ili podaci) i tako procesirani korisni podaci se vraćaju korisnicima preko uspostavljenih tačka-tačka veza između korisnika i multipoint kontrolne jedinice. Svaki novi korisnik koji se uključuje u konferencijsku vezu se povezuje sa multipoint

kontrolnom jedinicom, kao što su uradili i ostali učesnici konferencijske veze. Očigledno, ovakav pristup omogućava bolju kontrolu konferencijske veze, ali nije skalabilan jer prevelik broj učesnika u konferencijskoj vezi može da preoptereti resurse multipoint procesora. Multipoint kontrolna jedinica može biti zaseban uređaj, ali može da se nalazi i u sklopu gejtkipera (češći slučaj) ili gejtveja (ređi slučaj).

Decentralizovana konferencijska veza ima drugačiji pristup. Teret procesiranja se prebacuje na terminale. Svaki učesnik šalje po multikast principu svoje korisne signale ka svim ostalim učesnicima u konferencijskoj vezi. Terminali su dužni da vrše miksovanje govornih signala iz svih tokova, kao i selekciju i eventualno miksovanje video signala. Za upravljanje konferencijskom vezom se i dalje koristi multipoint kontroler (gotovo potpuno identična uloga kao kod centralizovane veze, sitnije razlike se odnose na činjenicu da sada nema kontrole rada multipoint procesora) koji sada može biti lociran u terminalu, gejtkiperu, gejtveju ili multipoint kontrolnoj jedinici. Decentralizovan pristup je skalabilniji, ali zahteva podršku za multikast saobraćaj u paketskoj mreži, a isto tako zahteva i terminale sa mogućnostima naprednijeg procesiranja korisnih signala pošto se sada radi i miksovanje, kao i selekcija video signala. Ako se prenose i podaci u konferencijskoj vezi, oni se ipak procesiraju centralizovano.

Postoje i hibridni pristupi koji podrazumevaju da se jedan korisni signal prenosi centralizovano, a drugi decentralizovano. Na primer, govorni signal da se prenosi centralizovano, a video signal decentralizovano ili obrnuto. Takođe, postoji i mešovit pristup konferencijskoj vezi, gde deo učesnika radi u centralizovanom modu, a deo učesnika u decentralizovanom modu. Mešovit pristup je tipično posledica činjenice da se deo učesnika nalazi u mreži koja podržava multikast saobraćaj, a deo učesnika se nalazi u mreži koja ne podržava multikast saobraćaj. U ovom slučaju se mora koristiti multipoint kontrolna jedinica, koja je dužna da obezbedi da korisnici ne vide ovu razliku, tj. da deo učesnika radi u suprotnom modu. U decentralizovanom delu se razmenjuje korisni saobraćaj po multikast principu, a u centralizovanom delu multipoint kontrolna jedinica razmenjuje unikast korisni saobraćaj sa učesnicima preko uspostavljenih tačka-tačka veza. Očigledno, multipoint kontrolna jedinica saobraćaj iz decentralizovanog dela procesira zajedno sa saobraćajem iz centralizovanog dela i šalje unikast principom ka učesnicima iz centralizovanog dela. S druge strane, korisni saobraćaj iz centralizovanog dela se šalje po multikast principu ka korisnicima u decentralizovanom delu (uz eventualno prethodno procesiranje).

H.323 oblast (ekvivalentan termin je H.323 zona) predstavlja skup entiteta (terminala, gejtveja, multipoint kontrolnih jedinica) koji rade pod kontrolom jednog gejtkipera. Pozivi koji se obavljaju unutar H.323 oblasti se nazivaju intrazonski pozivi, a između različitih H.323 oblasti interzonski pozivi. Svi entiteti (sem naravno gejtkipera) se moraju registrovati kod gejtkipera da bi mogli obavljati pozive. Sam proces nalaženja gejtkipera i registracije kod njega se obavlja pomoću H.225.0 RAS signalizacije. Na početku uspostave poziva, terminal (korisnik) se mora obratiti gejtkiperu da bi dobio dozvolu za obavljanje poziva i u slučaju pozitivnog odgovora terminal dobija mrežnu (IP) adresu traženog terminala. I ovaj deo se obavlja pomoću H.225.0 RAS signalizacije. Nakon toga sledi uspostava veze između korisnika upotrebom H.225.0 kontrola poziva signalizacijom koja je veoma slična procesu uspostave veze kod ISDN mreže. Nakon što se uspostavi veza sa traženim terminalom, pre same korisne komunikacije (razgovora) se upotrebom H.245 protokola pregovaraju osnovni parametri komunikacije (određuje se ko je master (*master*), a ko slejv (*slave*) u vezi, koji kodek/kodeci će se koristiti, koji protok će se koristiti, otvaranje logičkih kanala za prenos korisnih signala poput govora ili videa i dr.) tako da

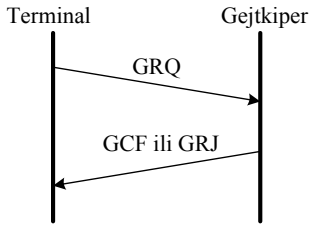
obe strane mogu komunicirati sa dogovorenim parametrima komunikacije. Nako toga, može da otpočne razgovor. Pomenuta tri protokola se javljaju navedenim redosledom prilikom uspostave veze, ali sva tri protokola su aktivna i tokom same veze i mogu da razmenjuju signalizaciju tokom veze (ovde nema redosleda, već svaki protokol radi za sebe). Postoje tri načina razmene navedena tri protokola signalizacije (odluku koji metod će se koristiti donosi gejtkiper, a terminal samo može da navede koji metod je za njega poželjniji):

- H.225.0 RAS signalizacija se razmenjuje sa gejtkiperom, a H.225.0 kontrola poziva i H.245 signalizacije se razmenjuju direktno između terminala između kojih se uspostavlja veza.
- H.225.0 RAS signalizacija se razmenjuje sa gejtkiperom. H.225.0 kontrola poziva se razmenjuje između terminala kroz gejtkiper (u suštini razmena kroz gejtkiper je i dalje razmena sa gejtkiperom, ali postoji velika korelacija u signalizaciji koju gejtkiper razmenjuje sa oba učesnika u vezi). H.245 signalizacija se razmenjuje direktno između terminala između kojih se uspostavlja veza. Ova metoda je pogodna za bolju kontrolu veze, pre svega sa stanovišta administracije veze (efikasnije tarifiranje i beleženje osnovnih informacija o vezi poput trajanja poziva, ko je pozivajući, a ko traženi korisnik i dr.), kao i ostvarivanja dodatnih servisa, ali naravno više opterećuje gejtkiper u odnosu na prethodni slučaj. U ovom slučaju gejtkiper navodi terminalu svoju IP adresu (a ne adresu traženog korisnika) za razmenu H.225.0 kontrola poziva signalizacije.
- H.225.0 RAS signalizacija se razmenjuje sa gejtkiperom. H.225.0 kontrola poziva i H.245 signalizacije se razmenjuju između terminala kroz gejtkiper. Ova metoda je zgodna za konferencijske veze koje započinju kao konferencijska tačka-tačka veza dva korisnika. U slučaju uključenja dodatnog ili dodatnih korisnika, gejtkiper ima mogućnost da izvrši preusmeravanje H.245 signalizacije na multipoint kontroler koji bi preuzeo kontrolu dogovora parametara veze u konferencijskoj vezi. U ovom slučaju gejtkiper navodi terminalu svoju IP adresu (a ne adresu traženog korisnika) za razmenu H.225.0 kontrola poziva i H.245 signalizacija.

Kao što smo ranije pomenuli, postoji mogućnost uspostava veza i bez gejtkipera, tj. kreiranje oblasti bez gejtkipera (doduše termin oblast i nije najadekvatniji pošto je sada ne kontroliše gejtkiper). U ovom slučaju se ne koristi H.225.0 RAS signalizacija jer je ona bitna samo ako je gejtkiper prisutan (tada su bitni postupci registracije i dobijanja dozvole za uspostavljanje veze). Terminali direktno između sebe komuniciraju, pri čemu se u uspostavi veze prvo direktno razmenjuju H.225.0 kontrola poziva, pa H.245 signalizacija pre samog razgovora, tj. sve je isto kao i u slučaju gejtkipera kada se H.225.0 kontrola poziva i H.245 signalizacije razmenjuju direktno između terminala (i dalje postoji mogućnost da ove dve signalizacije razmenjuju signalizaciju i tokom veze). Da bi terminali mogli direktno komunicirati, neophodno je da se u svim terminalima nalazi informacija o mrežnim adresama ostalih terminala. Očigledno, veoma je teško efikasno održavati ovakav imenik u terminalima, naročito ako mrežne adrese nisu statičke. Takođe, ako se dodaje novi korisnik, njega treba uneti u sve terminale. Pored toga, bez gejtkipera nema kontrole propusnog opsega, ali ni podrške dodatnim servisima. Stoga se ovaj metod bez upotrebe gejtkipera koristi u veoma malim mrežama sa malim brojem terminala i gde se obavljaju samo intrazonski pozivi bez potrebe za dodatnim servisima i kontrolom propusnog opsega.

10.1.1. H.225.0 RAS signalizacija

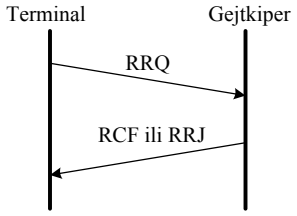
H.225.0 RAS signalizacija se koristi kada gejtkiper kontroliše oblast, što je uglavnom i slučaj. Ova signalizacija omogućava da gejtkiper kvalitetno obavlja svoju ulogu 'centrale'. H.225.0 standard definiše i H.225.0 RAS i H.225.0 kontrola poziva signalizaciju, pri čemu je sintaksa signalizacionih poruka za oba slučaja definisana u ASN.1 (*Abstract Syntax Notation One*) notaciji čija je sintaksa definisana u ITU-T preporuci X.680. Postoji više načina za kodiranje ASN.1 poruka u binarni format za prenos, a u slučaju H.225.0 signalizacije (i RAS i kontrola poziva) se koristi poravnato PER (*Packed Encoding Rules*) kodiranje definisano u X.691 standardu ITU-T organizacije. U okviru ove sekcije će biti dat pregled najpoznatijih i najvažnijih RAS poruka, pri čemu je bitno napomenuti da svaka od poruka sadrži veliki broj opcija (tj. parametara) koje neće biti izlagane u ovoj sekciji. Detaljnije informacije o RAS porukama (kao i njihovim opcijama) se mogu naći u ITU-T H.225.0 standardu.



Slika 10.1.1.1. Proces otkrivanja gejtkipera

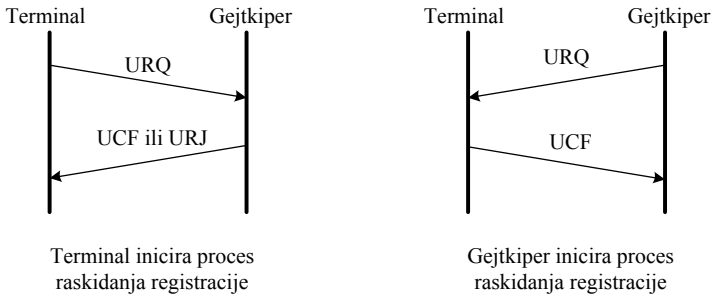
Poruke GRQ (*Gatekeeper ReQuest*), GCF (*Gatekeeper ConFirm*) i GRJ (*Gatekeeper ReJect*) se odnose na proces lociranja gejtkipera kojim terminal pronalazi lokaciju gejtkipera (IP adresu gejtkipera) čime dobija mogućnost da razmenjuje poruke sa gejtkiperom. Ovaj proces se tipično pokreće kada se terminal aktivira ili kada terminal izgubi mogućnost komunikacije sa gejtkiperom (na primer, usled kvara gejtkipera). Terminalima se mogu i ručno uneti podaci o gejtkiperu, i tada nema potrebe za korišćenjem GRQ, GCF i GRJ poruka jer terminali već imaju u sebi podatke neophodne za slanje poruka ka gejtkiperu (pre svega IP adresa gejtkipera). Mana ovog pristupa je slaba fleksibilnost, jer pri svakoj promeni kod gejtkipera, poput promene njegove IP adrese, moraju se ručno ažurirati podaci o gejtkiperu u svim terminalima. Otuda je znatno efikasnije automatizovati proces. Slanjem GRQ poruke na IP multikast adresu 224.0.1.41 i UDP port 1718 (slučaj IP mreže), terminal traži gejtkiper odgovoran za oblast kojoj terminal pripada. Gejtkiper, ako postoji i ako je aktivan, odgovara sa porukom GCF u okviru koje se nalaze podaci o njemu (pre svega njegova IP adresa). U H.323 oblasti može da bude samo jedan gejtkiper i sa njim treba obavljati celokupnu RAS komunikaciju, ali ovakvo rešenje nema redudansu, pa se otkazom gejtkipera gubi mogućnost telefonskih poziva u celokupnoj oblasti. Stoga se definišu i tzv. rezervni gejtkiperi. Rezervni gejtkiperi (ako postoje) se takođe navode u GCF poruci. Terminali sa njima komuniciraju samo ako ih na to uputi primarni gejtkiper, ili ako se primarni gejtkiper ne odazove na poslatu RAS poruku (istekne tajmer u terminalu koji predstavlja dužinu čekanja na odgovor gejtkipera). Gejtkiper može da pošalje i poruku GRJ kojom signalizira da on nije nadležan za dotični terminal (terminal ne pripada njegovoj oblasti, terminal nema pravo da koristi usluge tog gejtkipera i dr.). U slučaju da više gejtkipera odgovori sa GCF porukom, terminal bira gejtkiper kod kojeg će se registrovati. Očigledno je na osnovu navedenog da može doći do preklapanja H.323 oblasti na fizičkom sloju. Na primer, na istoj LAN mreži može da koegizistira više H.323 oblasti. Primer prethodno opisanog procesa razmene RAS poruka u procesu otkrivanja nadležnog gejtkipera je prikazan na slici 10.1.1.1. Osim

terminala, i gejtveji i multipoint kontrolne jedinice takođe rade proces otkrivanja gejtkipera ukoliko informacija o gejtkiperu nije ručno uneta u njihovu konfiguraciju.



Slika 10.1.1.2. Proces registracije

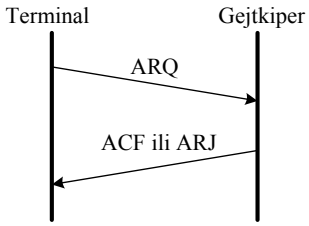
Nakon što terminal (ili gejtvej ili multipoint kontrolna jedinica - u nastavku ćemo navoditi samo terminal, ali navedeno važi i za ova dva tipa entiteta) sazna ko je njegov gejtkiper, tj. koja je mrežna (IP) adresa gejtkipera, terminal može koristiti usluge dotičnog gejtkipera. Sve ostale RAS poruke (preciznije zahtevi ili informacione poruke) terminal šalje na IP adresu gejtkipera i UDP port 1719koji se koristi za prijem RAS poruka koje nisu slate na multikast adresu. U slučaju odgovora terminala na zahtev koji je poslao gejtkiper, terminal će poslati odgovor na IP adresu gejtkipera i izvorišni UDP port iz primljenog zahteva (jer gejtkiper takođe šalje RAS zahteve na UDP port 1719 terminala jer na ovom portu i terminali osluškuju RAS poruke). Prvo što terminal treba da uradi jeste da se registruje kod gejtkipera. Proces registracije je neophodan da bi terminal zaista bio registrovan u H.323 oblast koju kontroliše dotični gejtkiper. Takođe, na ovaj način gejtkiper ažurira svoj imenik sa podacima o registrovanom korisniku, tako da može da prosledi informaciju (na primer, mrežnu adresu) o dotičnom korisniku kada ga neko bude tražio tj. pozivao. Terminal može da prilikom registracije navede i svoje rezervne terminale gde ti terminali mogu biti zaista različiti uređaji ili isti uređaj samo se oglašava njegov alternativni mrežni interfejs (ovo omogućava fleksibilnost i bolju dostupnost korisnika, jer isti korisnik može da bude dostupan na više terminala ili preko više mrežnih pristupa, ali i za realizaciju kol-centra ili drugih sličnih primena). Takođe, terminal navodi i sve svoje alijase tako da drugi korisnici mogu da pozovu dotičnog korisnika preko bilo kog od alijasa. Pri tome, terminal zasebno navodi IP adresu preko koje prima RAS signalizaciju, i IP adresu preko koje prima signalizaciju kontrola poziva, jer one mogu i da se razlikuju u opštem slučaju (ali u praksi se uglavnom, ipak, ne razlikuju). Za registraciju se koriste poruke RRQ (*Registration ReQuest*), RCF (*Registration ConFirm*) i RRJ (*Registration ReJect*). Terminal šalje RRQ zahtev za registracijom, a gejtkiper odgovara sa RCF porukom ako je registracija odobrena tj. uspešno završena ili sa RRJ porukom ako je zahtev za registracijom odbijen (slika 10.1.1.2).



Slika 10.1.1.3. Proces raskidanja registracije

H.323 predviđa i proces raskidanja registracije, čime se korisnik briše iz imenika gejtkipera. Raskidanje registracije se uglavnom radi kada korisnik tj. terminal menja mrežnu

adresu preko koje je dostupan, pa se tada nakon raskidanja registracije vrši nova registracija sa novom mrežnom adresom. Takođe, korisnik može u procesu raskidanja registracije samo delimično raskinuti registraciju u okviru koje će se raskinuti registracija samo za neke alijase koji će stoga biti obrisani iz imenika gejtkipera, ali će korisnik i njegovi preostali alijasi i dalje ostati registrovani. Proces raskidanja registracije može da pokrene i terminal (ili gejtvej ili multipoint kontrolna jedinica) i gejtkiper. Za proces raskidanja registracije se koriste poruke URQ (*Unregistration ReQuest*), UCF (*Unregistration ConFirm*) i URJ (*Unregistration ReJect*). Primeri obe varijante raskidanja registracije su prikazani na slici 10.1.1.3. U slučaju da je proces raskidanja registracije pokrenuo gejtkiper, terminal mora bezuslovno potvrditi prihvatanje raskidanja registracije, a u slučaju da je terminal pokrenuo proces raskidanja registracije, gejtkiper može i da pozitivno potvrdi ili da odbije zahtev za raskidanjem registracije.

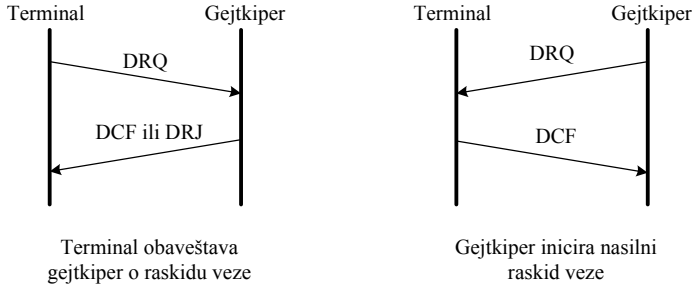


Slika 10.1.1.4. Proces dobijanja dozvole za nastavak uspostave veze

Na samom početku procesa uspostave veze neophodno je dobiti dozvolu od gejtkipera da se može nastaviti sa procesom uspostave veze. Ovime se postiže da gejtkiper može da kontroliše dešavanja u H.323 oblasti za koju je zadužen. Na primer, gejtkiper može da uskrati dozvolu ako proceni da bi time bio ugrožen kvalitet servisa tekućih veza jer je u toku suviše velik broj veza da bi nove smele da budu prihvaćene. Takođe, ako se sva ostala signalizacija, sem RAS, razmenjuje direktno između korisnika, tada gejtkiper jedino preko RAS signalizacije može da dobije informaciju o vezama (da se veza uspostavlja, ko sa kim priča i sl.) što je bitno sa aspekta administriranja i tarifiranja veza. Za proces dobijanja dozvole za nastavak uspostave veze se koriste poruke ARQ (*Admission ReQuest*), ACF (*Admission ConFirm*) i ARJ (*Admission ReJect*). Korisnik (terminal) šalje ARQ poruku u kojoj između ostalog navodi i traženog korisnika (njegove alijase). Gejtkiper po prijemu ARQ zahteva, odlučuje da li će da dozvoli traženu vezu ili ne. Ako dozvoli, gejtkiper šalje ACF odgovor, a ako odbije, tada šalje ARJ odgovor (na primer, odbijanje može da bude posledica biranja korisnika čiji broj tj. alijasi se ne nalaze u imeniku gejtkipera jer taj korisnik ili ne postoji ili nije trenutno registrovan kod dotičnog gejtkipera). U okviru ACF odgovora se nalazi mrežna adresa na koju treba slati H.225.0 kontrola poziva signalizaciju, a ta mrežna adresa može biti IP adresa traženog terminala ili samog gejtkipera u zavisnosti koji metod razmene signalizacije H.225.0 kontrola poziva je gejtkiper izabrao (direktno između terminala ili preko gejtkipera). Primeri procesa dobijanja dozvole za nastavak procesa uspostave veze je prikazan na slici 10.1.1.4. U nastavku procesa uspostave veze se prvo koristi H.225.0 kontrola poziva signalizacija kojom se vrši uspostava veze veoma slična onoj u ISDN mreži, kao što ćemo videti nešto kasnije.

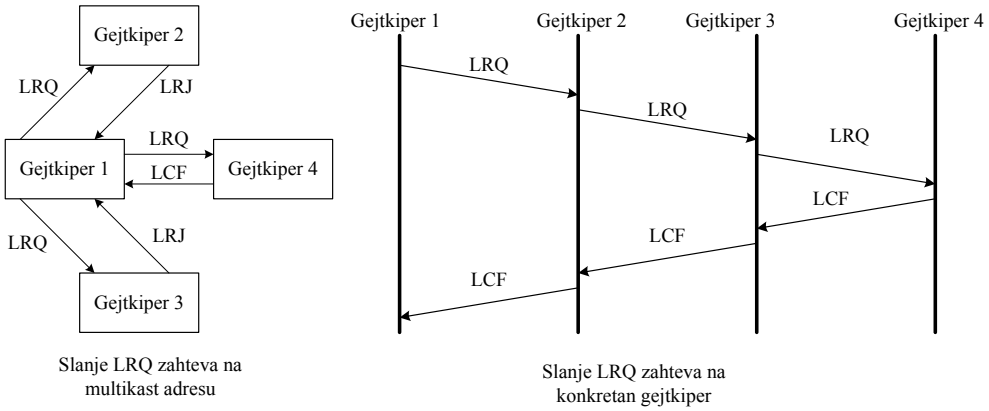
Tokom trajanja veze, može doći do zahteva za promenom vrednosti dodeljenog propusnog opsega (protoka) samoj vezi. Zahtev može poslati i terminal i gejtkiper. Za proces promene vrednosti dodeljenog propusnog opsega vezi se koriste poruke BRQ (*Bandwidth ReQuest*), BCF (*Bandwidth ConFirm*) i BRJ (*Bandwidth ReJect*). Princip razmene ovih poruka je sličan razmenama prethodno opisanih poruka. Strana koja zahteva promenu vrednosti propusnog opsega veze šalje BRQ zahtev, a na njega se odgovara sa BCF odgovorom ako se prihvata

promena vrednosti, odnosno BRJ odgovorom ako se odbija promena vrednosti. U slučaju kada gejtkiper zahteva od terminala promenu na nižu vrednost, terminal će bezuslovno odgovoriti pozitivno (BCF) ako tehnički podržava rad sa predloženom nižom vrednošću protoka, a ako ne podržava rad sa predloženim nižim protokom, terminal će poslati negativan odgovor (BRJ).



Slika 10.1.1.5. Proces raskidanja veze i na RAS nivou

Veza se raskida upotrebom H.225.0 kontrola poziva signalizacije. Međutim, u slučaju kada H.225.0 kontrola poziva signalizacija ne ide kroz gejtkiper (već direktno između terminala), gejtkiper ne bi bio svestan da je veza raskinuta, što je problem sa više aspekata. Gejtkiper ne bi mogao proceniti trenutnu zauzetost propusnog opsega, a takođe ne bi mogao administrirati ni tarifirati pozive. Stoga se nakon raskidanja veze upotrebom H.225.0 kontrola poziva signalizacije, vrši raskidanje veze i RAS signalizacijom, pri čemu je preciznije reći da se RAS signalizacijom, ustvari, gejtkiper obaveštava o raskidu veze. Za obaveštavanje gejtkipera o raskidu veze se koriste poruke DRQ (*Disengage ReQuest*), DCF (*Disengage ConFirm*) i DRJ (*Disengage ReJect*). Kada terminal raskine vezu pomoću H.225.0 kontrola poziva signalizacije, terminal šalje DRQ poruku da obavesti gejtkiper o završetku veze (oba terminala u vezi će ovo uraditi). Gejtkiper potvrđuje sa DCF odgovorom. Gejtkiper odgovara DRJ porukom u slučaju kada primi DRQ poruku od terminala koji nije registrovan kod dotičnog gejtkipera. Pored terminala, i gejtkiper može da šalje DRQ poruku. Tada terminal bezuslovno odgovara sa DCF porukom i raskida vezu. Prethodno opisani način razmene ovih poruka je ilustrovan na slici 10.1.1.5.



Slika 10.1.1.6. Proces određivanja lokacije korisnika

Gejtkiper ili terminal mogu da zahtevaju informaciju o (mrežnoj) adresi tj. lokaciji određenog korisnika. Na primer, gejtkiper to može da traži od drugih gejtkipera u slučaju interzonskih poziva. U takvu svrhu se koristi LRQ (*Location ReQuest*) zahtev koji sadrži alijase traženog korisnika. LRQ zahtev se ili šalje na multikast adresu i UDP port kao i GRQ zahtev ili

se šalje konkretnom gejtkiperu na UDP port 1719. U prvom slučaju se ne zna ko je gejtkiper oblasti u kojoj se nalazi traženi korisnik čija se lokacija određuje pa se propituju svi gejtkiperi do kojih će stići paket adresiran na multikast adresu 224.0.1.41. U drugom slučaju se podrazumeva svojevrsna organizacija (hijerarhija) H.323 oblasti, pa se svakom gejtkiperu H.323 oblasti definiše nadređeni gejtkiper tj. oblast - hijerarhija gejtkipera, slično kao kod DNS servera. Gejtkiper stoga šalje LRQ upit svom nadređenom gejtkiperu, a ovaj dalje svom nadređenom gejtkiperu ako nema traženu informaciju i tako redom dok se ne dođe do rezultata ili do najvišeg gejtkipera koji će vratiti ili pozitivan rezultat ili negativan rezultat potrage. LCF (*Location ConFirm*) predstavlja pozitivan odgovor koji sadrži lokaciju tj. adresu traženog korisnika, a LRJ (*Location ReJect*) negativan odgovor (na primer, gejtkiper nije nadležan dotičnom terminalu). Primer razmene ovih RAS poruka za obe varijante je prikazan na slici 10.1.1.6. U prvoj varijanti, gejtkiper 1 šalje LRQ zahtev na multikast adresu 224.0.1.41 i ovaj zahtev primaju ostala tri gejtkipera. Gejtkiperi 2 i 3 vraćaju odgovor LRJ jer nemaju traženu informaciju, a gejtkiper 4 vraća LCF odgovor sa adresom traženog korisnika. U drugoj varijanti, gejtkiper 1 šalje LRQ zahtev gejtkiperu 2, koji pošto nema traženu informaciju, šalje LRQ zahtev gejtkiperu 3. Gejtkiper 3 takođe nema traženu informaciju pa šalje LRQ zahtev ka gejtkiperu 4 koji ima traženu informaciju jer je korisnik registrovan kod njega pa vraća LCF odgovor. LCF odgovor se potom šalje od gejtkiper 3 ka gejtkiperu 2 i potom od gejtkipera 2 ka gejtkiperu 1.

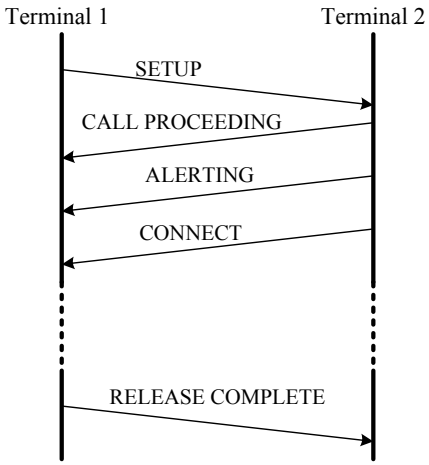
Kao što vidimo komunikacija u RAS signalizaciji je veoma jednostavna i sastoji se od razmene zahteva i odgovora, što je i razlog upotrebe UDP protokola. TCP protokol bi nepotrebno komplikovao prenos jer bi morale da se vrše i uspostave i raskidi TCP konekcije, a za ove kratke komunikacije to bi bilo nepotrebno tj. veoma neefikasno.

10.1.2. H.225.0 kontrola poziva signalizacija

H.225.0 kontrola poziva signalizacija se koristi za uspostavu, održavanje i raskid veze između korisnika i ona najvećim delom odgovara signalizaciji iz fiksne telefonije i ISDN mreže, što je i logično jer je zasnovana na Q.931 signalizaciji iz ISDN mreže. H.225.0 kontrola poziva signalizacija u suštini predstavlja podskup Q.931 signalizacije. Kao što smo već ranije naveli, H.225.0 kontrola poziva signalizacija se može razmenjivati direktno između korisnika ili kroz gejtkiper, a gejtkiper je taj koji odlučuje koji od ova dva principa će se koristiti. Pri tome, pre razmene signalizacije se prvo kreira TCP virtuelno kolo (uspostava TCP konekcije primenom trostrukog rukovanja) između terminala pozivajućeg i terminala traženog korisnika (direktna razmena signalizacije) ili gejtkipera (razmena signalizacije kroz gejtkiper). Pri tome, pozivajući terminal otvara TCP konekciju adresirajući IP adresu traženog terminala ili gejtkipera (zavisno koji metod razmene signalizacije se koristi) i TCP port 1720. TCP port 1720 je zadužen za osluškivanje H.225.0 kontrola poziva signalizacije. Nakon kreiranja virtuelnog kola, može se započeti sa razmenom H.225.0 kontrola poziva signalizacije preko dotičnog kola. Suprotna strana će slati signalizaciju (H.225.0 kontrola poziva) na IP adresu pozivajućeg terminala i TCP port koji koristi pozivajuća strana kao svoj izvorišni port u dotičnom virtuelnom kolu.

Poruke iz Q.931 signalizacije koje se mogu koristiti u H.323 kontrola poziva signalizaciji su: ALERTING, CALL PROCEEDING, CONNECT, PROGRESS, SETUP, SETUP ACK, RELEASE COMPLETE, USER INFORMATION, INFORMATION, NOTIFY, STATUS, STATUS ENQUIRY, FACILITY. Razlike u internoj strukturi ovih poruka koje unosi H.225.0 kontrola poziva signalizacija u odnosu na Q.931 preporuku su detaljno navedene u H.225.0 preporuci (napomenimo da razlike nisu velike). Pri tome, informacije specifične samo za H.323 mrežu se postavljaju u *user-user* informacionom elementu koji se stavlja u info polje, pri čemu

se sama korisna informacija ovog elementa predstavlja (kodira) primenom ASN.1 sintakse i PER kodiranja.



Slika 10.1.2.1. Primer uspostave i raskidanja veze H.225.0 kontrola poziva signalizacije

Prikažimo primer uspostave i raskida veze za slučaj kada se H.225.0 kontrola poziva signalizacija razmenjuje direktno između terminala (slika 10.1.2.1). Kao što vidimo, princip uspostave i raskida je uprošćen princip uspostave i raskida veze u ISDN mreži. Terminal 1 šalje SETUP poruku terminalu 2 čime signalizira da želi da uspostavi vezu sa njim. Terminal 2 šalje odgovor CALL PROCEEDING čime signalizira da je primio SETUP poruku i da je u toku njeno procesiranje. Zatim, terminal 2 šalje ALERTING poruku čime signalizira da se korisniku terminala 2 pušta obaveštenje da je tražen (da mu zvoni telefon ili da mu aplikacija na računaru pušta neko zvučno obaveštenje i sl.). Kada se traženi korisnik odazove, terminal 2 šalje CONNECT poruku kao signalizaciju da je uspostavljena veza (tj. da je faza uspostave u H.225.0 kontrola poziva završena) i potom kreće dogovor terminala o parametrima veze preko H.245 signalizacije. U CONNECT poruci terminal 2 ubacuje informaciju od IP adresi i TCP portu na kojima očekuje da primi H.245 signalizaciju od terminala 1. Raskid veze je veoma jednostavan. Raskid veze može da inicira bilo koja strana, a na slici je prikazana varijanta gde terminal 1 raskida vezu. Raskid se vrši slanjem poruke RELEASE COMPLETE. Posle nje bi oba terminala trebala da obaveste gejtkiper o kraju veze sa DRQ porukom iz RAS signalizacije. Napomenimo da prikazani primer važi za slučaj oblasti u kojoj ne postoji gejtkiper, ali i za slučaj gde se koristi gejtkiper, a signalizacija H.225.0 kontrola poziva se razmenjuje direktno između terminala. Inače, raskid veze može da inicira i gejtkiper ako se ova signalizacija (H.225.0 kontrola poziva) razmenjuje kroz gejtkiper.

10.1.3. H.245 signalizacija

H.245 signalizacija se razmenjuje nakon što je uspostavljena veza između korisnika preko H.225.0 kontrola poziva signalizacije, a pre same razmene korisnih signala. Kao što je ranije rečeno, H.245 signalizacija se može razmenjivati i tokom same veze. H.245 signalizacija omogućava terminalima da se dogovore oko parametara prenosa koji se biraju tako da oba terminala podržavaju dogovorene parametre prenosa. Otuda svaki terminal šalje u ovom procesu svoje tehničke mogućnosti u pogledu prijema i predaje (kodere koje podržava, protok koji podržava i dr.) i na osnovu poređenja primljenih tehničkih mogućnosti i sopstvenih tehničkih mogućnosti terminali određuju parametre prenosa. Kada se pregovori završe, terminali znaju parametre koji će se koristiti u vezi, poput kodeka govornog signala koji će se koristiti. Pošto se

može desiti da dođe do konflikta u komunikaciji (razmeni H.245 signalizacije) usled istovremenog slanja istih komandi obe strane, posle (ili za vreme) dogovora oko parametara prenosa, vrši se određivanje ko je nadležan (master) u komunikaciji da bi se ovi konflikti mogli jednoznačno rešiti. H.245 signalizacija takođe vrši otvaranje i zatvaranje unidirekcionih logičkih kanala koji se koriste za prenos korisnih signala (govor, video), pri čemu se za svaki tok ponaosob mora otvoriti logički kanal. Na primer, ako se šalju dva audio i jedan video signal, terminal će otvoriti tri unidirekciona logička kanala. Svaki terminal otvara logičke kanale za audio/video signale koje on šalje i taj terminal kontroliše otvaranje i zatvaranje tih kanala. To znači da u razgovoru gde obe strane šalju korisne informacije, svaka od strana će otvoriti unidirekcione logičke kanale za svoje signale koje šalju ka suprotnoj strani. U slučaju logičkih kanala koji će prenositi podatke moraju se otvoriti bidirekcioni logički kanali jer oni zahtevaju pouzdan prenos pa se mora koristiti TCP koji zahteva uspostavu bidirekcionog virtuelnog kola (logičkog kanala). Unidirekcioni logički kanali se odnose na tokove koje prenosi UDP protokol (na primer, RTP tokovi i njima pridruženi RTCP kontrolni tokovi, pri čemu jedan unidirekcioni logički kanal obuhvata i RTP tok i RTCP kontrolni tok koji kontroliše dotični RTP tok). Pored ovih osnovnih funkcija H.245 signalizacije, postoje i druge funkcije poput određivanja *round-trip* kašnjenja, signaliziranja aktivnosti/neaktivnosti signala govora ili video signala, i dr.

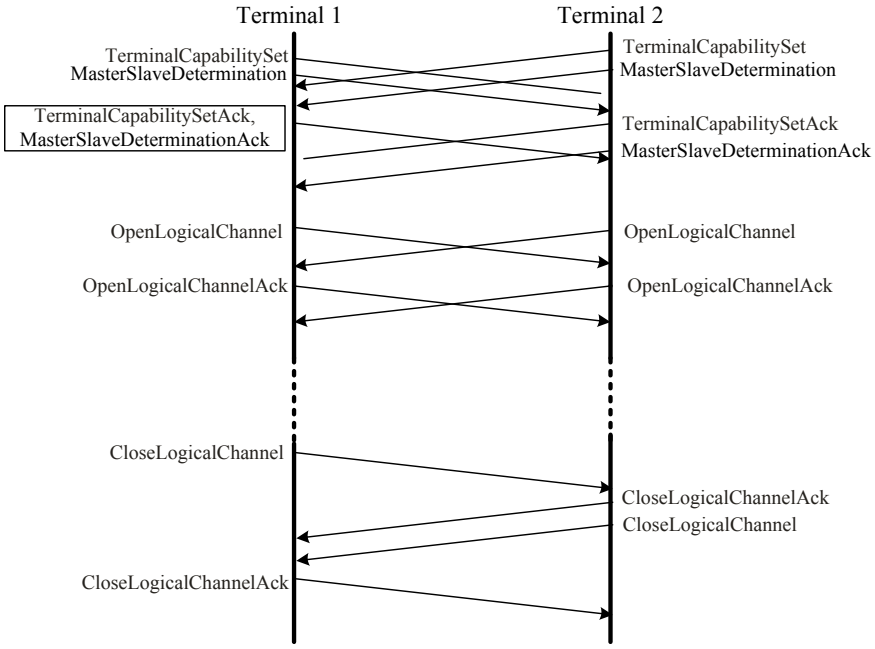
Sintaksa H.245 poruka je po ASN.1 notaciji, pri čemu se koristi poravnato PER kodiranje. H.323 predviđa i upotrebu tzv. ubrzane uspostave, u okviru koje se unutar H.225.0 kontrola toka poruka prenose i H.245 poruke da bi se ubrzao proces uspostave veze simultanim prenosom poruka obe signalizacije. SETUP poruka unutar sebe nosi informaciju da li se koristi ubrzani postupak ili ne.

Pre same razmene H.245 signalizacije je neophodno uspostaviti TCP virtuelno kolo između terminala (ako se H.245 signalizacija razmenjuje direktno između terminala) ili terminala i gejtkipera (ako se H.245 signalizacija razmenjuje kroz gejtkiper). U CONNECT poruci se nalazi informacija o IP adresi i TCP portu koji će koristiti tražena strana za razmenu H.245 signalizacije. Pozivajuća strana će izabrati svoj TCP port (tipično za jedan veći od broja TCP porta izabranog za H.225.0 kontrola poziva signalizaciju) za ovo virtuelno kolo. Pozivajuća strana pokreće proces kreiranja TCP virtuelnog kola i kada se formira virtuelno kolo može da otpočne razmena H.245 signalizacije. U slučaju kada se H.245 signalizacija razmenjuje preko gejtkipera, formira se virtuelno kolo između pozivajućeg korisnika i gejtkipera, kao i gejtkipera i traženog korisnika (isto kao i kod signalizacije H.225.0 kontrola poziva kada se ona razmenjuje preko gejtkipera). Tada će gejtkiper u CONNECT poruci koju šalje pozivajućem korisniku navesti TCP port na kome će očekivati prijem H.245 poruka koje šalje pozivajući korisnik.

Primer razmene H.245 poruka prilikom uspostave i raskida veze je prikazan na slici 10.1.3.1. Primer se odnosi na situaciju kada terminali direktno razmenjuju H.245 signalizaciju, a ne preko gejtkipera. Radi preglednosti, nazivi H.245 poruka su dati sa strane.

Na početku se vrši razmena podataka o tehničkim mogućnostima terminala. Svaki terminal šalje *TerminalCapabilitySet* poruku koju suprotna strana potvrđuje *TerminalCapabilitySetAck* porukom. *TerminalCapabilitySet* poruka sadrži podatke o tehničkim mogućnostima u pogledu predaje i prijema terminala. Na osnovu ove razmene svaka strana zna tehničke mogućnosti suprotne strane, tako da zna parametre tokova koje sme da šalje ka suprotnoj strani, a da ova to bude u stanju da primi (na primer, neće se slati G.729 kodiran govorni signal, ako suprotna strana može da prima samo G.711 kodiran govorni signal). Ovo oglašavanje tehničkih mogućnosti terminala se može ponovo vršiti i tokom veze, na primer,

ukoliko se želi oglasiti promena u tehničkim mogućnostima terminala (ustvari, ovime terminal želi da pređe na drugačije parametre tokova, na primer, da se koristi drugi koder govornog signala ili da se smanji protok).



Slika 10.1.3.1. Primer uspostave i raskidanja veze H.245 signalizacije

Posle razmene ili za vreme razmene tehničkih mogućnosti terminala (i time utvrđivanja tehničkih parametara veze), vrši se određivanje mastera i slejva u komunikaciji, tj. nadređene i podređene strane u komunikaciji. U datom primeru je prikazan slučaj u kome se uporedo sa razmenom tehničkih mogućnosti terminala vrši i određivanje nadređene/podređene strane u komunikaciji (što je češći slučaj jer skraćuje vreme signalizacije). Otuda oba terminala šalju poruku *MasterSlaveDetermination*, odmah nakon poruke *TerminalCapabilitySet*. Terminali po prijemu *MasterSlaveDetermination* poruke utvrđuju da li će biti master ili slejv i tu informaciju šalju u poruci *MasterSlaveDeterminationAck*. Utvrđivanje se vrši na osnovu nivoa važnosti terminala (pošto to može biti i gejtkiper, gejtvej ili multipoint kontrolna jedinica) tako da važniji entiteti postanu master. Na primer, multipoint kontrolna jedinica ima najveću važnost, što je i logično jer ako se ona koristi u pitanju je konferencijska veza pa je poželjno da ona bude master u komunikaciji. U slučaju istog nivoa važnosti, master se određuje poređenjem slučajnih brojeva koje generiše svaki od terminala (terminali šalju svoj slučajni broj u *MasterSlaveDetermination* poruci). Izbori bi trebali dati identičan rezultat - obe strane bi trebale izabrati identičan master, odnosno slejv (ako je terminal 1 utvrdio da je on master, a terminal 2 slejv, terminal 2 bi trebalo da utvrdi da je on slejv, a terminal 1 master). Jedan TCP paket (segment) može da sadrži više H.245 poruka. U primeru sa slike, terminal 1 šalje H.245 poruke *TerminalCapabilitySetAck* i *MasterSlaveDeterminationAck* u okviru istog paketa.

Nakon određivanja tehničkih mogućnosti terminala i određivanja nadređene i podređene strane u komunikaciji, svaka od strana otvara logički kanal upotrebom poruke *OpenLogicalChannel*, a suprotna strana vrši potvrđivanje porukom *OpenLogicalChannelAck*. U okviru poruke *OpenLogicalChannel* se navode osnovne informacije o toku koje su neophodne da bi prijemnik suprotne strane mogao korektno da prima dotični tok preko tog otvorenog logičkog

kanala. Na primer, koji tip informacije je u pitanju (na primer, govorni signal kodiran G.711 koderom). Svakom logičkom kanalu koji se otvori dodeljuje se jedinstven broj da bi se mogao jedinstveno razlikovati i ovaj broj se koristi u svim H.245 porukama koje se odnose na dotični logički kanal. U *OpenLogicalChannelAck* poruci, za slučaj unikast adresa i IP mreže, terminali navode na kom UDP portu i IP adresi će očekivati RTP pakete dotičnog otvorenog logičkog kanala, kao i na kom UDP portu i IP adresi će očekivati RTCP pakete (IP adresa je ista, a UDP port je za jedan veći od onog na kom će se primati RTP paketi). Ovo je i logično jer terminal koji šalje *OpenLogicalChannelAck* poruku predstavlja prijemni kraj unidirekcionog logičkog kanala pa je on taj koji treba da javi na kojim portovima i IP adresi će primati RTP i RTCP pakete na tom logičkom kanalu. U *OpenLogicalChannel* poruci terminali mogu da navedu na kom UDP portu i IP adresi će očekivati RTCP pakete od suprotne strane da bi se ostvarila povratna kontrolna sprega na dotičnom logičkom kanalu. Na osnovu rezultata razmene poruka *OpenLogicalChannel* i *OpenLogicalChannelAck* terminali znaju na koju IP adresu i UDP portove treba da šalju RTP i RTCP pakete koje kreiraju.

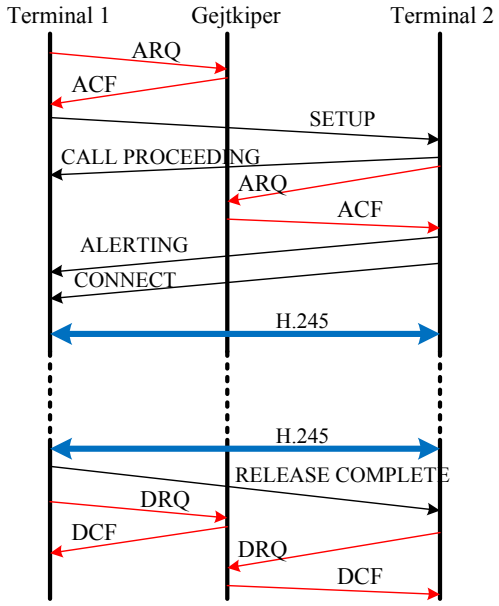
Zatvaranje logičkih kanala se vrši slanjem poruke *CloseLogicalChannel* na koju suprotna strana odgovara sa *CloseLogicalChannelAck* porukom. U prikazanom primeru logički kanali se zatvaraju jedan pa drugi, ali moglo je da se vrši i simultano zatvaranje (slično kao razmena tehničkih mogućnosti terminala u prikazanom primeru). Zatvaranje tipično vrši strana koja je i otvorila logički kanal, ali postoji i mogućnost da suprotna strana pokrene zahtev za zatvaranjem logičkog kanala (tada se koristi poruka *RequestChannelClose*). Takođe, nakon zatvaranja svojih logičkih kanala, terminal može da inicira raskid veze suprotnoj strani (da i ona zatvori svoje logičke kanale) H.245 porukom *EndSessionCommand*. Suprotna strana kada zatvori svoje logičke kanale odgovara takođe porukom *EndSessionCommand*. H.245 standard predviđa dve varijante raskidanja veze. U jednoj je dovoljno samo da obe strane zatvore svoje logičke kanale, a u drugoj se dodatno vrši i opisano slanje *EndSessionCommand* poruka.

10.1.4. Primeri intrazonskih veza

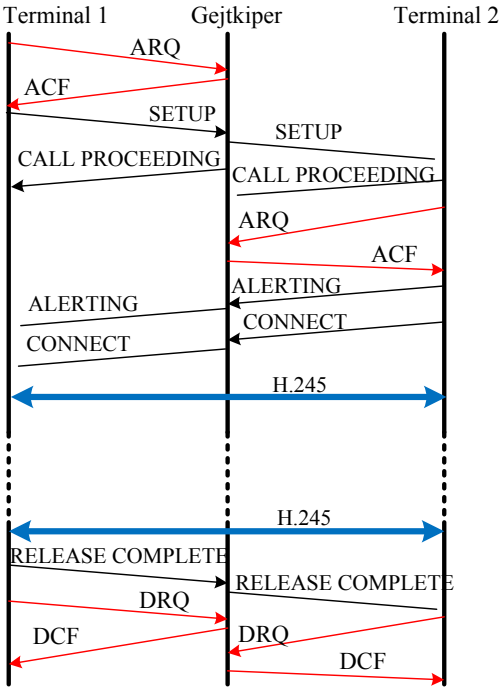
U ovoj sekciji ćemo prikazati sva tri moguća načina ostvarivanja intrazonskih veza (u svim primerima se koristi gejtkiper tj. posmatra se oblast sa gejtkiperom). Pri tome, H.245 signalizacija će biti prikazana zbirno radi bolje preglednosti. Oba terminala iz datih primera su već registrovana kod gejtkipera. Terminal 1 je pozivajući terminal, a terminal 2 je traženi terminal u svim datim primerima. Crvene linije predstavljaju RAS signalizaciju, plave H.245 signalizaciju, a crne kontrola poziva signalizaciju.

U primeru sa slike 10.1.4.1 se vrši samo razmena RAS signalizacije sa gejtkiperom, a H.225.0 kontrola poziva i H.245 signalizacija se razmenjuju direktno između terminala. Terminal 1 prvo traži dozvolu od gejtkipera ARQ porukom, a gejtkiper odobrava nastavak uspostave veze ACF porukom u kojoj šalje i IP adresu terminala 2. Sada terminal 1 zna IP adresu terminala 2 i ostale signalizacije može da razmeni direktno sa terminalom 2. Prvo šalje poruku SETUP, a terminal 2 javlja CALL PROCEEDING da bi terminal 1 znao da se SETUP poruka procesira. Terminal 2 prvo traži dozvolu od gejtkipera porukom ARQ, a gejtkiper odobrava zahtev sa ACF porukom tako da terminal 2 može da nastavi sa procesom uspostave veze. Terminal 2 šalje poruku ALERTING da bi obavestio terminal 1, da je pušten signal 'zvona' korisniku (šta je tačno signal 'zvona' zavisi od tipa terminala). Kada se korisnik odazove, terminal 2 šalje CONNECT poruku i potom kreće razmena H.245 signalizacije između terminala u okviru koje se otvaraju kanali za prenos govornog sadržaja (u datom primeru se ostvaruje telefonski razgovor). Nakon završetka razmene H.245 signalizacije kreće razgovor. Kada se veza

raskine, zatvaraju se kanali za prenos govornog sadržaja upotrebom H.245 signalizacije, a potom terminal 1 šalje RELEASE COMPLETE poruku (mogao je i terminal 2 da pošalje ovu poruku da je on raskidao vezu). Oba terminala šalju DRQ poruku da obaveste gejtkiper o kraju veze. Gejtkiper potvrđuje prijem DRQ poruka, DCF porukama.



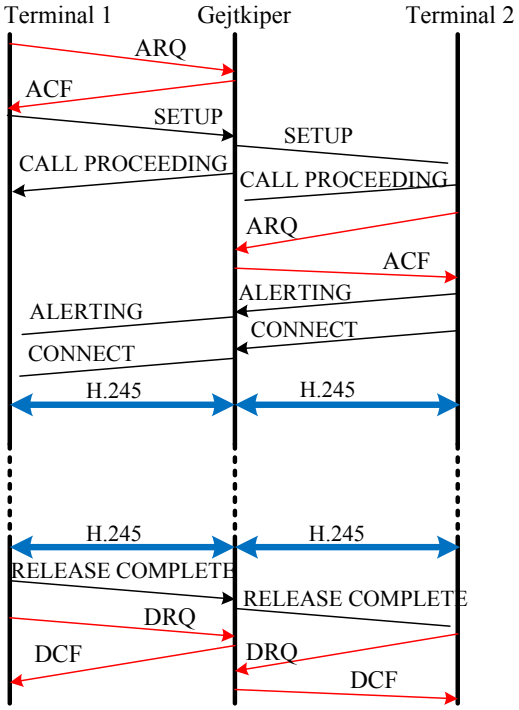
Slika 10.1.4.1. Primer ostvarivanja intrazonske direktne veze



Slika 10.1.4.2. Primer ostvarivanja intrazonske veze gde se RAS i kontrola poziva signalizacije razmenjuju preko gejtkipera

U primeru sa slike 10.1.4.2 se vrši razmena RAS i kontrola poziva signalizacije sa gejtkiperom, a H.245 signalizacija se razmenjuje direktno između terminala. Suštinska razlika u

odnosu na primer sa slike 10.1.4.2 je da terminali razmenjuju kontrola poziva signalizaciju sa gejtkiperom, tako da sa stanovišta te signalizacije gejtkiper izigrava traženog korisnika za pozivajućeg korisnika, odnosno pozivajućeg korisnika za traženog korisnika. Otuda se TCP virtuelno kolo za razmenu kontrola poziva signalizacije uspostavlja između pozivajućeg terminala i gejtkipera, kao i gejtkipera i traženog terminala.



Slika 10.1.4.3. Primer ostvarivanja intrazonske veze gde se sve tri signalizacije razmenjuju preko gejtkipera

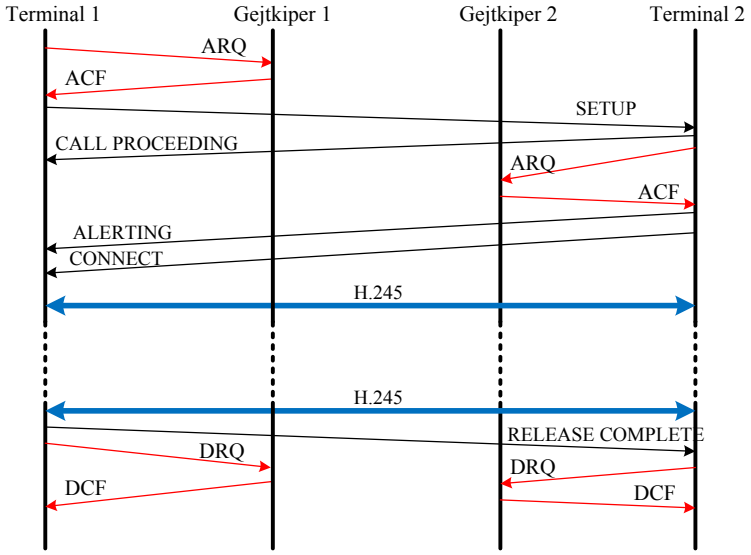
U primeru sa slike 10.1.4.3 se vrši razmena sve tri signalizacije sa gejtkiperom. U odnosu na prethodni slučaj, sada se i H.245 signalizacija razmenjuje preko gejtkipera. Ako se logički kanali otvore između terminala i gejtkipera, tada će i govorni signali (RTP paketi) da prolaze kroz gejtkiper (zgodna opcija ako se žele snimati razgovori, ali ova varijanta dodatno opterećuje gejtkiper). Ako se logički kanali otvore između terminala tada će govorni signali da se razmenjuju direktno između terminala.

10.1.5. Primeri interzonskih veza

U ovoj sekciji ćemo prikazati nekoliko primera uspostave interzonskih veza. Terminal 1 se nalazi u oblasti koju kontroliše gejtkiper 1, a terminal 2 u oblasti koju kontroliše gejtkiper 2. Pri tome, u primerima je terminal 1 pozivajuća strana, a terminal 2 tražena strana. U svim primerima se H.245 signalizacija razmenjuje direktno između korisnika, ali ona može da se razmenjuje i preko gejtkipera (tada bi se njena putanja razmene poklapala sa H.225.0 kontrola poziva signalizacijom). Takođe, u svim primerima pozivajući korisnik raskida vezu, ali to može da radi i traženi korisnik (tada bi RELEASE COMPLETE poruka išla po istom principu ali u suprotnom smeru). Oba terminala iz datih primera su već registrovana kod svojih nadležnih gejtkipera. Crvene linije predstavljaju RAS signalizaciju, plave H.245 signalizaciju, a crne kontrola poziva signalizaciju

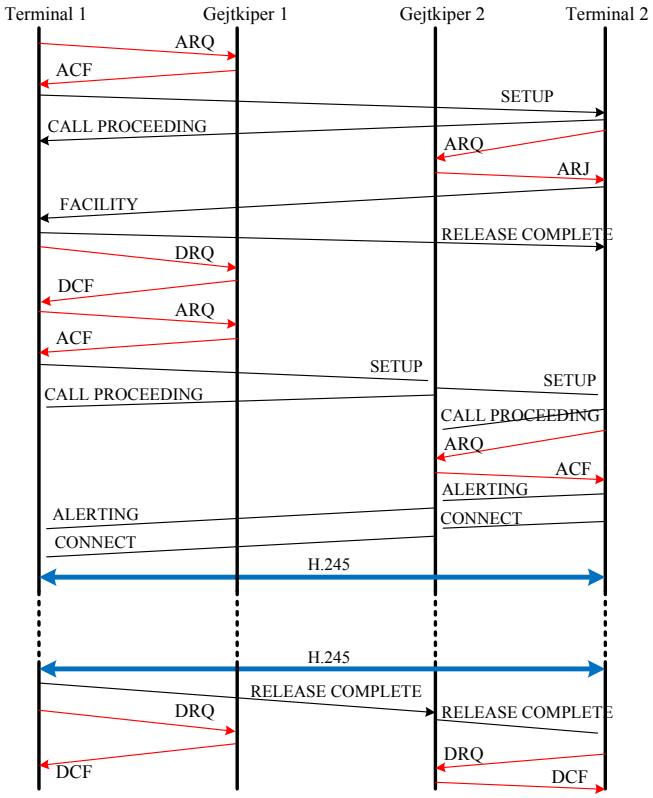
Na slici 10.1.5.1 je prikazan primer gde se H.225.0 kontrola poziva i H.245 signalizacije razmenjuju direktno između terminala. Terminal 1 se obraća svom gejtkiperu ARQ porukom za

dozvolu da ostvari vezu sa traženim korisnikom tj. terminalom 2. Gejtkiper 1 vraća adresu terminala 2 u ACF poruci kojom odobrava vezu i time signalizira terminalu 1 da H.225.0 kontrola poziva i H.245 signalizacije treba da se razmenjuju direktno između terminala. Gejtkiper 1 zna lokaciju terminala 2 tako što ju je saznao od gejtkipera 2. Gejtkiper 1 je poslao LRQ poruku kojom je tražio lokaciju terminala 2, i potom je dobio LCF odgovor od gejtkipera 2 koji mu je tako javio lokaciju (adresu) terminala 2. Ovaj proces razmene LRQ i LCF poruka nije prikazan na slici (nalazio bi se između trenutka prijema ARQ poruke od terminala 1 i trenutka slanja ACF poruke ka terminalu 1), ali proces odgovara nekom od dva metoda prikazanim na slici 10.1.1.6 (ovaj proces nalaženja adrese tj. lokacije traženog korisnika se vrši u svim prikazanim primerima ove sekcije). Terminal 1 šalje SETUP poruku terminalu 2 i nastavak razmene signalizacije je sličan kao u slučaju intrazonskog poziva gde se direktno razmenjuju H.225.0 kontrola poziva i H.245 signalizacije. Razlika je samo u RAS signalizaciji jer terminal 2 razmenjuje RAS signalizaciju sa gejtkiperom 2. Otuda traži dozvolu (ARQ) od gejtkipera 2 za nastavak uspostave veze, odnosno nakon raskida veze obaveštava gejtkiper 2 o kraju te veze (DRQ).



Slika 10.1.5.1. Primer ostvarivanja interzonske veze gde se H.225.0 kontrola poziva i H.245 signalizacije razmenjuju direktno između terminala

Na slici 10.1.5.2 je prikazan primer gde se H.225.0 kontrola poziva signalizacija razmenjuje kroz gejtkiper traženog korisnika (gejtkiper 2). Onog momenta kada terminal 2 zatraži dozvolu za nastavak veze, gejtkiper 2 u svojoj ARJ poruci navodi da želi da se signalizacija kontrola poziva razmenjuje preko njega i da je to razlog što nije dao dozvolu. Terminal 2 stoga porukom FACILITY obaveštava terminal 1 da razmena treba da ide kroz gejtkiper 2 i u okviru FACILITY poruke navodi (IP) adresu gejtkipera 2. Terminal 1 raskida vezu RELEASE COMPLETE porukom, i potom obaveštava gejtkiper 1 o raskidu veze sa DRQ porukom. Terminal 1 sada ponovo pokreće uspostavu veze i traži dozvolu od gejtkipera 1 slanjem ARQ poruke. Po dobijanju dozvole (ACF), terminal 1 šalje SETUP poruku ka gejtkiperu 2. Nastavak veze je sličan intrazonskoj vezi u kojoj signalizacija kontrola poziva ide preko gejtkipera (u ovom slučaju je u pitanju gejtkiper 2). Naravno, razlika je u tome što svaki terminal razmenjuje RAS signalizaciju sa svojim gejtkiperom.

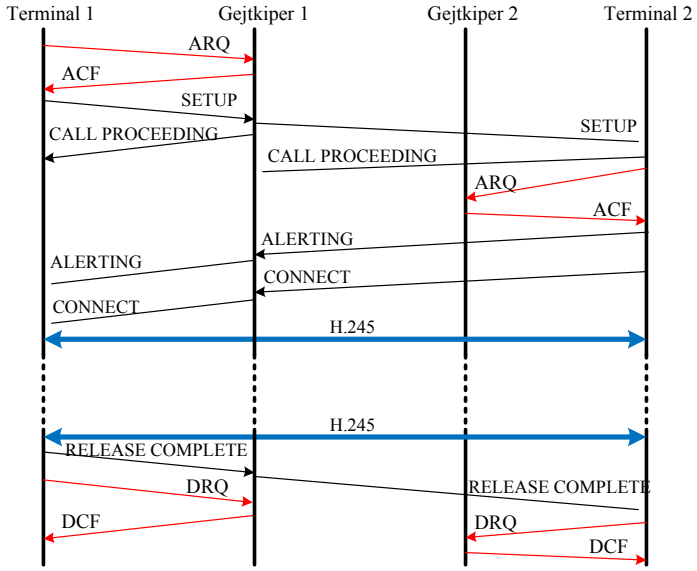


Slika 10.1.5.2. Primer ostvarivanja interzonske veze gde se H.225.0 kontrola poziva razmenjuje kroz gejtkiper traženog korisnika

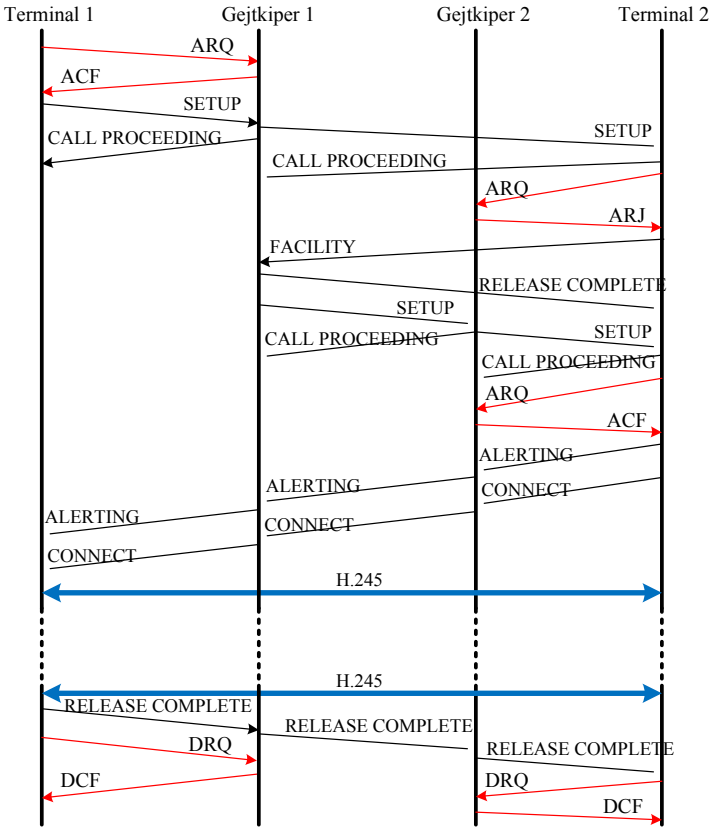
Na slici 10.1.5.3 je prikazan primer gde se H.225.0 kontrola poziva signalizacija razmenjuje kroz gejtkiper pozivajućeg korisnika (gejtkiper 1). Gejtkiper 1 u ACF poruci koju šalje ka terminalu 1 navodi da želi da se signalizacija kontrola poziva razmenjuje preko njega. Potom se signalizacija razmenjuje po sličnom principu kao u slučaju intrazonske veze u kojoj signalizacija kontrola poziva ide preko gejtkipera (u ovom slučaju je u pitanju gejtkiper 1). Naravno, razlika je u tome što svaki terminal razmenjuje RAS signalizaciju sa svojim gejtkiperom.

Na slici 10.1.5.4 je prikazan primer gde se H.225.0 kontrola poziva signalizacija razmenjuje kroz oba gejtkipera. Gejtkiper 1 je u ACF poruci naveo da želi da se signalizacija kontrola poziva razmenjuje preko njega. Nakon prosleđivanja SETUP poruke od gejtkipera 1 ka terminalu 2, terminal 2 šalje ARQ poruku ka gejtkiperu 2 da bi dobio dozvolu za nastavak uspostave veze. Međutim, gejtkiper 2 u ARJ poruci navodi da želi da se signalizacija kontrola poziva razmenjuje preko njega i da je to razlog što nije dao dozvolu. Stoga terminal 2 šalje FACILITY poruku ka gejtkiperu 1 u kojoj navodi da razmena mora da ide preko gejtkipera 2 (u poruci se navodi i IP adresa gejtkipera 2). Gejtkiper 1 raskida vezu sa RELEASE COMPLETE porukom i potom pokreće uspostavu veze preko gejtkipera 2 tako što mu šalje SETUP poruku. Gejtkiper 2 odgovara sa CALL PROCEEDING porukom, i šalje SETUP poruku ka terminalu 2. Terminal 2 odgovara sa CALL PROCEEDING porukom i potom sa porukom ARQ traži dozvolu za nastavak uspostave od gejtkipera 2 koji mu je odobrava ACF porukom. ALERTING poruka se potom šalje od terminala 2 ka gejtkiperu 2, pa potom od gejtkipera 2 ka gejtkiperu 1 i konačno od gejtkipera 1 ka terminalu 1. Kada se traženi korisnik odazove, na isti način se šalje i CONNECT poruka. Nakon toga kreće razmena H.245 signalizacije direktno između terminala.

Pozivajući terminal u jednom trenutku raskida vezu tako što se prvo izvršava raskidanje preko H.245 signalizacije, pa potom terminal 1 šalje RELEASE COMPLETE poruku gejtkiperu 1, koji je šalje ka gejtkiperu 2, a ovaj potom ka terminalu 2. Na kraju DRQ porukama terminali obaveštavaju svoje nadležne gejtkipere o završetku veze.



Slika 10.1.5.3. Primer ostvarivanja interzonske veze gde se H.225.0 kontrola poziva razmenjuje kroz gejtkiper pozivajućeg korisnika



Slika 10.1.5.4. Primer ostvarivanja interzonske veze gde se H.225.0 kontrola poziva razmenjuje kroz oba gejtkipera

10.2. SIP sistem signalizacije

SIP protokol je razvila IETF organizacija za potrebe kreiranja, modifikovanja i raskidanja multimedijalnih sesija u kojima učestvuje jedan ili više korisnika (očigledno se pod sesijom podrazumeva i puštanje multimedijalnog sadržaja koji može da prima samo jedan korisnik). SIP protokol je protokol aplikacionog sloja i definisan je u preporuci RFC 3261. Pošto je SIP protokol aplikacionog sloja, SIP mora da koristi usluge transportnog sloja. SIP može da koristi za prenos svojih poruka bilo koji od tri transportna protokola (TCP, UDP, SCTP) koji su na raspolaganju u IP mrežama. SIP protokol je nastao na osnovu potrebe za uvođenjem signalizacije neophodne za ostvarivanje interaktivne komunikacije poput telefonskih ili video razgovora. Naime, već su postojali protokoli za paketsku razmenu multimedijalnog sadržaja poput RTP i RTCP protokola, kao i za podršku striming multimedijalnog sadržaja (RTSP), ali je nedostajala signalizacija koja bi omogućila fleksibilniji okvir za kreiranje raznovrsnih aplikacija poput paketske telefonije (VoIP). Na primer, za ostvarivanje telefonskog poziva potrebno je prvo pronaći lokaciju korisnika (njegovu IP adresu) jer u IP mrežama korisnik često menja svoju IP adresu, naročito ako mu se ona dinamički dodeljuje što je čest slučaj pošto je IPv4 adresni prostor već devedesetih godina bio kritičan (ranije smo već napomenuli da je IPv4 prostor potrošen). Zatim, potrebno je obavestiti traženog korisnika da je tražen, a takođe potrebno je omogućiti traženom korisniku mogućnost da prihvati ili odbije vezu. Takođe, potrebno je omogućiti korisnicima da se dogovore o parametrima prenosa da bi uskladili svoju predaju i prijem sa mogućnostima suprotne strane. Sve ovo je nedostajalo u IP mrežama, pa je na osnovu toga prvo kreiran H.323 skup protokola od strane ITU-T organizacije. Međutim, ovaj skup protokola je obuhvatao i druge aspekte pored signalizacije - na primer, predviđao je standarde za kodere govornog signala, video signala, prenos podataka. Takođe, H.323 je bio predviđen za proizvoljnu paketsku tehnologiju, a ne samo IP, iako se ispostavilo da je IP tehnologija na kraju i postala dominantna. H.323 je bio i prilično kompleksan jer je, kao što smo mogli videti u prethodnom potpoglavlju, signalizacija praktično bila podeljena na tri celine. Iako se očekivalo da će H.323 popuniti prazninu nedostatka signalizacije za multimedijalnu komunikaciju i postati dominantan standard, ipak, se krenulo u razvoj SIP protokola u čijem razvoju su korišćena iskustva iz drugih aplikacionih protokola koji su zaživeli u IP mrežama poput HTTP (*Hyper Text Transport Protocol*) i SMTP (*Simple Mail Transport Protocol*) protokola. Ispostavilo se da je SIP adekvatnije prilagođen potrebama Internet mreže tj. korisnika, pa je preuzeo primat u odnosu na H.323 standard. Međutim, važno je naglasiti da konačnog pobednika između SIP i H.323 standarda nema, već se oba standarda i danas koriste u praksi.

SIP protokol je zasnovan na klijent-server principu koji je veoma popularan pristup u kreiranju aplikacija na Internetu. Klijent šalje zahtev serveru na koji, potom, server šalje odgovor klijentu. U slučaju SIP protokola, na klijentov SIP zahtev, server šalje jedan ili više SIP odgovora. Većina entiteta koji koriste SIP signalizaciju ima potrebu i da šalje i da prima zahteve, odnosno odgovore, stoga većina entiteta može da bude i klijent i server. Koja je trenutna uloga entiteta (klijent ili server) zavisi od trenutne komunikacije - da li trenutno šalje zahtev ili odgovor. Entiteti koji koriste (razmenjuju) SIP signalizaciju su:

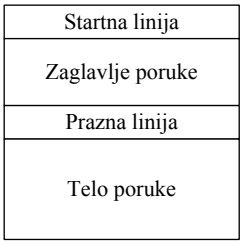
- Korisnički agent (*UA - User Agent*) - Korisnički agent, ustvari, predstavlja terminal (krajnji uređaj) poput IP telefona (koji se često označava terminom SIP telefon da se naglasi da radi sa SIP signalizacijom), video telefona ili računara sa instaliranim odgovarajućim aplikacijama. Korisnički agent u sebi sadrži i klijent

(*UAC - User Agent Client*) i server (*UAS - User Agent Server*) implementaciju, pošto može da se u komunikaciji ponaša i kao klijent (šalje zahteve) i kao server (šalje odgovore na primljene zahteve).

- Server prisutnosti (*Presence Server*) - Ovaj server prima i čuva podatke o trenutnoj prisutnosti korisnika. Na primer, korisnici mogu da se prijave da se trenutno nalaze kod svojih uređaja (na primer, računara) ili da se neće više nalaziti kod svojih računara, što može biti korisna informacija za korisnike koji žele da ih kontaktiraju. Takođe, korisnici mogu prijaviti i svoju trenutnu lokaciju poput 'u kancelariji', 'kod kuće', 'u labu' i sl. Ovakav tip informacije je pogodan za kvalitetnije odlučivanje koji kontakt korisnika izabrati ako ih je više ponuđeno (na primer, poseban telefonski broj za svaku od lokacija).
- Leđa u leđa korisnički agent (*B2BUA - Back-to-Back User Agent*) - Entitet koji prima zahtev i procesira ga kao UAS. Potom kreira novi SIP zahtev koji prosleđuje dalje ka drugom SIP entitetu da bi dobio SIP odgovor na osnovu kojeg će formirati odgovor koji će vratiti originalnom SIP entitetu koji je poslao prvobitni zahtev. Ovaj novi SIP zahtev šalje kao UAC. Kada primi SIP odgovor na svoj zahtev, ovaj uređaj formira SIP odgovor koji šalje entitetu koji je formirao prvobitni zahtev. B2BUA se može koristiti kao gejtvej ili za sakrivanje IP adresa (i drugih podataka) između krajnjih korisnika. Bitno je naglasiti da u SIP signalizaciji koja se odnosi na jednu vezu sve poruke (zahtevi i odgovori) moraju prolaziti kroz B2BUA, ako se B2BUA koristi u SIP signalizaciji između krajnjih uređaja.
- Gejtvej - Entitet koji omogućava komunikaciju SIP korisnika sa korisnicima iz drugih mreža (fiksna telefonija, H.323 mreža i dr.). Gejtvej vrši dvosmernu konverziju SIP signalizacije u (iz) signalizaciju koja se koristi u drugoj mreži (H.323, signalizacija No7). U slučaju ostanka u IP mreži (povezivanje SIP i H.323 mreže) konverzija korisničkih informacija (multimedije) nije obavezna, u suprotnom je potrebno izvršiti i konverziju korisničkih informacija. Kao što vidimo, gejtvej ima istu ulogu kao u H.323 mreži.
- Proksi server - Proksi server je zadužen za rutiranje SIP zahteva ka konačnom odredištu, odnosno SIP odgovora ka izvorištu SIP zahteva na koji se odgovor odnosi (odgovor prolazi kroz identičan put kao i zahtev, ali u suprotnom smeru). Za razliku od B2BUA, proksi server ne modifikuje SIP poruke, sem pojedinih polja što je neophodno za uspešno prosleđivanje (usmeravanje) SIP poruka, pa se otuda kaže za proksi server da vrši transparentan prenos SIP poruka. Za određivanje lokacija korisnika tj. korisničkih agenata koristi usluge lokacijskog servera koji čuva informacije o lokacijama korisnika, ali i usluge DNS servera za slučaj kada mora da uspostavi konekciju ka drugom proksi serveru u cilju da dođe do željenog korisnika tj. korisničkog agenta. Proksi server može da radi u modu sa memorijom i modu bez memorije. U modu bez memorije, proksi server samo prosleđuje zahteve na odgovarajući proksi server ili korisnički agent (uz potrebne modifikacije pojedinih polja poruke radi uspešnog prosleđivanja) i čim prosledi poruku odmah je zaboravlja. Ovaj mod je jednostavniji za implementaciju, ali ne omogućava dodatne servise korisnicima. U modu sa memorijom, proksi server

pamti primljeni zahtev i sve poslate zahteve koji su posledica procesiranja dotičnog primljenog zahteva, i ove informacije koristi u procesiranju budućih poruka koje su vezane za dotični zahtev. Ovaj mod je, na primer, neophodan kada proksi server račva primljeni zahtev na više odredišta da bi mogao kvalitetno da obradi odgovore i pošalje odgovor korisničkom agentu od koga je potekao originalni zahtev. Na primer, ako traženi korisnik ima više odredišta (adresa), može se poslati SIP poruka (tačnije zahtev) za uspostavom veze na sva odredišta i u zavisnosti od primljenih odgovora može se detektovati na kojoj adresi je traženi korisnik i tu adresu koristiti kao adresu traženog korisnika sa kojom će pozivajući korisnik uspostaviti vezu. Kao što vidimo iz ovog primera, mod sa memorijom je poželjan ako se želi kreirati podrška dodatnim servisima. Proksi server je najsličniji po svojoj funkcionalnosti gejtkiperu iz H.323 mreže.

- Preusmeravački server - Ovaj server vrši preusmeravanje SIP zahteva na sledeći način. On kao i proksi server vrši pretragu lokacijskog servera ili DNS servera, da bi našao adresu (lokaciju) traženog korisničkog agenta ili proksi servera i potom vraća odgovor izvorištu SIP zahteva u kome se navodi adresa entiteta kome treba poslati dotični SIP zahtev (koji je primio i na njega odgovorio preusmeravački server). Razlika u odnosu na proksi server je u tome što preusmeravački server ne vrši prosleđivanje SIP zahteva/odgovora, već samo vraća adresu entiteta na koju treba poslati SIP zahtev. Odgovor koji vraća preusmeravački server je iz grupe 3xx odgovora.
- Registracioni server - Ovaj server se još naziva i registrar. Korisnici se mogu registrovati na ovaj server sa ciljem da se pribeleži njihova lokacija tj. IP adresa koja se vezuje za njihov URI naziv (ili neki drugi alijas). Korisnik može prilikom registracije prijaviti i više svojih lokacija. Registracioni server može da zahteva autentifikaciju korisnika pre prihvatanja njihove registracije. Registracioni server na osnovu primljenih registracija ažurira lokacijski server koji čuva adrese (lokacije) SIP korisnika.
- Lokacijski server - Ovaj server čuva podatke o svim lokacijama SIP korisnika (tj. korisničkih agenata). Proksi i preusmeravački serveri koriste njegove usluge kao što smo već ranije naveli. Za jednog korisnika može biti vezano i više lokacija tj. adresa.



Slika 10.2.1. Struktura SIP poruke

U okviru SIP signalizacije se razlikuju SIP zahtevi i SIP odgovori. SIP zahtev šalje klijent serveru, a server odgovara sa jednim ili više SIP odgovora. Struktura SIP poruke za oba slučaja (zahtev, odgovor) je prikazana na slici 10.2.1. Kao što vidimo SIP poruka se sastoji od startne linije, zaglavlja poruke, prazne linije i tela poruke. Telo poruke je opciono tj. može i da

izostane iz poruke (prazna linija čak i u tom slučaju mora da postoji). Startna linija, sve linije u zaglavlju i prazna linija (svaka ponaosob) moraju da se završe CRLF (*Carriage Return, Line Feed*) karakterom.

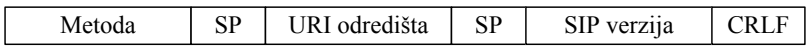
Sve SIP poruke koje se razmene u okviru jedne signalizacione veze čine jedan SIP dijalog. SIP dijalog se sastoji od transakcija. Jednu transakciju čine jedan SIP zahtev i svi SIP odgovori na dotični zahtev. Na jedan zahtev se može dobiti više odgovora, jer se razlikuju privremeni odgovori (odgovori grupe 1xx) i finalni odgovori (ostale grupe odgovora). Poseban slučaj čini INVITE zahtev na koji se dobija finalni odgovor koji ne pripada 2xx grupi odgovora jer tada i ACK zahtev, koji se šalje po prijemu finalnog odgovora, pripada toj transakciji koju je inicirao INVITE zahtev.

Kao što vidimo princip komunikacije je jednostavan i radi po klijent-server principu koji koriste mnogi popularni aplikacioni protokoli poput HTTP i SMTP. Princip transakcija omogućava upotrebu proizvoljnog transportnog protokola (pouzdanog ili nepouzdanog) jer se potvrđivanje proteže samo na jedan zahtev. Tipično se usled toga koristi jednostavniji UDP protokol, a TCP i SCTP protokol se koriste u slučaju predugačkih poruka koje ne mogu stati u jednu SIP poruku ili u slučaju kada je potrebno koristiti sigurnosne mehanizme. Ako se koriste TCP ili SCTP, tada se virtuelno kolo uspostavlja za jednu transakciju i potom, kada se transakcija završi, virtuelno kolo se raskida. Zahtev se smatra predugačkim ako je njegova dužina na 200 bajtova ili manje ispod vrednosti MTU (*Maximum Transmission Unit*) putanje, ili ako je dužina zahteva 1300 bajtova u slučaju nepoznate vrednosti MTU putanje (ova granica je formirana na osnovu MTU eternet okvira koji iznosi 1500 bajtova). MTU putanje predstavlja maksimalnu veličinu korisnog dela okvira na putanji kojom ide SIP zahtev. Ofset od 200 bajtova u odnosu na MTU veličinu se koristi jer odgovori mogu da imaju više bajtova od zahteva, ali se procenjuje da taj višak neće biti veći od 200 bajtova .

U nastavku teksta ćemo pod pojmom server podrazumevati UAS, a pod pojmom klijent ćemo podrazumevati UAC. Pri tome, pošto se pojam server javlja kod pojedinih entiteta (proksi server, preusmeravački server i dr.) ti entiteti će biti navođeni punim imenom da bi se izbegla dvosmislenost pojma server. Takođe, pod pojmom dijalog ćemo podrazumevati SIP dijalog, a pod pojmom sesija ćemo podrazumevati multimedijalnu sesiju za koju se razmenjuje SIP signalizacija.

10.2.1. Startna linija SIP zahteva

Struktura startne linije SIP zahteva je prikazana na slici 10.2.1.1. Sa SP je označen jedan *space* karakter. Startna linija zahteva se završava CRLF karakterom kako smo i naveli u opisu strukture SIP poruke.



Slika 10.2.1.1. Struktura startne linije SIP zahteva

Metoda definiše sam zahtev tj. predstavlja tip zahteva. Većina tipova zahteva (metoda) je definisana u okviru osnovne preporuke za SIP protokol (RFC 3261), a ostale su definisane u naknadnim RFC preporukama koje proširuju osnovnu SIP preporuku (RFC 3261). Spisak svih metoda koje su standardizovane se može naći na http://www.iana.org/assignments/sip-parameters/sip-parameters.xhtml. Neke od standardizovanih metoda su (za metode koje nisu definisane u RFC 3261 će biti naveden RFC u kome su definisane):

- INVITE - Metoda kojom se otvara uspostava veze (ekvivalent SETUP poruke iz H.323). Korisnik koji šalje INVITE zahtev, nakon prijema definitivnog odgovora od traženog korisnika (na INVITE zahtev traženi korisnik može da pošalje više od jednog odgovora kao što ćemo i videti nešto kasnije) kojim se prihvata ili ne prihvata INVITE zahtev (tj. komunikacija) obavezno šalje ACK zahtev. INVITE zahtev se može iskoristiti i za promenu parametara veze u toku trajanja multimedijalne sesije (veze). Takav INVITE zahtev se naziva i ponovni INVITE zahtev.
- REGISTER - Metoda kojom se vrši registracija korisnika (na registrar). Ovim zahtevom korisnik javlja svoju lokaciju (IP adresu) na koju mogu da ga dobiju ostali korisnici. Korisnik može registrovati i više lokacija preko kojih je dostupan.
- BYE - Metoda kojom se okončava tj. raskida veza.
- ACK - Metoda kojom se potvrđuje poslednji (definitivni) odgovor na INVITE zahtev.
- CANCEL - Metoda kojom se raskida veza čija je uspostava u toku.
- OPTIONS - Metoda kojom se traže mogućnosti entiteta koji je adresiran kao odredište u OPTIONS zahtevu. Ovaj zahtev se može iskoristiti i za ispitivanje trenutne dostupnosti entiteta.
- REFER - Metoda kojom klijent od servera (koji je adresiran kao odredište u zahtevu) zahteva da pristupi trećoj destinaciji koja je navedena u vidu URL ili URI identifikatora. Ova metoda je definisana u RFC 3515. Ova metoda je uvedena da bi omogućila servise poput transfera poziva (transfer poziva podrazumeva da u slučaju veze dva korisnika, jedan od korisnika u vezi prebaci poziv (sa sebe) na trećeg korisnika).
- SUBSCRIBE - Metoda kojom se (zajedno sa NOTIFY metodom) omogućava mehanizam obaveštavanja između SIP čvorova o asinhronim događajima. SUBSCRIBE zahtevom korisnik od suprotne strane zahteva trenutno stanje i sva buduća ažuriranja (promene) stanja. Suprotna strana koristi NOTIFY zahtev za slanje promena stanja. Na primer, korisnik može SUBSCRIBE metodom da se prijavi na server govorne pošte (koji ima SIP funkcionalnost). Ovaj server će svaki put kada stigne nova poruka u govornu poštu korisnika da pošalje NOTIFY poruku korisniku kojom ga obaveštava o ovom događaju. Postoje i druge primene, poput automatskog ponovnog poziva (ovaj servis je opisan u poglavlju 6). Ova metoda je definisana u RFC 6665 (prvobitno su SUBSCRIBE i NOTIFY metode bile definisane u RFC 3265, ali je RFC 6665 zamenio ovu preporuku).
- NOTIFY - Metoda koja se koristi u paru sa SUBSCRIBE zahtevom kao što je navedeno kod SUBSCRIBE zahteva. NOTIFY zahtev prenosi obaveštenja o promenama stanja tj. pojavi asinhronih događaja. NOTIFY metoda se koristi u sprezi i sa nekim drugim metodama poput REFER metode. Ova metoda je definisana u RFC 6665.
- MESSAGE - Metoda koja se koristi za slanje instant poruka pomoću SIP signalizacije. Ova metoda se može koristiti unutar dijaloga, ali standard

preporučuje da se za razmenu instant poruka ne formira dijalog u kojem bi se samo razmenjivale instant poruke. Otuda se tipično bez ikakve uspostave dijaloga INVITE zahtevom, samo vrši slanje MESSAGE zahteva koji u svom telu poruke nosi instant poruku, i potom slanja odgovora sa suprotne strane kojim se potvrđuje prijem MESSAGE zahteva. Za slanje instant poruka se, inače, može oformiti i multimedijalna sesija koja bi, ustvari, predstavljala sesiju preko koje bi se prenosile instant poruke. Ova metoda je definisana u RFC 3428.

- UPDATE - Metoda kojom se vrši ažuriranje parametara sesije (veze koja se uspostavlja) pre njenog uspostavljanja. Naime, kada je veza uspostavljena, INVITE metodom se mogu modifikovati parametri sesije, ali dok je uspostava u toku ne smeju se slati INVITE zahtevi dok se na inicijalni INVITE zahtev ne dobije konačni odgovor. Stoga se u tom periodu uspostave veze koriste UPDATE poruke za modifikovanje tj. ažuriranje parametara sesije. Ova metoda je definisana u RFC 3311.
- INFO - Metoda koja omogućava slanje poruka između aplikacija (krajnjih tačaka) preko SIP signalizacionog dijaloga za vreme trajanja uspostavljene multimedijalne sesije. Postoji više primena ovog metoda, poput enkapsulacije QSIG poruka, enkapsulacije ISUP poruka, enkapsulacije DTMF tonova, itd. Ova metoda je definisana u RFC 6086.
- PRACK - Metoda koja se koristi za potvrđivanje odgovora iz grupe 1xx, sem odgovora 100. Odgovori iz grupe 1xx predstavljaju privremene odgovore, a ne finalne odgovore (na primer, odgovor 180 označava da traženom korisniku zvoni telefon, ali to nije definitivan odgovor da li će veza biti uspostavljena ili ne). Finalni odgovori u procesu uspostave veze su potvrđeni ACK zahtevom. Ova metoda je definisana u RFC 3262.

URI odredišta predstavlja URI krajnjeg odredišta kojem je SIP zahtev namenjen. URI je tipično u formatu 'sip' ili 'sips', ali RFC 3261 dozvoljava i upotrebu drugih formata. Primer URI-ja u 'sip' formatu (tzv. SIP URI) je *sip:petar.petrovic@etf.rs*. Format 'sips' (tzv. *Secure SIP URI*) se koristi kad se želi obezbediti enkripcija (zaštita) s kraja na kraj. Format je sličan 'sip' formatu samo se stavlja *sips* umesto *sip* (na primer, *sips:petar.petrovic@etf.rs*). Opšta struktura SIP URI formata je:

sip:user:password@host:port;uri-parameters?headers

SIP URI format se sastoji iz sledećih delova:

- *sip* - Stavlja se na početak da bi označio upotrebu 'sip' formata. Da je stavljena vrednost *sips*, time bi bila označena upotreba 'sips' formata.
- *user* - Označava identifikaciju određenog korisnika na hostu definisanom u *host* delu.
- *password* - Označava lozinku korisnika označenog u *user* delu. Iako predviđen strukturom SIP URI formata, iz sigurnosnih razloga *password* se izostavlja (sam RFC 3261 preporučuje izostavljanje). Nije preporučljivo slati lozinku na ovaj način jer bi presretanjem SIP zahteva napadač saznao lozinku traženog korisnika.

- *host* - Označava host na kome se nalazi korisnik označen u *user* delu. Host može biti domen u kome se korisnik nalazi pa se tada u *host* deo stavlja ime domena. Ako se želi navesti i sam host (uređaj) na kome se korisnik nalazi tada se uz ime domena stavlja i naziv hosta (na primer, *host33.etf.rs*, gde je *host33* ima hosta u domenu *etf.rs* - u suštini *host33.etf.rs* takođe predstavlja ime domena). Takođe, IPv4 ili IPv6 adresa se takođe mogu staviti u host deo. RFC 3261 preporučuje da se koristi ime domena kad god je to moguće.
- *port* - Broj porta (TCP, UDP ili SCTP) na koji treba poslati zahtev. Ako se vrednost porta ne navede podrazumeva se vrednost 5060 ili 5061. Vrednost 5061 se koristi ako se koriste mehanizmi zaštite ('sip' format pri čemu se koristi TLS (*Transport Layer Security*) preko TCP-a ili 'sips' format)
- *uri-parameters* - Dodatni parametri koji se odnose na zahtev. Parametri se navode u formatu *naziv parametra = vrednost parametra*. Ako ima više parametara, oni se međusobno razdvajaju tačka-zarezom (;). Ne sme više od jednom da se pojavi isti naziv parametra (tj. isti parametar) u SIP URI-ju. Parametri predviđeni RFC 3261 preporukom su *transport*, *maddr*, *ttl*, *user*, *method* i *lr*. Pored ovih parametara moguće je koristiti i druge parametre. U slučaju da entitet koji procesira zahtev ne razume neki parametar, tada taj entitet samo ignoriše dotični parametar. Parametar *transport* definiše koji transportni protokol se koristi (UDP, TCP, TLS ili SCTP - TLS označava TLS preko TCP). U slučaju *Secure SIP URI*-ja mora se koristiti TCP ili SCTP. Ako se parametar *transport* ne navede, tada se podrazumeva difolt vrednost UDP za 'sip' format, odnosno TCP za 'sips' format. Parametar *maddr* predstavlja adresu proksi servera kroz koji mora proći dotični zahtev čime se obezbeđuje svojevrsno upravljanje rutom poruke do konačnog odredišta jer se na ruti mora naći dotični proksi server. Tada se vrednost porta i parametra *transport* vezuju za adresu proksi servera navedenog u *maddr* parametru i na osnovu ta tri podatka se kreira datagram koji se šalje u mrežu i koji treba prvo stići do proksi servera čija je adresa navedena u *maddr* parametru. RFC 3261 preporučuje da se ne koristi *maddr* parametar u dotičnu svrhu, već da se koriste alternativni mehanizmi opisani u RFC 3261. Parametar *ttl* se koristi samo ako je u *maddr* parametru navedena multikast adresa i pri tome se koristi UDP kao transportni protokol. Tada ovaj parametar označava maksimalan broj hopova dotičnog zahteva pre nego što dođe do njegovog odbacivanja. Parametar *user* se koristi da označi da je u *user* deo stavljena vrednost koja treba da se tumači kao telefonski broj, a ne kao korisničko ime (tada *user* parametar ima vrednost *phone*, čime se signalizira da je u *user* deo stavljen telefonski broj - na primer, +381-11-3221-457). Parametar *method* se koristi za kreiranje SIP zahteva na osnovu SIP URI-ja, pri čemu ovaj parametar navodi metodu tj. tip SIP zahteva. Parametar *lr* signalizira da dotični entitet (čiji je SIP URI u pitanju) podržava labavo rutiranje koje ćemo nešto kasnije objasniti.
- *headers* - Definiše vrednosti polja zaglavlja koja će se staviti u SIP zahtev koji se kreira na osnovu SIP URI-ja. Vrednosti polja zaglavlja se navode u formatu *naziv polja = vrednost polja*.

Bitno je naglasiti da se, u slučaju da se SIP URI ili *Secure SIP URI* koriste kao URI odredišta, ne sme koristiti parametar *method*, ni *headers* deo. Takođe, tada je samo *host* deo obavezan, a svi preostali delovi/parametri su opcioni. Sintaksna pravila vezana za URI identifikatore se mogu pronaći u RFC 2396. Nekoliko primera SIP URI identifikatora je dato u tabeli 10.2.1.1.

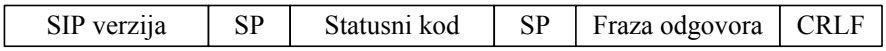
Tabela 10.2.1.1 - Primeri SIP URI identifikatora

SIP URI	Komentar
sip:petar.petrovic@etf.rs	
sip:milan:lozinkax@etf.rs;transport=tcp	U URI je navedena lozinka *lozinkax*, i koristi se TCP kao transportni protokol
sip:+381-11-3221-457@telco.com;user=phone	Stavljen je telefonski broj u user deo, pa je morao da se navede parametar *user* sa vrednošću *phone*
sip:+381-11-3221-457:4214@telco.com;user=phone	U odnosu na prethodni primer je dodata i lozinka korisnika koja se sastoji samo od cifara jer telefon jedino njih može da unosi
sip:kancelarija19@192.0.2.4:4428	Umesto imena domena navedena je IP adresa, a takođe je naveden i port na kojem se očekuje prijem
sip:ana@etf.rs:5060;transport=udp;user=ip; method=INVITE;?Subject=nagrada	Primer SIP URI na osnovu koga treba da se kreira zahtev INVITE

SIP verzija označava verziju SIP implementacije koju koristi entitet koji je kreirao zahtev. Format ispisa verzije je preuzet iz HTTP protokola, pri čemu SIP implementacija koja implementira preporuku RFC 3261 ima verziju 2. Otuda, u svim današnjim implementacijama bi u polju SIP verzija trebalo da stoji *SIP/2.0*.

10.2.2. Startna linija SIP odgovora

Struktura startne linije SIP odgovora je prikazana na slici 10.2.2.1. Sa SP je označen jedan *space* karakter. Startna linija odgovora se završava CRLF karakterom kako smo i naveli u opisu strukture SIP poruke.



Slika 10.2.2.1. Struktura startne linije SIP odgovora

SIP verzija se navodi u istom formatu kao u slučaju SIP zahteva. Statusni kod predstavlja kod odgovora, dok fraza odgovora predstavlja tekstualni opis odgovora. Većina odgovora je definisana u okviru osnovne preporuke za SIP protokol (RFC 3261), a ostali su definisani u naknadnim RFC preporukama koje proširuju osnovnu SIP preporuku (RFC 3261). Spisak svih odgovora koji su standardizovani se može naći na http://www.iana.org/assignments/sip-parameters/sip-parameters.xhtml. Odgovori se mogu podeliti u sledeće grupe odgovora (nazivi odgovora dati u zagradama pored statusnog koda odgovora tipično predstavljaju frazu odgovora ili deo fraze odgovora), pri čemu će za odgovore koji nisu definisani u RFC 3261 biti naveden RFC u kome su definisani:

- 1xx - Informativni (privremeni) odgovori kojima se signalizira da je zahtev prihvaćen i da je u toku njegovo procesiranje. Odgovori iz ove grupe su:
  - 100 (*Trying*) - Ovim odgovorom se signalizira primanje i procesiranje zahteva. Koristi se da bi se izbegle nepotrebne retransmisije zahteva (ako se dovoljno dugo ne dobije odgovor dolazi do retransmisije zahteva).

- 180 (*Ringing*) - Ovim odgovorom se signalizira da se traženi korisnik (koji je primio INVITE zahtev) obaveštava o pozivu ('zvoni' mu telefon).
- 181 (*Call Is Being Forwarded*) - Ovim odgovorom se signalizira da je poziv prosleđen na jednu ili više drugih destinacija.
- 182 (*Queued*) - Ovim odgovorom se signalizira da je zahtev primljen, ali trenutno ne može da se opsluži. Međutim, zahtev nije odbijen, već stavljen u red za čekanje. Fraza odgovora može da sadrži informaciju o broju zahteva koji se nalaze u redu za čekanje i procenu vremena čekanja. Na primer, *3 calls queued; expected waiting time is 5 minutes*.
- 183 (*Session Progress*) - Ovim odgovorom se signalizira da je procesiranje u toku, pri čemu nijedan od prethodno opisanih 1xx odgovora nije adekvatan, pa se može reći da odgovor 183 predstavlja sve slučajeve koji nisu pokriveni preostalim 1xx odgovorima. Informacije o progresu procesiranja mogu da se navedu u frazi odgovora, telu poruke ili u poljima zaglavlja poruke.

- 2xx - Pozitivni odgovori kojima se signalizira uspešna obrada zahteva (zahtev je primljen, razumljiv i prihvaćen). Odgovori iz ove grupe su:
  - 200 (*OK*) - Ovim odgovorom se signalizira uspešna obrada zahteva. Informacija koja se nalazi u telu poruke zavisi od tipa zahteva na koji se odgovara. Na primer, u slučaju odgovora na INVITE zahtev, telo poruke će sadržati parametre prenosa prijemnika (mogućnosti prijemnika). Telo poruke neće postojati ako se ovaj odgovor šalje na zahteve CANCEL, INFO, MESSAGE, SUBSCRIBE, NOTIFY, PRACK.
  - 202 (*Accepted*) - Ovaj odgovor je originalno zamišljen kao odgovor koji bi se koristio u sprezi sa SUBSCRIBE i NOTIFY zahtevima, a kasnije se definisala sprega i sa drugim metodama poput REFER. Međutim, u praksi se pokazalo da se njegova upotrebna vrednost ne razlikuje mnogo od one koja bi se postigla odgovorom 200, a čak su i primećene nekompatibilnosti između različitih implementacija. Otuda je preporuka da se ovaj odgovor više ne generiše, a ako se primi (od starijih implementacija), treba da se tretira kao odgovor 200. Ovaj odgovor je originalno definisan u RFC 3265 koji je potom zamenjen sa RFC 6665 u kome je preporučeno da se ne treba više generisati odgovor 202.
- 3xx - Preusmeravački odgovori kojima se signalizira nova lokacija traženog korisnika ili alternativni servisi kojima bi se mogao alternativno ispuniti zahtev korisnika (na primer, mejl servis ili govorna pošta). Odgovori iz ove grupe su:
  - 300 (*Multiple Choices*) - Za korisnika je vezano više lokacija, pa se ovim odgovorom vraća lista lokacija da pozivajući korisnik sam izabere adresu (lokaciju) koju će pozvati da bi došao do traženog korisnika. Naravno, ovaj odgovor se vraća ako proksi server ne želi sam da izabere lokaciju traženog korisnika koju će nazvati (jer proksi server nije tako programiran).

- 301 (*Moved Permanently*) - Traženi korisnik se više ne nalazi na adresi navedenoj u URI odredišta koja se nalazi u startnoj liniji zahteva, i u odgovoru se vraća nova adresa korisnika koju treba koristiti u budućim komunikacijama sa njim.
- 302 (*Moved Temporarily*) - Traženi korisnik se ne nalazi na adresi navedenoj u URI odredišta koja se nalazi u startnoj liniji zahteva, i u odgovoru se vraća nova (privremena) adresa korisnika koju treba koristiti u komunikaciji sa njim. U ovom odgovoru se može nalaziti vrednost trajanja privremene adrese i dok ne istekne to vreme ova privremena adresa se može koristiti u budućim komunikacijama sa tim traženim korisnikom. Ako vrednost trajanja nije navedena, onda se privremena adresa može samo trenutno (odmah) iskoristiti.
- 305 (*Use Proxy*) - Poziv mora da ide kroz proksi server naveden u odgovoru, pa je stoga pozivajući korisnik dužan da ponovo pošalje zahtev, ali sada preko navedenog proksi servera.
- 380 (*Alternative Service*) - Poziv nije mogao da se uspešno uspostavi, ali ovim odgovorom se nude alternativni servisi (koje nudi traženi korisnik) koji mogu da se iskoriste za (svojevrsni) kontakt sa traženim korisnikom, poput govorne pošte. Alternativni servisi se navode u telu poruke.

- 4xx - Odgovori koji signaliziraju greške na klijent strani (koja je i slala zahtev). Na primer, klijentov zahtev sadrži sintaksne greške ili klijentov zahtev traži od servera nešto što server ne može da uradi. Odgovor iz ove grupe definitivno odbija primljeni zahtev. Zahtev se ne sme ponovo slati istom serveru, a da prethodno nije modifikovan tako da se koriguje greška koja je signalizirana odgovorom iz ove grupe. Odgovori ove grupe su:
  - 400 (*Bad Request*) - Ovim odgovorom se signalizira greška u sintaksi zahteva. Na primer, ne postoji prazna linija. Fraza odgovora bi trebala da sadrži detalje o detektovanoj sintaksnoj grešci.
  - 401 (*Unauthorized*) - Ovaj odgovor signalizira da korisnik (klijent) mora da se autentifikuje da bi se zahtev mogao izvršiti. Ovaj odgovor šalje server ili registrar, dok u identičnoj situaciji proksi server šalje odgovor 407.
  - 402 (*Payment Required*) - Ovaj odgovor je rezervisan za buduću upotrebu i očigledno je predviđen za situacije u kojoj servis mora da se plati.
  - 403 (*Forbidden*) - Server je primio i razumeo zahtev, ali odbija da ga izvrši.
  - 404 (*Not Found*) - Ovaj odgovor signalizira da traženi korisnik sigurno ne postoji u domenu koji je naveden u URI odredišta startne linije zahteva ili da sam domen ne postoji.
  - 405 (*Method Not Allowed*) - Server je primio i razumeo zahtev, ali dotični zahtev nije podržan. Na primer, korisnički agent je primio REGISTER zahtev. U odgovoru se nalazi i lista metoda koje server podržava.

- 406 (*Not Acceptable*) - Ovim odgovorom server signalizira klijentu da procesiranje njegovog zahteva ne može da se izvrši jer ne podržava opcije navedene u *Accept* polju zaglavlja.
- 407 (*Proxy Authentication Required*) - Odgovor ekvivalentan odgovoru 401, samo ga u ovom slučaju šalje proksi server (klijent mora prvo da se autentifikuje kod proksi servera).
- 408 (*Request Timeout*) - Server nije mogao da izvrši zahtev u određenom vremenskom okviru (definisan u *Expires* polju zaglavlja dotičnog zahteva). Klijent može kasnije da ponovi ovaj zahtev u neizmenjenom obliku.
- 410 (*Gone*) - Traženi korisnik se više ne nalazi u navedenom domenu (koji je naveden u okviru URI odredišta), pri čemu se ne zna njegova nova lokacija. Server je siguran da je ovo stanje permanentno (korisnik sigurno nije više u tom domenu), u suprotnom bi server poslao 404 odgovor.
- 413 (*Request Entity Too Large*) - Ovim odgovorom se signalizira da je telo poruke unutar primljenog zahteva predugačko i da server stoga neće da ga procesira.
- 414 (*Request-URI Too Long*) - Ovim odgovorom se signalizira da je URI odredišta predugačak i da ga stoga server ne može procesirati.
- 415 (*Unsupported Media Type*) - Ovim odgovorom se signalizira da je telo poruke zahteva u formatu koji server ne može da procesira. U okviru ovog odgovora se vraća lista podržanih formata upotrebom polja zaglavlja *Accept*, *Accept-Encoding*, ili *Accept-Language* u zavisnosti koji problem u formatu je detektovao server.
- 416 (*Unsupported URI Scheme*) - Ovim odgovorom se signalizira da format korišćen za URI identifikator nije podržan od strane servera. Na primer, u zahtevu se koristio format *tel* (*Telephone URI*) koji server ne podržava.
- 420 (*Bad Extension*) - Ovim odgovorom se signalizira da server nije prepoznao ekstenziju protokola navedenu u polju zaglavlja *Proxy-Require* ili *Require* primljenog zahteva. U ovom odgovoru server navodi listu nepodržanih ekstenzija (one se stavljaju u polje zaglavlja *Unsupported*).
- 421 (*Extension Required*) - Ovim odgovorom se signalizira da u zahtevu nije navedena određena ekstenzija protokola (u polju zaglavlja zahteva *Supported*), a bez koje server ne može da procesira zahtev. Odgovor vraća listu zahtevanih ekstenzija u okviru polja zaglavlja *Required*. Pre nego što se ovaj odgovor vrati, server mora da pokuša da procesira zahtev koristeći difolt podešavanja, kao i sve ekstenzije navedene u *Supported* polju zaglavlja zahteva, a koje server podržava.
- 422 (*Session Timer Interval Too Small*) - Ovim odgovorom server signalizira da je navedeno dozvoljeno vreme trajanja sesije u polju zaglavlja zahteva *Session-Expires* prekratko. U odgovoru se, u okviru

polja zaglavlja *Min-SE*, navodi minimalna prihvatljiva vrednost za trajanje sesije. Ovaj odgovor je definisan u RFC 4028.

- 423 (*Interval Too Brief*) - Ovim odgovorom registrar signalizira da je navedeno vreme važenja jednog od navedenih kontakata (ili više njih) prekratko. U odgovoru se obavezno vraća minimalna dozvoljena vrednost za vreme važenja u okviru polja zaglavlja *Min-Expires*.
- 480 (*Temporarily Unavailable*) - Ovim odgovorom se signalizira da je zahtev uspešno primljen, ali da je traženi korisnik trenutno nedostupan (na primer, uključio je uslugu 'ne smetaj' kojom se onemogućava prijem poziva od drugih, pri čemu sam taj korisnik i dalje može da poziva druge). U frazi odgovora se navodi detaljnije zbog čega je korisnik nedostupan. Ovaj odgovor može vratiti i preusmeravački ili proksi server u slučaju da prepoznaju traženog korisnika, ali trenutno ne mogu odrediti njegovu lokaciju.
- 481 (*Call/Transaction Does Not Exist*) - Ovim odgovorom se signalizira da server ne može da odredi kom dijalogu ili transakciji pripada primljeni zahtev.
- 482 (*Loop Detected*) - Ovim odgovorom se signalizira da je detektovana petlja.
- 483 (*Too Many Hops*) - Ovim odgovorom se signalizira da je primljeni zahtev imao vrednost 0 u polju zaglavlja *Max-Forwards* čime je detektovano da je zahtev imao prevelik broj hopova (prošao kroz prevelik broj posrednih tačaka tj. proksi servera).
- 484 (*Address Incomplete*) - Ovim odgovorom se signalizira da je URI odredišta iz startne linije zahteva nepotpun.
- 485 (*Ambiguous*) - Ovim odgovorom se signalizira da je URI odredišta neodređen tj. dvosmislen pa samim tim ne može da se procesira. U okviru ovog odgovora se mogu poslati predlozi kontakata koji su nedvosmisleni tj. određeni, a koje pošiljalac zahteva eventualno može iskoristiti. Na primer, klijent je u URI odredišta mogao navesti *sip:jelena@etf.rs*, ali proksi server nije mogao odredi korisnika jer je našao više poklapanja, pa je vratio odgovor 485 u kom je naveo potencijalne kandidate da klijent proveri koga je od njih tražio:

  SIP/2.0 485 Ambiguous
  Contact: Jelena Petrovic <sip:jelena.petrovic@etf.rs>
  Contact: Jelena Milanovic <sip:jelena.milanovic@etf.rs>
  Contact: Jelena Katic <sip:jelena.katic@etf.rs>

- 486 (*Busy Here*) - Ovim odgovorom traženi korisnik signalizira da ne želi ili ne može da prihvati zahtev za uspostavom veze.
- 487 (*Request Terminated*) - Ovim odgovorom se signalizira nasilni prekid procesiranja zahteva usled prijema CANCEL ili BYE zahteva od samog klijenta.

- 488 (*Not Acceptable Here*) - Ovaj odgovor je sličan 606 odgovoru. Razlika je u tome što se ovaj odgovor odnosi samo na URI odredišta, ali na drugim lokacijama (alternativnim lokacijama traženog korisnika) zahtev bi mogao da bude uspešno obrađen.
- 489 (*Bad Event*) - Ovaj odgovor se koristi za odbijanje SUBSCRIPTION zahteva ili za odbijanje NOTIFY zahteva. Zahtev je odbijen jer tip *Event* paketa iz zahteva nije prepoznat ili podržan od strane servera. Ovaj odgovor je definisan u RFC 6665.
- 491 (*Request Pending*) - Server signalizira da trenutno procesira zahtev unutar istog dijaloga. Ovaj odgovor se koristi za razrešavanje situacije simultanog ponovnog slanja INVITE poruke od oba učesnika u komunikaciji. Ponovno slanje INVITE poruke predstavlja slanje INVITE poruke u toku veze (multimedijalne sesije), a cilj ove poruke je modifikacija parametara prenosa.
- 493 (*Undecipherable*) - Server signalizira da je primio šifrovani sadržaj od klijenta, ali nema ključ za dešifrovanje tog sadržaja (ne može da nađe javni ključ klijenta). Ovaj odgovor može da sadrži javni ključ koji bi klijent mogao da iskoristi za šifrovanje.

- 5xx - Odgovori koji signaliziraju greške na serverskoj strani (koja je primila zahtev). Serverska strana ovim signalizira da iz određenog razloga nije mogla da ispuni validan klijentov zahtev. Odgovor iz ove grupe definitivno odbija primljeni zahtev. Odgovori iz ove grupe su:
  - 500 (*Server Internal Error*) - Ovim odgovorom se signalizira da je došlo do neočekivane greške u procesiranju zahteva i da stoga nije došlo do ispunjenja zahteva.
  - 501 (*Not Implemented*) - Ovim odgovorom se signalizira da tip zahteva (metoda) nije prepoznat i stoga ne može da se procesira jer nije implementirana funkcionalnost obrade dotičnog tipa zahteva.
  - 502 (*Bad Gateway*) - Ovim odgovorom se signalizira da gejtvej nije uspeo uspešno da procesira zahtev jer je primio negativan odgovor od druge mreže sa kojom gejtvej povezuje SIP mrežu (došlo je do greške u drugoj mreži koja sprečava uspešno procesiranje zahteva).
  - 503 (*Service Unavailable*) - Ovim odgovorom se signalizira privremena nedostupnost servera usled preopterećenja ili održavanja. Korisnik može da ponovi zahtev nakon vremena specificiranog u zaglavlju poruke (*Retry-After* polje). Ako ovo vreme nije specificirano, klijent tretira ovaj odgovor kao odgovor 500.
  - 504 (*Server Time-Out*) - Ovim odgovorom se signalizira da je server koji je primio zahtev tražio uslugu od nekog drugog servera prilikom procesiranja zahteva, ali da je vreme čekanja na odgovor od tog drugog servera isteklo pa stoga server koji je originalno primio zahtev ne može da

ga uspešno obradi. Na primer, ako se tražila usluga od DNS servera radi određivanja proksi servera u domenu u kome se nalazi traženi korisnik.

- 505 (*Version Not Supported*) - Server ne podržava verziju SIP protokola navedenu u startnoj liniji zahteva i samim tim ne može da obradi primljeni zahtev.
- 513 (*Message Too Large*) - Server ne može da obradi primljenu poruku jer je predugačka.

- 6xx - Odgovori koji signaliziraju generalne greške. Ovi odgovori signaliziraju da nijedna serverska strana ne može da ispuni klijentov zahtev. Odgovor iz ove grupe definitivno odbija primljeni zahtev. Odgovori iz ove grupe su:
  - 600 (*Busy Everywhere*) - Ovim odgovorom se signalizira da je zahtev uspešno stigao na odredište, ali da je korisnik zauzet na svim lokacijama koje su vezane za njega.
  - 603 (*Decline*) - Ovaj odgovor ima isti efekat kao odgovor 600. Razlika je u tome što se ovde ne navodi razlog odbijanja veze (da li je u pitanju zauzetost korisnika ili korisnik jednostavno ne želi da prihvati poziv).
  - 604 (*Does Not Exist Anywhere*) - Ovim odgovorom se signalizira da korisnik naveden u URI odredišta sigurno ne postoji.
  - 606 (*Not Acceptable*) - Traženi korisnik je uspešno primio zahtev, ali ovim odgovorom signalizira da ne može da prihvati vezu jer parametri veze koji su mu ponuđeni nisu za njega prihvatljivi. Korisnik ovim odgovorm signalizira da je želeo da prihvati vezu, ali da nije mogao iz tehničkih razloga.

10.2.3. Zaglavlje poruke

Polja zaglavlja SIP poruka su definisana kao polja zaglavlja HTTP poruka. Polje zaglavlja se definiše u formatu:

naziv polja: vrednost polja

pri čemu se za *vrednost polja* može navesti više vrednosti koje su međusobno razdvojene zarezima. Svako polje zaglavlja mora da se završi CRLF karakterom. Takođe, iza vrednosti polja mogu da se stave parametri i njihove vrednosti u formatu:

naziv parametra = vrednost parametra

U slučaju upotrebe parametara u polju zaglavlja, iza *vrednost polja* mora da stoji tačka-zarez (;). Parametri su međusobno razdvojeni tačka-zarezom (;). Isti parametar ne sme da se javi više od jednom u okviru iste vrednosti polja.

Pojedina polja mogu da se pojave samo u zahtevima, a pojedina samo u odgovorima. Takođe, pojedina polja mogu da jave samo u određenim tipovima zahteva ili odgovora. Svaki tip zahteva/odgovora ima listu obaveznih polja zaglavlja koja obavezno moraju da budu prisutna u zaglavlju dotične poruke.

Većina polja zaglavlja je definisana u okviru osnovne preporuke za SIP protokol (RFC 3261), a ostala su definisana u naknadnim RFC preporukama koje proširuju osnovnu SIP

preporuku (RFC 3261). Spisak svih polja zaglavlja koja su standardizovana se može naći na http://www.iana.org/assignments/sip-parameters/sip-parameters.xhtml. U nastavku ćemo za polja zaglavlja koja nisu definisana u RFC 3261 navesti RFC preporuke u kojima su definisani.

Tipovi polja zaglavlja koji mogu da se pojave i u zahtevima i u odgovorima su:

- *Call-ID* - Predstavlja jedinstveni identifikator veze. Na osnovu ovog identifikatora se zna kom SIP dijalogu pripada zahtev/odgovor. Ovo polje je obavezno u svim SIP porukama.
- *Contact* - Ovo polje sadrži URI identifikator čije tumačenje zavisi od tipa zahteva/odgovora. Na primer, u slučaju INVITE zahteva označava lokaciju na koju suprotna strana treba da šalje svoje (eventualne) buduće zahteve u dijalogu. U slučaju odgovora na INVITE označava lokaciju na koju suprotna strana treba da šalje svoje buduće zahteve u dijalogu čime se omogućava direktna razmena SIP signalizacije (bez učešća proksi servera) između korisnika u nastavku dijaloga. Može biti navedeno i više identifikatora. Uz identifikator može da stoji i tzv. *display name*. U slučaju da se koristi *display name* tada se URI identifikator stavlja u <> zagradu. Parametri koji mogu da se koriste su *q* parametar za definisanje prioriteta i *expires* parametar za definisanje trajanja validnosti identifikatora (ova dva parametra se smeju koristiti u *Contact* polju samo u slučaju 3xx odgovora, kao i REGISTER zahteva i odgovora na REGISTER zahtev).
- *CSeq* - Ovo polje predstavlja jedinstvenu identifikaciju transakcije unutar dijaloga. Time je omogućeno i da se razlikuju novi zahtevi od retransmitovanih zahteva. Ovo polje sadrži decimalnu vrednost i naziv metoda zahteva. Za svaki novi zahtev unutar istog dijaloga se decimalna vrednost tipično inkrementira (vrednost mora da se promeni, a promena se tipično sastoji u inkrementiranju za 1 u odnosu na prethodnu decimalnu vrednost). Jedino se kod slanja ACK i CANCEL ne inkrementira decimalna vrednost, već se stavlja vrednost iz INVITE zahteva na koji se ACK Ili CANCEL odnose. Naziv metoda zahteva je stoga neophodan da bi se razlikovali odgovori na zahteve koji imaju istu decimalnu vrednost ovog polja. Na primer, korisnik može poslati INVITE zahtev za otvaranjem (uspostavom) veze, ali odmah potom može da pošalje CANCEL zahtev za nasilno raskidanje veze (odustajanje od veze). Oba zahteva će imati isti decimalni broj, ali na osnovu naziva metode će klijent moći da razlikuje odgovore na INVITE i CANCEL zahteve.
- *From* - Ovo polje sadrži URI identifikator izvorišta zahteva. U slučaju odgovora ovo polje predstavlja izvorište zahteva na koji se odnosi odgovor. U ovom polju se može koristiti *tag* parametar koji predstavlja jedinstveni identifikator dijaloga (u gotovo svim slučajevima se koristi *tag* parametar). Kao i u slučaju *Contact* polja, uz URI se može navesti i *display name*, i tada URI identifikator ide u <> zagradu.
- *To* - Ovo polje sadrži URI identifikator odredišta zahteva. U slučaju odgovora ovo polje mora sadržati *tag* parametar. Ovaj parametar iz 200 odgovora se mora koristiti u nastavku sesije (dijaloga) kao identifikator dijaloga. Važno je napomenuti da se ovo polje ne koristi za rutiranje SIP poruke iako ime polja to

sugeriše. Za rutiranje zahteva se koristi URI odredišta iz startne linije zahteva, a rutiranje odgovora se vrši na osnovu *Via* polja.

- *Via* - Ovo polje snima putanju zahteva tako što svaki proksi server dodaje ovo polje i u njega upisuje svoju URI lokaciju. Polje se dodaje ispred ostalih *Via* polja ako ona postoje. Na osnovu ovog polja, koje se kopira u odgovor, se postiže da odgovor ide istom putanjom kao zahtev. Tada svaki proksi server skida svoje *Via* polje kako odgovor prođe kroz njega. Ovo polje koristi tzv. *branch* parametar u koji se stavlja heširana vrednost polja *To*, *From*, *Call-ID*, kao i vrednost URI odredišta iz startne linije zahteva. Naravno, pod heširanjem ovih vrednosti se misli na heširanje ovih vrednosti posmatranih zajedno. Parametar *branch* predstavlja identifikaciju transakcije i pomoću ovog parametra proksi serveri mogu detektovati eventualne petlje. Vrednost *branch* parametra mora početi vrednošću *z9hG4bK* koja predstavlja tzv. magični kolačić (*magic cookie*). Na početku *Via* polja se nalazi naziv protokola (SIP), verzija protokola (2.0) i identifikacija transportnog protokola (UDP, TCP, SCTP ili TLS, gde TLS predstavlja TLS preko TCP).
- *Allow-Events* - Sadrži listu podržanih *event* paketa. Neki od *event* paketa su *conference* (sadrži informacije o konferenciji, poput liste učesnika), *dialog* (sadrži informacije o stanju dijaloga), *presence* (sadrži informacije o prisutnosti), i dr. Ovo polje je definisano u RFC 6665.
- *Alert-Info* - U slučaju INVITE zahteva predstavlja URI lokaciju tona zvonjenja koji se može pustiti traženom korisniku umesto njegovog difolt tona zvonjenja. U slučaju 180 odgovora, predstavlja URI lokaciju tona koji se može pustiti pozivajućem korisniku kao svojevrsna tonska indikacija da suprotnoj strani zvoni telefon.
- *Call-Info* - Ovo polje sadrži dodatne informacije o pozivu, preciznije o pozivajućem ili traženom korisniku u zavisnosti da li se ovo polje nalazi u zahtevu ili odgovoru. Uz vrednost se postavlja parametar *purpose* koji predstavlja tumačenje dodatne informacije. Na primer, korisnici na taj način mogu proslediti ikonice koje ih predstavljaju ili veb stranice koje sadrže informacije o njima i sl. Preporuka SIP protokola je da se ove dodatne informacije koriste samo ako je korisnik siguran u njihovu autentičnost, jer zlonamerni napadač može ovim putem da korisniku prikaže neprikladan materijal (na primer, umesto veb stranice sa dodatnim informacijama o korisniku se prikaže veb stranica sa neprikladnim sadržajem).
- *Content-Disposition* - Ovo polje definiše kako korisnički agent treba da interpretira telo poruke unutar SIP poruke. Vrednosti ovog polja mogu biti *session*, *render*, *icon*, *alert* i dr. Ako ovo polje izostane iz zaglavlja tada se u slučaju da *Content-Type* polje sadrži vrednost *application/sdp* podrazumeva vrednost *session* koja označava da se telo poruke treba tretirati po SDP (*Session Description Protocol*) formatu, u suprotnom se podrazumeva vrednost *render*.
- *Content-Encoding* - Ovo polje definiše način kodiranja tela poruke. Na primer, *gzip*.

- *Content-Language* - Ovo polje definiše jezik koji se koristi u telu poruke.
- *Content-Length* - Ovo polje sadrži vrednost dužine tela poruke u bajtovima. Vrednost ovog polja je 0, ako nema tela poruke. Ovo polje nije obavezno tj. može da se izostavi.
- *Content-Type* - Ovo polje definiše tip sadržaja koji se nalazi u telu poruke (SDP format, HTML format i dr.). Ovo polje mora da postoji u zaglavlju ako telo poruke nije prazno.
- *Date* - Ovo polje sadrži datum i vreme prvog slanja zahteva/odgovora, pri čemu mora da se koristi format definisan u RFC 1123. SIP podržava samo GMT vremensku zonu, odnosno sva vremena su konvertovana u ovu zonu.
- *Organization* - Ovo polje sadrži informaciju o organizaciji kojoj pripada entitet koji predstavlja izvorište poruke.
- *Record-Route* - Ovo polje ubacuje proksi server. Proksi server kreira ovo polje i stavlja svoj URI u njega, ako polje ne postoji, odnosno dopisuje sebe (svoj URI) na kraj ovog polja ako ono postoji. Ovim poljem proksi server forsira da svi budući zahtevi (a time i odgovori) u dotičnom dijalogu prolaze kroz njega. Server koji primi zahtev sa ovim poljem će kopirati ovo polje u svoj pozitivan odgovor 200 (u slučaju negativnog odgovora sesija će biti raskinuta tako da neće biti budućih zahteva) tako da se time obezbeđuje da budući zahtevi prolaze navedenom rutom (preciznije, kroz naveden lanac proksi servera).
- *Subject* - Ovo polje predstavlja sažet opis (temu) sesije slično *subject* polju u elektronskoj pošti.
- *Supported* - Ovo polje sadrži listu podržanih ekstenzija protokola (podržanih od strane entiteta koji je kreirao dotičnu poruku). Tipično se šalje u odgovoru na OPTIONS zahtev. Neke od ekstenzija su *events* (SIP događaji), *join* (podrška za pridruživanje pozivu), *rel100* (podrška za PRACK zahteve) i dr.
- *Timestamp* - Ovo polje sadrži precizno vreme slanja zahteva na strani klijenta. Format vremena je specificiran SIP protokolom. Server će da prepiše ovu vrednost u svom odgovoru, pri čemu može da dopiše i vreme kašnjenja u serveru (vreme između prijema zahteva i slanja odgovora, ali precizna definicija ovog kašnjenja zavisi od same implementacije servera). Ovo polje omogućava da klijent proceni RTT vreme.
- *User-Agent* - Ovo polje sadrži osnovne informacije o korisničkom agentu koji je kreirao zahtev. U suštini nije preporučljiva upotreba ovog polja jer može da pruži osetljive informacije napadaču koje može potom zloupotrebiti. Na primer, ako u ovom polju korisnički agent navede verziju softvera koju koristi, napadač na osnovu poznavanja potencijalnih sigurnosnih rupa u dotičnoj verziji softvera može napasti korisnika.

Tipovi polja zaglavlja koji mogu da se pojave samo u zahtevima su:

- *Accept* - Definiše format koji je prihvatljiv da se koristi u telu poruke. Može se navesti i lista formata, pri čemu se parametar *q* može koristiti za definisanje

prioriteta među članovima liste (*q* parametar može imati vrednosti iz opsega 0 do 1). Ako se ovo polje ne navede u zaglavlju, podrazumeva se SDP (*Session Description Protocol*) format.

- *Accept Contact* - Ovo polje sadrži listu URI lokacija na koje proksi server može da prosledi zahtev. Ovim poljem se korisničkom agentu omogućava bolja kontrola usmeravanja zahteva, ako korisnički agent ima potrebu za takvom funkcionalnošću. Ovo polje je definisano u RFC 3841.
- *Accept Encoding* - Definiše tip kodiranja tela poruke koji je prihvatljiv. Ovime se omogućava upotreba šema za kompresiju (na primer, gzip) za smanjivanje veličine poruke u slučaju da je poruka prevelika da stane u jedan UDP paket. Može se navesti i lista tipova kodiranja, pri čemu se parametar *q* može koristiti za definisanje prioriteta među članovima liste. Ako se ovo polje ne navede u zaglavlju, podrazumeva se da se koristi običan nekomprimovani tekst (*plain text*).
- *Accept Language* - Definiše poželjni jezik ili jezike koji treba da se koriste u telu poruke, u pojedinim poljima zaglavlja informativnog tipa poput *Subject* ili frazi odgovora. Parametar *q* se može koristiti za definisanje prioriteta u izboru jezika.
- *Authorization* - Ovo polje se koristi u procesu autentifikacije korisničkog agenta koji šalje zahtev koji sadrži ovo polje.
- *Event* - Ovo polje se koristi u SUBSCRIBE i NOTIFY zahtevima da naznači tip *event* paketa koji se koristi. U slučaju SUBSCRIBE zahteva u pitanju su tipovi *event* paketa za koje korisnik želi da prima obaveštenja. U slučaju NOTIFY zahteva u pitanju su tipovi *event* paketa o kojima NOTIFY zahtev nosi korisne informacije. Ovo polje je definisano u RFC 6665.
- *In-Reply-To* - Ovo polje sadrži vrednost *Call-ID* poziva koje dotični zahtev referencira ili uzvraća. Na primer, korisnik 2 je zvao korisnika 1, ali je korisnik 1 iz nekog razloga propustio poziv (na primer, bio je odsutan sa lokacije na kojoj je bio tražen). Korisnik 1 će primetiti u nekom momentu propušten poziv i krenuće da nazove korisnika 2. Korisnik 1 može da pokrene uspostavu veze koja neće referencirati propušteni poziv (polje *In-Reply-To* se neće staviti u INVITE zahtev), a može i da pokrene uspostavu veze u kojoj će referencirati propušteni poziv (polje *In-Reply-To* će se staviti u INVITE zahtev). Ovo polje omogućava traženom korisniku da efikasnije filtrira i prioritetizuje svoje primljene pozive, pa tako referencirane pozive može da stavi kao najprioritetnije. U datom primeru, u polje *In-Reply-To* će se staviti *Call-ID* vrednost iz propuštenog poziva. Postoje i druge slične primene ovog polja.
- *Join* - Ovo polje se koristi za pridruživanje SIP dijaloga koji se uspostavlja postojećem SIP dijalogu, čime se postiže pridruživanje korisnika postojećoj sesiji tj. vezi. U slučaju da je u pitanju konferencijska veza, vrši se priključivanje konferencijskoj vezi, a u slučaju da je u pitanju veza dva učesnika kojoj se pridružuje treći učesnik tada veza prerasta u konferencijsku vezu. Ovo polje sadrži podatke kojima se identifikuje postojeći dijalog, a time i multimedijalna sesija kojoj se želi pridružiti. Ovo polje je definisano u RFC 3911.

- *Max-Forwards* - Ovo polje definiše maksimalan broj hopova zahteva. Pod hopom se podrazumeva jedan prolazak kroz proksi server. Proksi server dekrementira vrednost u ovom polju. Kada se detektuje da je vrednost ovoga polja 0 (u proksi serveru ili korisničkom agentu), vraća se odgovor 483 (*Too Many Hops*).
- *Priority* - Ovo polje predstavlja nivo prioriteta zahteva. Vrednosti ovog polja mogu biti *non-urgent*, *normal*, *urgent*, ili *emergency*. Ovo polje ne utiče na prioritet u prosleđivanju kroz mrežu, već samo na proces obrade (na primer, u slučaju zagušenja servera biće odbacivani zahtevi nižeg prioriteta, ili za određivanje prosleđivanja poziva ka lokacijama traženog korisnika gde se prioritetniji pozivi upućuju na jednu lokaciju, a ostali na drugu lokaciju). Ako se izostavi ovo polje iz zaglavlja, podrazumeva se *normal* vrednost za nivo prioriteta.
- *Privacy* - Ovim poljem klijent zahteva određeni nivo i tip privatnosti. Moguće vrednosti ovog polja su *critical*, *header*, *id*, *session*, *user*, ili *none* čime se signalizira za koje podatke se želi privatnost. U polje je moguće upisati i više navedenih vrednosti odjednom (na primer, i *header* i *user*) pri čemu se one razdvajaju tačka-zarezom (;) jer se tumače kao parametri. Upisom više vrednosti se postiže privatnost za veći deo informacija. Ovo polje je definisano u RFC 3323.
- *Proxy-Authorization* - Ovo polje se koristi u procesu autentifikacije korisničkog agenta na proksi server.
- *Proxy-Require* - Ovo polje se koristi da bi klijent signalizirao ekstenzije protokola koje proksi server mora da podržava da bi mogao da procesira zahtev koji je poslao klijent. Ako proksi server ne podržava sve navedene ekstenzije u ovom polju, poslaće odgovor 420 (*Bad Extension*).
- *Reason* - Ovo polje nosi dodatnu informaciju o raskidanju veze (stoga se ovo polje koristi u BYE ili CANCEL zahtevima). Ovo polje je definisano u RFC 3326.
- *Refer-To* - Ovo polje se obavezno nalazi u REFER zahtevu i predstavlja URI (ili URL) entiteta koji se referencira. Ovo polje je definisano u RFC 3515.
- *Referred-By* - Ovo polje se opciono nalazi u REFER zahtevu ili zahtevu koji se šalje na osnovu primljenog REFER zahteva. Predstavlja URI identifikaciju izvorišta originalnog REFER zahteva. Ovo polje je definisano u RFC 3892.
- *Reply-To* - Predstavlja URI na koji treba poslati odgovor ukoliko u *From* polju nema URI identifikacije koja bi se inače trebala koristiti. Takođe, URI iz ovog polja se može koristiti za vraćanje poziva u suprotnom smeru u slučaju propuštenih poziva ili poziva koji nisu uspešno uspostavljeni.
- *Replaces* - U slučaju prijema INVITE zahteva sa ovim poljem u kome se nalaze podaci koji ukazuju na tekuću sesiju, tada korisnički agent treba sačuvati sve relevantne podatke tekuće sesije, raskinuti sesiju BYE zahtevom i prebaciti te sačuvane podatke u sesiju koja je uspostavljena INVITE zahtevom sa *Replaces* poljem. Ova opcija se može koristiti za postizanje '*call pickup*' servisa. Primer

ovog servisa je kancelarija sa više zaposlenih i gde svaki zaposleni ima telefon. Ako odsutnom zaposlenom zazvoni telefon, poziv može pokupiti drugi zaposleni sa svog telefona. Ovo polje je definisano u RFC 3891.

- *Reject-Contact* - Ovo polje sadrži listu kontakata ka kojima proksi server ne sme proslediti zahtev (koji sadrži ovo polje). Ovo polje je definisano u RFC 3841.
- *Require* - Ovo polje se koristi da bi klijent signalizirao ekstenzije protokola koje server mora da podržava da bi mogao da procesira zahtev koji je poslao klijent. Ako server ne podržava sve navedene ekstenzije u ovom polju, poslaće odgovor 420 (*Bad Extension*).
- *Route* - Ovo polje se koristi za definisanje rute koju mora da sledi zahtev. Postoji striktno i labavo definisanje rute. U striktnoj varijanti, proksi server uzima URI identifikator sa početka liste URI identifikatora iz *Route* polja i njega stavlja na mesto URI odredišta u zahtevu koji prosleđuje dalje (naravno, uzeti URI identifikator je izbrisan sa početka liste iz *Route* polja u prosleđenom zahtevu). U slučaju labavog rutiranja, proksi server prosleđuje zahtev ka proksi serveru sa početka liste iz *Route* polja (tada ga i skida sa liste) ili nekom drugom proksi serveru koji podržava labavo rutiranje. Pri tome, u zahtevu čitavo vreme ostaje originalni URI odredišta. U slučaju fiksnog rutiranja zahtev prolazi samo kroz proksi servere navedene u *Route* polju, dok u slučaju labavog rutiranja zahtev prolazi kroz sve proksi servere iz *Route* polja, ali može da prođe i kroz dodatne proksi servere. Navođenje parametra *lr* uz URI proksi servera u listi proksi servera u *Route* polju označava da se koristi labavo rutiranje.
- *RAck* - Ovo polje se koristi u PRACK zahtevu da bi se potvrdio uspešan prijem odgovora iz 1xx grupe koji je zahtevao potvrdu. U ovo polje se kopiraju vrednosti polja *CSeq* i *RSeq* iz 1xx odgovora koji se potvrđuje. Ovo polje je definisano u RFC 3262.
- *Session-Expires* - Ovo polje sadrži vrednost trajanja sesije, tj. posle koliko vremena će sesija da istekne. Ako se želi produžiti trajanje sesije, tada tokom sesije treba poslati ponovni INVITE zahtev ili UPDATE zahtev u kojima će biti stavljena (unutar polja *Session-Expires*) nova vrednost trajanja sesije (može se i skratiti sesija u odnosu na prethodno vreme trajanja). Vreme trajanja se predstavlja u vidu integer broja sekundi. Ideja uvođenja vremena trajanja sesije je da se izbegne situacija u kojoj proksi server sa memorijom kroz koji ide dijalog ne bude svestan da je sesija, ustvari, okončana jer nije primio BYE zahtev (na primer, došlo je do gubitka BYE zahteva u mreži). Stoga, korisnički agenti povremeno šalju ponovni INVITE ili UPDATE zahtev čime signaliziraju proksi serveru (ili proksi serverima) sa memorijom kroz koji dijalog prolazi da je komunikacija i dalje u toku. Ovo polje je definisano u RFC 4028.
- *Subscription-State* - Ovo polje se obavezno nalazi u NOTIFY poruci kojom se signalizira trenutno stanje prijave na obaveštenja. Vrednosti mogu biti *active*, *pending*, ili *terminated*. Parametri koji se mogu koristiti su *expires*, *reason*, i *retry-after*. Ovo polje je definisano u RFC 6665.

Tipovi polja zaglavlja koji mogu da se pojave samo u odgovorima su:

- *Authentication-Info* - Ovo polje se koristi u slučaju obostrane autentifikacije klijenta i servera. Tipično, server vrši autentifikaciju klijenta da bi proverio da je klijent zaista onaj za koga se predstavlja (a ne napadač koji se lažno predstavlja kao dotični klijent). Međutim, i klijent može da traži autentifikaciju servera da bi bio siguran da zaista komunicira sa željenim serverom (a ne lažnim kojega je postavio napadač). Ovo polje se šalje u odgovoru na zahtev u okviru koga se klijent autentifikovao.
- *Error-Info* - Ovo polje omogućava fleksibilno prezentovanje greške korisniku. Na primer, fraza odgovora može biti prezentovana tekstualno korisniku i time će korisnik vizuelno biti obavešten o grešci. S druge strane, ako SIP korisnički agent (terminal) ima samo audio mogućnosti tj. nema displej onda fraza odgovora ne može biti vizuelno prikazana. Otuda se u *Error-Info* polje može staviti SIP URI lokacija audio snimka koji predstavlja audio zapis obaveštenja o grešci, pa se terminal može povezati na dotični snimak i pustiti ga korisniku. *Error-Info* polje, stoga, omogućava serveru da pošalje sve opcije za obaveštavanje korisnika o grešci, a korisničkom agentu (klijentu) pruža izbor načina obaveštavanja korisnika o grešci.
- *Min-Expires* - Ovo polje sadrži dozvoljeno minimalno vreme trajanja validnosti kontakta i stavlja se u 423 (*Interval Too Brief*) odgovor.
- *Min-SE* - Ovo polje sadrži dozvoljeno minimalno vreme trajanja sesije i stavlja se u 422 (*Session Timer Interval Too Small*) odgovor. Sesija može da se prekine za kraće vreme, ali je bitno da ne može da istekne njena validnost za kraće vreme. Ovo polje je definisano u RFC 4028.
- *Proxy-Authenticate* - Ovo polje sadrži vrednost koja se koristi u procesu autentifikacije. Ovo polje se stavlja u odgovor 407 (*Proxy Authentication*), tako da klijent onda može da formira polje *Proxy Authorization* koje će staviti u zaglavlje svog narednog zahteva da bi mogao uspešno da se autentifikuje na proksi server.
- *Retry-After* - Ovim poljem se signalizira posle koliko vremena se može ponovo poslati zahtev koji je doživeo neuspeh u procesiranju. Vreme može biti izraženo u formatu datuma koji se koristi u *Date* polju, ili kao integer broj sekundi. U okviru ovog polja se može koristiti i *duration* parametar koji definiše koliko dugo će servis biti na raspolaganju nakon vremena specificiranog za ponovni pokušaj. Takođe, uz navedeno vreme može da se stavi i komentar koji pobliže opisuje situaciju oko ponovnog pokušaja.
- *RSeq* - Ovo polje se koristi u odgovorima iz grupe 1xx da bi se zahtevalo njihovo potvrđivanje preko PRACK zahteva. U polje se upisuje redni broj koji treba da se koristi u PRACK zahtevu koji, ustvari, predstavlja potvrdu. Ovo polje je definisano u RFC 3262.
- *Server* - Ovo polje sadrži osnovne informacije o softveru servera i za njega važe iste napomene vezane za sigurnost kao za polje *User-Agent*.
- *Unsupported* - Ovo polje sadrži listu ekstenzija SIP protokola koje nisu podržane.

- *Warning* - Ovo polje sadrži dodatne informacije koje statusni kod odgovora ne može da pruži. Ovo polje sadrži statusni kod (kopiran iz startne linije), ime hosta, i tekstualno objašnjenje. Cilj polja je da omogući lakše debagovanje tj. otkrivanje i ispravljanje grešaka u implementaciji ili konfiguraciji SIP entiteta.
- *WWW-Authenticate* - Ovo polje je ekvivalentno *Proxy-Authenticate* polju. Razlika je u tome što se ovo polje šalje u okviru odgovora 401 (*Unauthorized*) i što se vrši autentifikacija na server ili registrar.

Napomenimo da se za pojedina polja mogu koristiti i skraćeni nazivi radi smanjenja veličine SIP poruke. Na primer, naziv polja *Contact* se može skraćeno napisati *m*. Spisak svih skraćenih naziva se može takođe naći na http://www.iana.org/assignments/sip-parameters/sip-parameters.xhtml. Ovo donekle narušava ideju da zaglavlje bude čitljivo, ali je zgodna opcija ako je potrebno skratiti poruku tako da može da se prenese UDP protokolom.

10.2.4. Telo poruke

Telo poruke (ako postoji) nosi korisnu informaciju. Polje zaglavlja *Content-Type* definiše format tela poruke. Za opis multimedijalnih sesija se koristi SDP (dozvoljeno je koristiti i druge formate, ali uglavnom se, ipak, koristi SDP). SDP je razvijen radi podrške multimedijalnim aplikacijama na Internetu. Naime, za ispravno konfigurisanje prijemnika i predajnika multimedijalnog sadržaja sesije, neophodno je definisati multimedijalni sadržaj koji će se prenositi, poput tipa sadržaja (na primer, audio, video), IP adrese i porta transportnog protokola koji će se koristiti, tipa kodera (na primer, G.711, G.729, H.261), protoka i sl. Upravo u tu svrhu se koristi SDP protokol koji standardizuje opis multimedijalne sesije tako da je olakšan razvoj aplikacija i njihova interoperabilnost. SDP se može koristiti u SIP signalizaciji, u RTSP protokolu, HTTP protokolu, itd. SDP protokol je definisan u RFC 4566 preporuci.

SDP poruka predstavlja niz polja koja se moraju navoditi u definisanom redosledu. Redosled je definisan da bi se olakšalo procesiranje SDP sadržaja, a i da bi se uprostilo kreiranje SDP sadržaja. Svako polje je formata (polje se treba završiti CRLF karakterom):

skraćeni naziv polja= vrednost polja

U SDP sadržaju prvo sledi opis sesije, kojeg potom slede 0 ili više opisa multimedijalnog sadržaja. Opis sesije se sastoji od sledećih polja, pri čemu su u zagradi pored naziva polja dati skraćeni nazivi polja (polja su navedena u redosledu kojim treba da se pojave u SDP sadržaju):

- Verzija protokola (*v*) - Aktuelna verzija SDP protokola je 0, pa u SDP opisima sesija treba da stoji *v*=0. Ovo polje je obavezno u SDP opisu sesije.
- Kreator i identifikator sesije (*o*) - Ovo polje pruža informacije o izvorištu sesije i identifikaciji sesije. Ovo polje je obavezno u SDP opisu sesije. Delovi ovog polja su (dati u redosledu kojim treba da se pojavljuju u polju):
    - Korisničko ime kreatora na hostu koji predstavlja izvorište sesije.
    - Identifikator sesije koji uz ostale delove ovog polja (sem verzije sesije) treba da obezbedi jedinstvenu identifikaciju sesije. Preporuka je da se koristi vremenski trenutak u NTP (*Network Time Protocol*) formatu, ali sam način definisanja vrednosti ovog dela je ostavljen konkretnoj implementaciji.

- Verzija sesije. Ideja ovog polja je da se prate modifikacije sesije tako što će se za svaku modifikaciju povećati ovaj broj. Preporuka je da se i ovde koristi vremenski trenutak u NTP formatu, ali i ovde je sam način definisanja vrednosti ovog dela ostavljen konkretnoj implementaciji.
- Tip mreže preko koje se prenosi sesija. Vrednost IN označava Internet (IP) mrežu.
- Tip adrese koja se koristi u mreži. Vrednosti IP4 i IP6, označavaju IPv4 i IPv6 adrese, respektivno.
- Unikast adresa koja predstavlja adresu uređaja koji je kreirao sesiju.

- Naziv sesije (*s*) - Predstavlja tekstualni naziv sesije i ovo polje je obavezno u SDP opisu sesije.
- Informacije o sesiji (*i*) - Ovo polje pruža tekstualne informacije o sesiji, tipično deskriptivni opis svrhe ili teme sesije i sl. Informacije nisu namenjene procesiranju već su u čitljivom obliku tako da korisnik na osnovu ovog polja odmah može da ima uvid temu/svrhu sesije. Ovo polje je opciono.
- URI identifikator (*u*) - URI identifikator www lokacije na kojoj se nalaze dodatne informacije o sesiji. Ovo polje je opciono.
- E-mejl adrese (*e*) - E-mejl adresa osobe odgovorne za sesiju. Ovo polje je opciono.
- Telefon (*p*) - Telefonski broj osobe odgovorne za sesiju. Ovo i prethodno polje imaju za cilj da obezbede kontakt informacije u slučaju eventualnih problema (pre svega se misli na konferencijske veze ili multikast distribuciju striming sadržaja). Ovo polje je opciono.
- Informacije za povezivanje (*c*) - Ovo polje sadrži informacije za povezivanje da bi se mogao primati multimedijalni sadržaj. Ovo polje se ne pojavljuje u opisu sesije samo u slučaju kada svi opisi multimedijalnog sadržaja sadrže svoje informacije za povezivanje, u suprotnom se mora ovo polje pojaviti u opisu sesije. Sastoji se iz tri obavezna dela:
  - Tip mreže u kome se nalazi kontakt za povezivanje. Vrednost IN označava Internet (IP) mrežu.
  - Tip adrese kontakta za povezivanje. Vrednosti IP4 i IP6, označavaju IPv4 i IPv6 adrese, respektivno.
  - Adresa kontakta za povezivanje. U slučaju multikast adrese u pitanju je multikast adresa grupe preko koje se treba primati multimedijalni sadržaj, odnosno u slučaju izvorišta multimedijalnog sadržaja na koju se treba slati multimedijalni sadržaj. Ako je u pitanju unikast adresa, tada je u pitanju tzv. udaljena adresa uređaja sa stanovišta onoga ko čita SDP opis sesije, pa se ova adresa koristi kao adresa na koju treba da se šalje multimedijalni sadržaj. Kreator SDP opisa, ustvari, javlja na koju adresu želi da prima multimedijalni sadržaj (slično važi i za port kao što ćemo u nastavku videti). Ako je u pitanju IPv4 multikast adresa mora se dodati TTL

vrednost iz opsega 0-255 iza IPv4 adrese, iako se u praksi ta vrednost više ne koristi (na primer, 188.67.123.11/125, kao što vidimo TTL vrednost se dodaje tako što se iza IP adrese stavlja / pa sama TTL vrednost).

Pod kontaktom za povezivanje se u slučaju SIP telefonskih poziva očigledno podrazumeva lokacija na koju strana koja primi opis treba da šalje svoj multimedijalni sadržaj, odnosno sam SDP opis sesije predstavlja ekvivalenciju H.245 signalizaciji iz H.323 mreže. Pored ova tri obavezna polja se mogu dodati eventualno i neka opciona potpolja, a tipovi potpolja, koji mogu da se koriste, zavise od tipa adrese.

- Informacija o propusnom opsegu (*b*) - Ovo opciono polje navodi predlog propusnog opsega za sesiju.
- Trenutak početka i kraja sesije (*t*) - Ovo opciono polje sadrži trenutak početka i kraja sesije koji se navode u tom redosledu unutar polja. Ovo polje može da se javi više puta ako sesija ima više aktivnih intervala sa pauzama između (tada svako polje obeležava početak i kraj aktivnog intervala sesije). Trenuci se navode u NTP formatu. Ako se za trenutak početka navede 0 sesija se smatra permanentnom, a ako se za trenutak kraja navede 0 sesija se smatra neograničenom. Ako su oba trenutka 0, onda je sesija i permanentna i neograničena. Preporuka je izbegavanje postavljanja ovih trenutaka na vrednost 0.
- Intervali ponavljanja (*r*) - U slučaju da sesija ima više aktivnih intervala sa pauzama između, pri čemu postoji periodičnost aktivnih intervala i pauza, tada se umesto više uzastopnih *t* polja, navodi samo jedno *t* polje koje deklariše početak i kraj sesije, a *r* polje se koristi za opis perioda ponavljanja. Opis se sastoji u navođenju periode ponavljanja, trajanja aktivnog intervala i niza ofseta u odnosu na vreme starta sesije svih aktivnih intervala u okviru jedne periode. Očigledno, svi aktivni intervali unutar periode moraju imati isto trajanje. Sva vremena u ovom polju se mogu navoditi u sekundama, minutima, časovima ili danima, pri čemu su dozvoljena i mešanja jedinica vremena (na primer, perioda ponavljanja da bude izražena u danima, a ostala vremena u časovima). Ovo polje je opciono.
- Korekcija vremenske zone (*z*) - Ovo polje se koristi za usklađivanja vremena iz različitih vremenskih zona pošto postoje potencijalne varijacije u razlici vremena tokom godine između različitih zona, na primer, usled zimskog i letnjeg računanja vremena u nekim zemljama dolazi do pomeranja vremena za 1h unazad ili unapred. Ovo polje je opciono.
- Ključ za šifrovanje (*k*) - Ovo opciono polje omogućava slanje ključa koji se može iskoristiti za šifrovanje multimedijalnog sadržaja koji se šalje. Nije preporučljivo koristiti ovo polje, a ako se koristi tada SDP sadržaj mora da se prenosi poverljivim i zaštićenim kanalom. Razlog je što šifrovanje multimedijalnog sadržaja mora biti dovoljno brzo pa bi po pravilu trebalo koristiti simetrično šifrovanje što znači da se isti ključ koristi i za šifrovanje i dešifrovanje, pa presretanjem ključa napadač može da dešifruje multimedijalni sadržaj.
- Atributi sesije (*a*) - Ovo opciono polje služi za eventualna proširenja opisa sesije.

Iza opisa sesije slede eventualni opisi multimedijalnih sadržaja koji se prenose u okviru sesije. Ako ima više multimedijalnih sadržaja tj. njihovih opisa, oni se navode jedan za drugim. U slučaju SIP telefonskih poziva ovi opisi, ustvari, predstavljaju mogućnosti prijema multimedijalnog sadržaja u procesu svojevrsnog pregovaranja razmenom SDP opisa sesije, slično kao u slučaju H.245 signalizacije iz H.323 mreža. Opis multimedijalnog sadržaja se sastoji od sledećih polja, pri čemu su u zagradi pored naziva polja dati skraćeni nazivi polja (polja su navedena u redosledu kojim treba da se pojave u SDP sadržaju):

- Informacije o multimedijalnom sadržaju (*m*) - Ovo je obavezno polje za opis multimedijalnog sadržaja. Sastoji se iz delova koji daju opis multimedijalnog sadržaja. Delovi od kojih se sastoji su (navedeni redom kako se pojavljuju u polju):
    - Tip sadržaja koji može biti audio, video, tekst, aplikacija ili poruka.
    - Port transportnog protokola na koji treba slati multimedijalni sadržaj. Strana koja primi SDP opis na osnovu ovog parametra zna na koji port treba da šalje multimedijalni sadržaj.
    - Tip transportnog protokola koji se koristi (UDP, RTP za AVP profil preko UDP (RTP/AVP), zaštićeni RTP za AVP profil preko UDP (RTP/SAVP)).
    - Opis formata multimedijalnog sadržaja. Na primer, ako je tip transportnog protokola RTP/AVP ili RTP/SAVP, opis formata će sadržati odgovarajući kod tipa korisnog sadržaja iz ovih profila (*Payload Type* vrednost).
- Naziv multimedije (*i*) - Predstavlja tekstualnu labelu multimedijalnog sadržaja radi njihovog lakšeg razlikovanja. Opciono polje.
- Informacije za povezivanje (*c*) - Ovo polje je ekvivalentno polju *c* iz dela za opis sesije. Koristi se da premosti podešavanja *c* polja iz dela za opis sesije tako da se podešavanja ovog polja primene na multimedijalni sadržaj na koji se odnosi ovo polje. Ovo polje je opciono, sem u slučaju kada *c* polje ne postoji u opisu sesije (tada je ovo polje obavezno).
- Informacija o propusnom opsegu (*b*) - Ovo opciono polje ekvivalentno polju *b* iz dela za opis sesije. Koristi se da premosti podešavanja *b* polja iz dela za opis sesije tako da se podešavanja ovog polja primene na multimedijalni sadržaj na koji se odnosi ovo polje.
- Ključ za šifrovanje (*k*) - Ovo opciono polje omogućava slanje ključa koji se može iskoristiti za šifrovanje dotičnog multimedijalnog sadržaja na koji se odnosi ovo polje. Sve napomene navedene za isto polje iz opisa sesije važe i u ovom slučaju. Ako je definisan ključ i u delu za opis sesije, on se ignoriše za dotični multimedijalni sadržaj.
- Atributi multimedije (*a*) - Ovo opciono polje služi za eventualna proširenja opisa multimedijalnog sadržaja.

Kao što vidimo, nazivi pojedinih polja se poklapaju, ali to ne pravi problem pri procesiranju SDP sadržaja, zato što se unapred zna redosled kojim se polja moraju pojaviti. Pogledajmo primer SDP opisa multimedijalne sesije:

v=0
o=ivan 1380212345 1380212345 IN IP4 193.52.21.8
s=Multikast sesija za onlajn predavanje
i=Predavanje iz predmeta x
u=http:// telekomunikacije.etf.rs/predmeti/x
e=Ivan Jovanovic ivan.jovanovic@etf.rs
p=+381-11-3218-878
c=IN IP4 225.45.13.28/240
t=1380200400 1380211200
a=recvonly
m=audio 37314 RTP/AVP 8
m=video 35548 RTP/AVP 31

Kao što vidimo iz opisa multimedijalne sesije u pitanju je predavanje u kome se audio i video sadržaj šalju na IPv4 multikast adresu 225.45.13.28 (polje *c*). Postoje dva multimedijalna sadržaja (jedan audio i jedan video) koji su navedeni kroz *m* polja. Koristi se AVP profil definisan u RFC 3551. Tip sadržaja (*payload type*) 8 označava audio G.711 koder po A zakonu kompresije, a 31 označava video koder H.261. Audio sadržaj treba da se prima preko UDP porta 37314, a video sadržaj preko UDP porta 35548. U *t* polju je korišćen NTP format u sekundama, pa je trajanje sesije 3h (ako se napravi razlika između kraja i početka sesije dobija se 10800s tj. 3h). Atribut *a* sa vrednošću *recvonly* označava da je u pitanju sadržaj koji se samo može primati. Po difoltu je komunikacija dvosmerna (*sendrecv*) i ova difolt vrednost se ne mora navoditi u SDP opisu za slučaj dvosmerne komunikacije.

Razmotrimo i primer SDP opisa multimedijalne sesije za slučaj telefonskog razgovora:

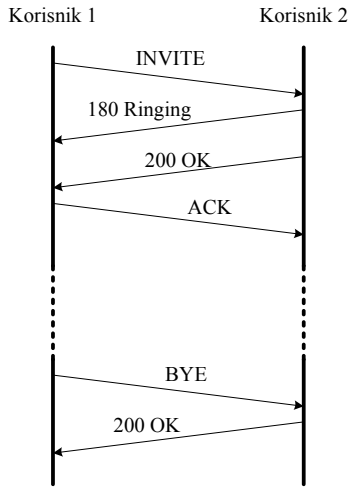
v=0
o=ivan 1380123987 1380123987 IN IP4 193.52.21.8
s= Ivan SIP telefonski poziv
c=IN IP4 193.52.21.8
t=0 0
m=audio 37314 RTP/AVP 8 18 4 0

Sada je adresa unikast IPv4 adresa 193.52.21.8 (polje *c*), pri čemu se ona poklapa i sa kreatorom sesije (jedan od dva učesnika u razgovoru). Strana koja primi ovaj SDP opis treba na tu IP adresu da šalje RTP pakete sa govornim signalom. Sesija je permanentna i neograničena pošto su oba vremenska trenutka u polju *t* postavljena na 0. Iako je preporuka da se izbegava ovakvo postavljanje *t* polja, ono se često koristi pri uspostavi telefonskih poziva SIP signalizacijom. Na kraju primetimo da je u *m* polju navedeno više tipova korisnog sadržaja. Na osnovu tabele 8.2.1.4.1, vrednostima 8, 18, 4 i 0 redom odgovaraju G.711 A zakon, G.729, G.723 i G.711 μ zakon. Ovo predstavlja opis tehničkih mogućnosti strane koja je kreirala dotični SDP opis. Prva navedena vrednost u nizu tipova korisnih sadržaja je najpoželjnija. Ako suprotna strana podržava G.711 koder po A zakonu, onda će ona slati govorni sadržaj u ovom formatu, u suprotnom će se koristiti neki od preostala tri formata u zavisnosti kojeg od njih podržava. Port 37314 označava da suprotna strana (strana koja je primila ovaj SDP opis) treba da šalje pakete na taj UDP port.

10.2.5. Primeri uspostave veze SIP signalizacijom

U ovoj sekciji ćemo prikazati nekoliko slučajeva za uspostavu i raskidanje veze pomoću SIP signalizacije. Na slici 10.2.5.1. je prikazana direktna razmena SIP signalizacije između dva korisnika bez učešća proksi servera. Očigledno, kao i u H.323 signalizaciji je moguća direktna

razmena signalizacije, ali se ta varijanta tipično koristi u manjim mrežama sa malim brojem korisnika.



Slika 10.2.5.1. Direktna razmena SIP signalizacije

Korisnik 1 šalje INVITE zahtev korisniku 2 kojim signalizira da želi da uspostavi vezu sa njim. Korisnički agent korisnika 2 prvo vraća privremeni odgovor 180 (*Ringing*) kojim signalizira da se korisniku pušta 'zvono' tj. da se obaveštava o pozivu. Kada se korisnik 2 odazove, vraća se konačni odgovor 200 (*OK*) kojim se signalizira prihvatanje veze. Korisnik 1 potvrđuje uspostavu veze slanjem ACK zahteva čime je sesija uspostavljena i počinje razmena paketa koji nose govorne signale. Bilo koja od strana može da raskine vezu, a u primeru sa slike 10.2.5.1 vezu raskida korisnik 1 slanjem BYE zahteva. Korisnik 2 potvrđuje prihvatanje BYE zahteva slanjem odgovora 200 (*OK*). Sve SIP poruke sa slike 10.2.5.1 čine jedan dijalog. Dijalog iz primera se sastoji od tri transakcije:

1. Prvu transakciju čine INVITE zahtev i odgovori na njega (180 i 200).
2. Drugu transakciju čini ACK zahtev. Na ACK zahtev se ne šalju odgovori.
3. Treću transakciju čine BYE zahtev i odgovor 200 na njega.

Pogledajmo sada strukturu INVITE zahteva bez tela poruke:

```
INVITE sip:korisnik2@kompanijax.com SIP/2.0
Via: SIP/2.0/UDP comp1.kompanijax.com:5060;branch=z9hG4bK777koqlhl
Max-Forwards: 20
To: Goran Popovic <sip:korisnik2@kompanijax.com>
From: Marko Markovic <sip:korisnik1@kompanijax.com>;tag=12865
Call-ID: 98afvh3n1@comp1.kompanijax.com
CSeq: 1 INVITE
Subject: Zakazivanje sastanka
Contact: Marko Markovic <sip:korisnik1@comp1.kompanijax.com>
Content-Type: application/sdp
Content-Length: 158
```

Objasnili smo već ulogu polja zaglavlja i startne linije, pa se sad koncentrišimo na najbitnije detalje. U datom primeru se SIP URI odredišta i *To* polje poklapaju tj. odnose se na istog korisnika (*sip:korisnik2@kompanijax.com*). To je čest slučaj u praksi, ali ove dve vrednosti ne moraju da se poklapaju u opštem slučaju. Polje zaglavlja *To* definiše kome je namenjena SIP

poruka, a SIP URI odredišta može da definiše posrednika u SIP komunikaciji, pri čemu će poslednji posrednik da u SIP URI odredišta stavi vrednost koja se nalazi u *To* polju. *From* polje definiše izvorište dotične SIP poruke, dok *Contact* polje sadrži lokaciju na koju treba vratiti odgovor (treba primetiti da je ispred domena *kompanijax.com* stavljen registrovan naziv hosta korisnika 1 *comp1* - ustvari, *comp1.kompanijax.com* predstavlja domensko ime na osnovu kojega se može odrediti IP adresa hosta, na primer, DNS upitom - ako host nije registrovan onda se umesto registrovanog imena hosta stavlja njegova IP adresa), preciznije na koju korisnik 2 treba slati svoje eventualne buduće zahteve jer u suštini *Via* polje određuje putanju odgovora. I ove dve lokacije su u najvećem broju identične, ali u opštem slučaju mogu da se razlikuju. U *From* polje je stavljen i *tag* parametar koji omogućava identifikaciju dijaloga. Na osnovu ovog parametra će korisnik 1 prepoznati odgovor/odgovore koje mu vrati korisnik 2 na INVITE zahtev. *Via* polje predstavlja putanju preko koje se mora vratiti odgovor na primljeni zahtev. Svaki posrednik se dopisuje u *Via* polje. Pošto u ovom primeru nema posrednika, *Via* polje će sadržati samo lokaciju korisnika 1 i može se videti da on očekuje odgovor preko UDP porta 5060. Razlika između *Via* polja i *Contact* polja je u tome što *Via* polje određuje kojim putem treba da vrati odgovor, a *Contact* polje govori korisniku 2 na koju lokaciju treba slati svoje buduće zahteve u tom dijalogu. Parametar *branch* se koristi za identifikaciju transakcije tj. da se odredi na koji zahtev se odnosi odgovor, a dodatno se koristi i za detekciju petlji, ali tu funkcionalnost ima prevashodno u slučaju proksi servera. *Call-ID* polje sadrži jedinstvenu identifikaciju poziva (ispred @ se dodaje slučajni string, a ispred imena domena koji se nalazi iza @ se dodaje registrovano ime hosta korisnika ili IP adresa korisnika - u našem slučaju je dodato ime hosta *comp1* - odnosno iza @ je stavljeno kvalifikovano domensko ime *comp1.kompanijax.com*), tako da se i na osnovu ovog polja određuje pripadnost SIP poruka dijalogu. *CSeq* polje je ekvivalent rednog broja poruke koji se koristi za vezivanje odgovora za poslate zahteve. U telu poruke se smešta SDP opis sesije koju predlaže korisnik 1.

Odgovor 180 ima sledeću strukturu:

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP comp1.kompanijax.com:5060;branch=z9hG4bK777koqlhl;received=200.199.55.24
To: Goran Popovic <sip:korisnik2@kompanijax.com>;tag=c3h95jk
From: Marko Markovic <sip:korisnik1@kompanijax.com>;tag=12865
Call-ID: 98afvh3n1@comp1.kompanijax.com
CSeq: 1 INVITE
Contact: Goran Popovic <sip:korisnik2@comp4.kompanijax.com>
Content-Length: 0
```

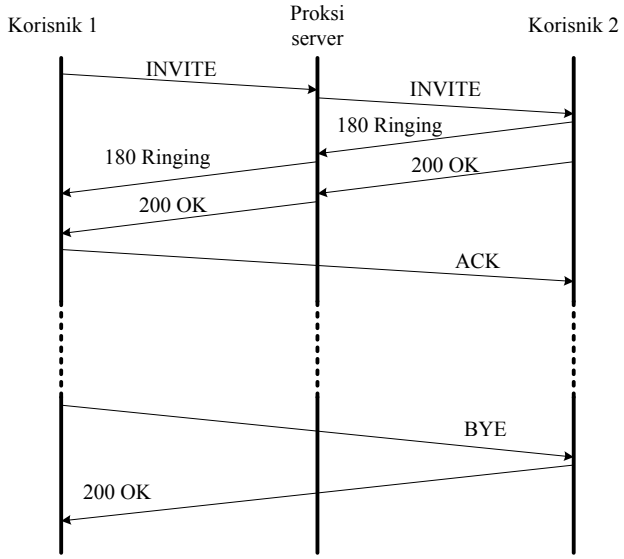
Većina polja je iskopirano iz INVITE zahteva na koji se šalje ovaj odgovor. U *To* polje je dodat parametar *tag* takođe kao jedinstvena identifikacija dijaloga, pa se otuda može reći da *tag* parametri iz *To* i *From* polja, zajedno sa *Call-ID* polje čine jedinstvenu identifikaciju dijaloga. Na kraju *Via* polja je dodata i IP adresa sa koje primljen INVITE zahtev (IP adresa korisnika 1 - da je INVITE zahtev primljen od proksi servera, stajala bi IP adresa proksi servera). Telo poruke ne postoji u ovom slučaju. Kada se korisnik 2 odazove, šalje se odgovor 200 (telo poruke nije prikazano):

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP comp1.kompanijax.com:5060;branch=z9hG4bK777koqlhl;received=200.199.55.24
To: Goran Popovic <sip:korisnik2@kompanijax.com>;tag=c3h95jk
From: Marko Markovic <sip:korisnik1@kompanijax.com>;tag=12865
Call-ID: 98afvh3n1@comp1.kompanijax.com
CSeq: 1 INVITE
```

Contact: Goran Popovic <sip:korisnik2@comp4.kompanijax.com>
Content-Type: application/sdp
Content-Length: 155

Ovaj odgovor je gotovo identičan strukturi odgovora 180. Razlika je u startnoj liniji i u tome što postoji telo poruke u kome se smešta SDP opis predloga sesije korisnika 2. Kontakt u oba odgovora nosi naziv hosta korisnika 2 (*comp4*, odnosno kontakt sadrži puno domensko ime na osnovu koga se može odrediti IP adresa korisnika 2 - umesto *comp4* mogla se direktno staviti IP adresa korisnika 2). Cilj dodavanja naziva hosta u kontakt polje zahteva/odgovora omogućava da korisnik sa suprotne strane sazna puno ime domena (domen + ime hosta u domenu se takođe tretira kao domen) tako da pomoću DNS upita može da sazna IP adresu suprotne strane što je bitno kada komunikacija u početku ide preko proksi servera, a posle treba da se pređe na direktnu razmenu SIP poruka između korisnika. Pored naziva hosta se može staviti IP adresa hosta, pošto najčešće hostovi nemaju registrovano ime unutar domena (umesto *comp4* moglo je da stoji 200.199.55.28 ako je to IP adresa korisnika 2) i tada se direktno saznaje IP adresa suprotne strane pa nema potrebe za DNS upitom. Pošto su oba korisnika razmenili opise predloga sesija, oba sada znaju da podese svoje predajnike i prijemnike za predaju i prijem paketa sa govornim signalima. Korisnik 1 šalje ACK zahtev kao finalnu potvrdu da je veza uspostavljena uspešno. Struktura ACK odgovora je:

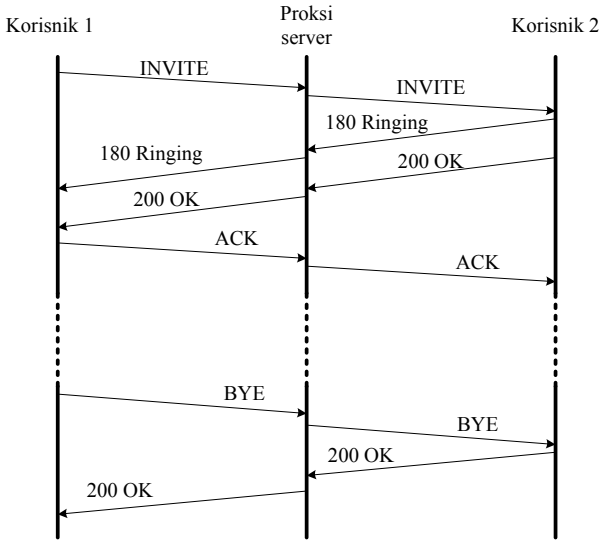
ACK sip:korisnik2@kompanijax.com SIP/2.0
Via: SIP/2.0/UDP comp1.kompanijax.com:5060;branch=z9hG4bK184avqert
Max-Forwards: 20
To: Goran Popovic <sip:korisnik2@kompanijax.com>;tag=c3h95jk
From: Marko Markovic <sip:korisnik1@kompanijax.com>;tag=12865
Call-ID: 98afvh3n1@comp1.kompanijax.com
CSeq: 1 INVITE
Content-Length: 0



Slika 10.2.5.2. Razmena SIP signalizacije preko proksi servera

Pogledajmo sada nešto složeniji primer sa slike 10.2.5.2 koji je ekvivalentan intrazonskom pozivu iz H.323 mreže. U ovom slučaju korisnik 1 ne zna lokaciju korisnika 2, već samo njegovu SIP URI identifikaciju. Korisnički agent korisnika 1 se obraća proksi serveru tako što mu šalje INVITE zahtev gde kao URI odredišta, navodi SIP URI korisnika 2. Korisnički

agent zna lokaciju tj. IP adresu proksi servera (na primer, ručno je konfigurisan sa tom informacijom, ili preko DHCP protokola mu je dostavljena ta informacija, ili preko DNS upita ako zna naziv proksi servera, itd). Proksi server prima INVITE zahtev, ispituje lokacijski server da odredi IP adresu korisnika 2 i potom mu šalje INVITE zahtev. U INVITE zahtev dodaje sebe u novom *Via* polju (koje ide iznad svih ostalih *Via* polja, u našem primeru samo *Via* polja kojeg je kreirao korisnik 1) jer odgovor od korisnika 2 na INVITE zahtev korisnika 1 mora proći isti put kao INVITE zahtev samo u suprotnom smeru. Korisnik 2 prvo šalje odgovor 180, pa odgovor 200 da prihvata vezu i oba ova odgovora idu preko proksi servera (prilikom prolaska odgovora, proksi server skida iz njih *Via* polje koje je dodao - setimo se da se *Via* polja kopiraju iz zahteva u odgovor). Pošto je primio odgovore, korisnik 1 preko 200 odgovora tj. polja *Contact* (koje je obavezno u odgovoru 200) saznaje IP adresu korisnika 2 (ili direktno ako je stavljena IP adresa ispred naziva domena ili indirektno ako je stavljen naziv hosta jer tada treba da se obavi DNS upit). Pošto sada oba korisnika iz polja *Contact* u INVITE zahtevu, odnosno u 200 odgovoru znaju IP adrese suprotne strane, preostale SIP poruke mogu da se razmenjuju direktno između korisnika 1 i korisnika 2 (ACK, BYE i odgovor 200 na BYE zahtev).



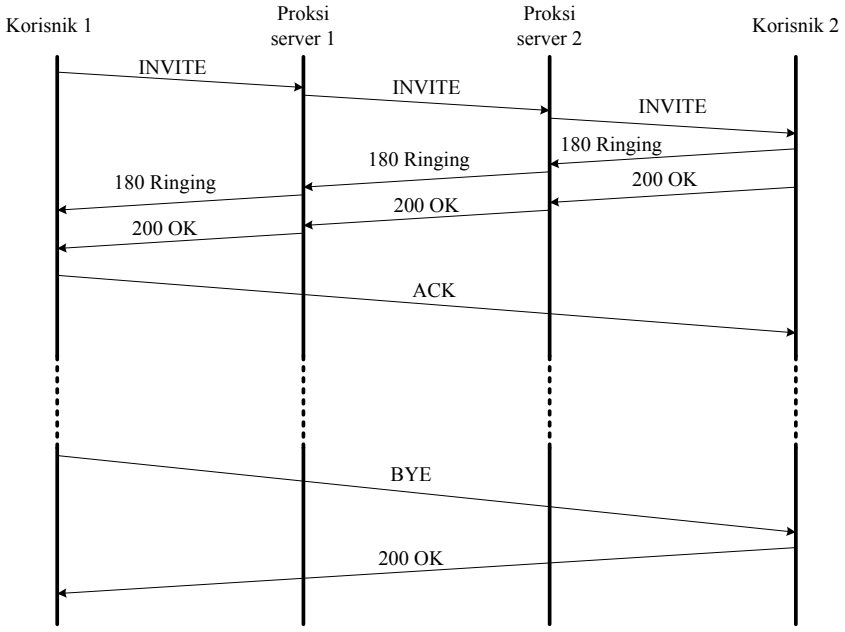
Slika 10.2.5.3. Razmena kompletne SIP signalizacije preko proksi servera

Ako proksi server želi da se sve SIP poruke u dijalogu razmenjuju kroz njega tada on u INVITE poruci kreira *Record-Route* polje i upisuje sebe u njega (ako bi ovo polje već postojalo tada bi sebe dopisao na početak polja). Odgovor 200 će imati iskopirano *Record-Route* polje čime će oba korisnika biti svesni da moraju slati svoje buduće zahteve kroz proksi server naveden u *Record-Route* polju (odgovori ionako uvek idu istim putem samo suprotnim smerom usled *Via* polja). Ovaj primer je prikazan na slici 10.2.5.3. Proksi server bi uneo u ovo polje svoju SIP URI identifikaciju koristeći pun naziv domena (naziv servera + naziv domena) ili svoju IP adresu. Parametar *lr* označava da se koristi labavo rutiranje.

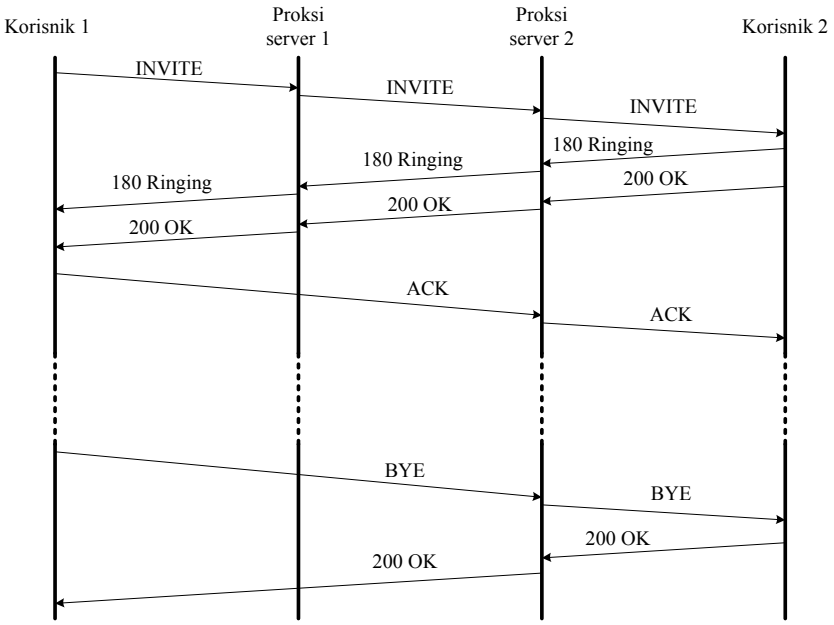
Record-Route: <sip:proksiserver1.kompanijax.com.;lr>

Pogledajmo primer kada se korisnici nalaze u različitim domenima i kada je potrebna upotreba dva proksi servera za njihovu međusobnu komunikaciju. Ovaj primer je prikazan na slici 10.2.5.4. Korisnik 1 se opet obraća svom proksi serveru (proksi server 1) šaljući mu INVITE zahtev u kome se kao URI odredišta navodi korisnik 2. Proksi server 1 shvata, na osnovu SIP URI identifikatora korisnika 2, da se korisnik 2 nalazi u drugom domenu i obraća se

DNS serveru da sazna IP adresu proksi servera 2 koji je nadležan za domen u kome se nalazi korisnik 2. Potom šalje INVITE zahtev proksi serveru 2.



Slika 10.2.5.4. Razmena SIP signalizacije preko dva proksi servera

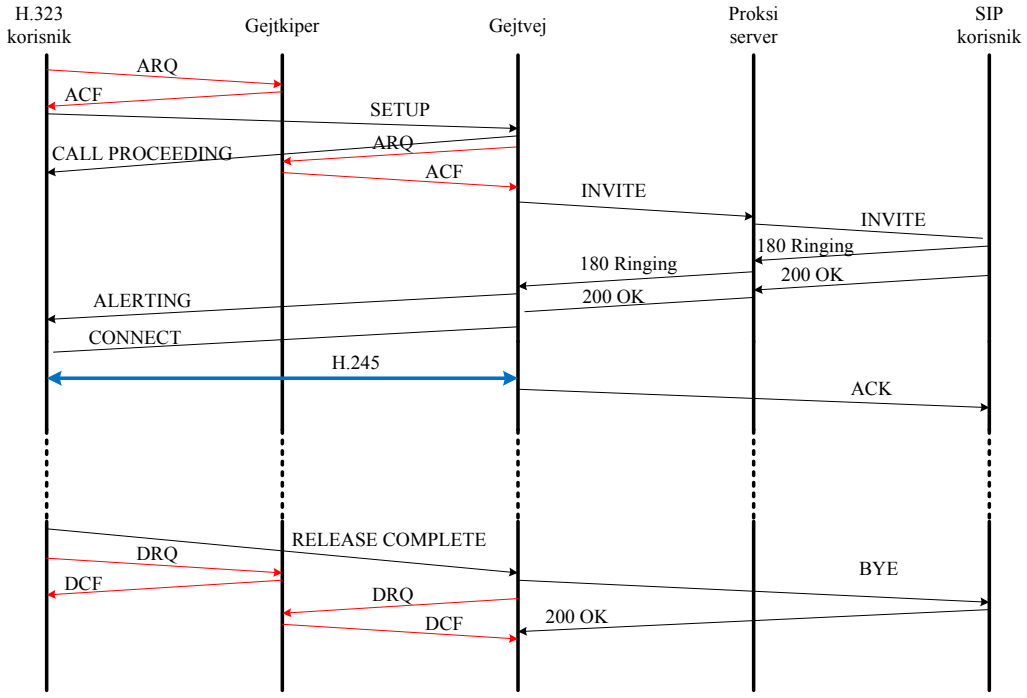


Slika 10.2.5.5. Razmena kompletne SIP signalizacije preko proksi servera 2

Proksi server 2 u lokacijskom serveru saznaje IP adresu korisnika 2 i prosleđuje mu INVITE zahtev. Korisnik 2 šalje prvo odgovor 180, pa odgovor 200 koji idu istim putem kao INVITE zahtev samo u suprotnom smeru, što je postignuto time što su u *Via* poljima redom bili navedeni proksi server 2, proksi server 1 i korisnik 1. Pošto preko *Contact* polja INVITE zahteva, odnosno 200 odgovora korisnici 1 i 2 znaju IP adrese suprotne strane (direktno ili indirektno preko DNS) preostale poruke se mogu razmeniti direktno između korisnika, pa tako

ACK, BYE i odgovor 200 na BYE idu direktno između korisnika. Ako bi bilo koji od proksi servera (ili oba) hteli da se SIP poruke dijaloga razmenjuju i dalje kroz njih, onda bi onaj proksi server koji bi to želeo u INVITE zahtevu dodao sebe u *Record-Route* polje (i kreirao ovo polje ako nije postojalo u INVITE zahtevu). Kao što vidimo forsiranje da signalizacija prolazi kroz proksi server je jednostavnije nego u H.323 slučaju. Na slici 10.2.5.5 je prikazana varijanta gde je proksi server 2 kreirao i dodao sebe u *Record-Route* polje INVITE zahteva pa sve SIP poruke u dijalogu prolaze kroz njega.

10.2.6. Mešoviti rad SIP i H.323 signalizacije

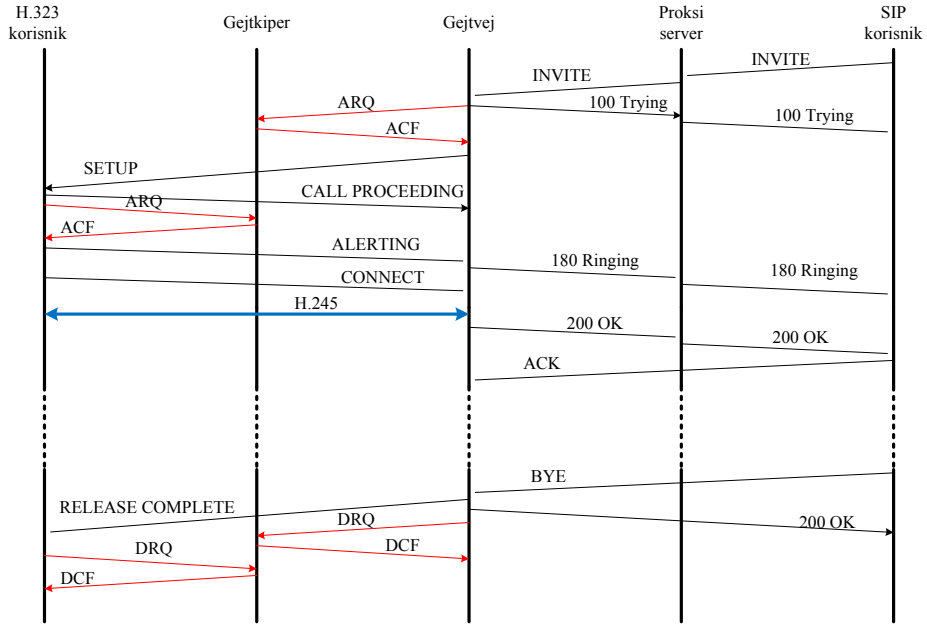


Slika 10.2.6.1. Komunikacija između H.323 korisnika i SIP korisnika - H.323 korisnik inicijator

Pošto se neki korisnici mogu nalaziti u H.323 mreži, a neki u SIP mreži potrebno je omogućiti njihovu međusobnu komunikaciju. Pre svega je potrebno obezbediti konverziju H.323 signalizacije u SIP signalizaciju i obrnuto. Na slici 10.2.6.1 je prikazan primer uspostave veze gde korisnik iz H.323 mreže poziva korisnika iz SIP mreže. H.323 korisnik prijavljuje poziv gejtkiperu preko ARQ poruke, a gejtkiper odobrava vezu i šalje IP adresu gejtveja preko ACF poruke. H.323 korisnik šalje SETUP poruku gejtveju koji odmah šalje kao odgovor CALL PROCEEDING kao potvrdu da je SETUP poruka krenula da se procesira. Gejtvej prvo traži odobrenje od gejtkipera za nastavak veze ARQ porukom, a kada dobije odobrenje preko ACF poruke, gejtvej kreće u uspostavljanje veze sa SIP korisnikom. INVITE zahtev prolazi kroz proksi server do traženog SIP korisnika. INVITE zahtev u ovom slučaju ne nosi opis predloga sesije već se koristi alternativna varijanta u kome će ACK zahtev da nosi opis predloga sesije pozivajuće strane. Ova alternativna varijanta mora da se koristi jer H.245 signalizacija može da počne da se razmenjuje tek kad se H.225.0 kontrola poziva signalizacijom potvrdi uspostava veze, preciznije odziv traženog korisnika, a H.245 signalizacija je ta koja dogovara parametre prenosa u H.323 mreži. Gejtvej primljeni odgovor 180 konvertuje u ALERTING poruku koju šalje H.323 korisniku, odnosno 200 odgovor konvertuje u CONNECT poruku. Tek po prijemu CONNECT poruke dolazi do razmene H.245 signalizacije, u okviru koje gejtvej opisuje tehničke

mogućnosti (tj. predlog sesije) na osnovu sadržaja iz 200 odgovora. Nakon dogovora parametara prenosa i otvaranja logičkih kanala H.245 signalizacijom, gejtvej formira ACK poruku u kojoj daje opis predloga sesije pozivajuće strane tj. H.323 korisnika. Nakon toga, H.323 korisnik i SIP korisnik mogu direktno između sebe da razmenjuju korisne podatke tj. multimedijalni sadržaj (tipično u vidu RTP paketa), jer je SIP korisnik saznao IP adresu H.323 korisnika, a H.323 korisnik je saznao IP adresu SIP korisnika, pri čemu oba korisnika znaju i UDP portove na koje treba da šalju pakete ka suprotnoj strani (napomena gejtvej je u ime SIP korisnika izvršio otvaranje logičkog kanala H.245 signalizacijom). Raskid veze u ovom primeru vrši H.323 korisnik (raskid može da uradi bilo koja strana) slanjem RELEASE COMPLETE poruke. Gejtvej šalje BYE zahtev SIP korisniku koji ga potvrđuje 200 odgovorom. Uporedo, H.323 korisnik i gejtvej prijavljuju kraj veze gejtkiperu DRQ porukama.

Na slici 10.2.6.2 je prikazana varijanta kada je SIP korisnik inicijator. SIP korisnik šalje INVITE zahtev proksi serveru koji ga prosleđuje na gejtvej (INVITE zahtev sada nosi opis sesije). Gejtvej vraća odgovor 100 čime se signalizira da je INVITE zahtev krenuo da se procesira. Gejtvej traži dozvolu od gejtkipera ARQ porukom i kada je dobije ACF porukom, dobiće i IP adresu H.323 korisnika. Gejtvej šalje SETUP poruku H.323 korisniku koji odgovara sa CALL PROCEEDING porukom. Nakon traženja (ARQ) i dobijanja (ACF) dozvole od gejtkipera, H.323 korisnik prvo šalje poruku ALERTING, a potom kada se korisnik odazove i CONNECT poruku. ALERTING poruka se konvertuje u 180 odgovor ka SIP korisniku. Nakon CONNECT poruke kreće H.245 signalizacija za dogovaranje parametara prenosa i otvaranje logičkih kanala (gejtvej opet u ime SIP korisnika otvara logički kanal). Nakon toga, gejtvej šalje 200 odgovor u kome se nalazi opis predloga sesije H.323 korisnika. SIP korisnik potvrđuje 200 odgovor, sa ACK zahtevom koji šalje direktno ka gejtveju. Nakon toga može da krene komunikacija između korisnika razmenom RTP paketa. Raskid veze u ovom primeru vrši SIP korisnik (raskid može da uradi bilo koja strana) slanjem BYE zahteva, na koji gejtvej odgovara sa 200 odgovorom, a takođe ka H.323 korisniku šalje RELEASE COMPLETE poruku. Nakon toga i H.323 korisnik i gejtvej prijavljuju raskid veze gejtkiperu DRQ porukama.



Slika 10.2.6.2. Komunikacija između H.323 korisnika i SIP korisnika - SIP korisnik inicijator

Naravno, postoje i varijante u kojima H.225.0 kontrola poziva i/ili H.245 signalizacija ide kroz gejtkiper, a isto važi i za SIP signalizaciju koja kompletno (čitav dijalog) prolazi kroz proksi server, u zavisnosti da li su gejtkiper i/ili proksi server to zahtevali.

Pošto su objašnjeni i H.323 i SIP signalizacija možemo i da ih uporedimo. H.323 signalizacija je nešto bolje zaokružena celina koja je imala za cilj da korisničke usluge iz fiksne telefonije (tj. iz mreže sa komutacijom kola) preslika u paketsku telefoniju i da obezbedi kvalitetnu podršku za konferencijske veze. Takođe, pošto se H.323 signalizacija delom bazira na ISDN signalizaciji olakšan je mešovit rad H.323 mreže sa ISDN mrežama, fiksnom telefonskom mrežom i privatnim telefonskim mrežama (koje se sastoje od kućnih centrala). Velika mana H.323 je što je signalizacija prilično složenija u odnosu na SIP signalizaciju. SIP signalizacija je 'lakša' signalizacija što se moglo videti i po manje komplikovanoj razmeni signalizacionih poruka što je posledica direktnog prilagođenja IP mrežama. Mana je što SIP signalizacija nije u startu pružila sve korisničke servise kao H.323 signalizacija, pa su neprestano dodavane dopune u vidu RFC dokumenata. S jedne strane to pomalo otežava implementaciju jer treba prvo odrediti (i naravno proučiti) sve RFC dokumente vezane za SIP signalizaciju pa tek potom krenuti u implementaciju, ali s druge strane to znači i da SIP implementacija osluškuje dešavanja na terenu i time implementira one funkcionalnosti koje se traže ne opterećujući signalizaciju funkcionalnostima koje se neće koristiti (ili će se veoma retko koristiti). Upravo ta filozofija SIP signalizacije i njena prilagođenost IP mrežama je omogućila dobru penetraciju SIP signalizacije u IP mrežama. Takođe, vidljiv je različit pristup i u prezentaciji informacija. SIP koristi čitljiv format koji je lakši čoveku za čitanje, a time i vizuelno ispitivanje poruka i debagovanje, ali nije optimalan po pitanju prostora koji te poruke zauzimaju, dok s druge strane H.323 koristi optimalnije kodiranje, ali koji nije prilagođen čoveku za čitanje pa tako nije moguće vizuelno čitati poruke i vršiti debagovanje. Kao što se vidi, obe signalizacije imaju svoje prednosti i mane. Nijedna od signalizacija nije apsolutni pobednik, već se obe danas koriste u praksi, pri čemu se obe neprestano razvijaju u cilju obezbeđivanja bolje funkcionalnosti korisnicima.

10.3. Mešoviti rad mreža sa komutacijom kola i komutacijom paketa

U okviru ovog potpoglavlja ćemo prikazati kako se ostvaruju telefonski pozivi između korisnika u paketskoj mreži (SIP ili H.323 signalizacija) i korisnika u fiksnoj telefonskoj mreži tj. prikazaćemo mešoviti rad mreža sa komutacijom kola i mreža sa komutacijom paketa.

Navedimo prvo probleme koji se javljaju prilikom obavljanja telefonskih poziva između korisnika u paketskoj mreži i korisnika u mreži sa komutacijom kola. U paketskoj mreži korisnici se identifikuju URI identifikatorima, dok se u fiksnoj telefonskoj mreži korisnici identifikuju telefonskim brojevima. Očigledno, da bi korisnik iz paketske mreže mogao biti biran iz fiksne telefonske mreže, mora mu biti dodeljen telefonski broj, pošto korisnici iz fiksne telefonske mreže imaju samo mogućnost biranja cifara (adresa se sme sastojati samo od cifara). S druge strane, da bi korisnik iz fiksne telefonije bio pozvan od korisnika iz paketske mreže, neophodno je da se telefonski broj fiksne telefonske mreže prevede u URI identifikator. To se vrši pretvaranjem telefonskog broja u kvalifikovano domensko ime. Proces prevođenja u kvalifikovano domensko ime se vrši na sledeći način primenom ENUM postupka (navedeni proces prevođenja je definisan u RFC 6116):

1. Telefonski broj se predstavlja u E.164 formatu. Na primer, +381-11-3218-890.
2. Zatim se ostavljaju samo cifre. Za primer broja iz tačke 1 imamo 381113218890.

3. Zatim se vrši obrtanje redosleda cifara (098812311183).
4. Zatim se vrši kreiranje domenskog imena tako što svaka cifra predstavlja poddomen i na kraju se dodaje domen *e164.arpa*. Za telefonski broj iz tačke 1 imamo *0.9.8.8.1.2.3.1.1.1.8.3.e164.arpa*. Razlog za obrtanje redosleda cifara telefonskog broja leži u činjenici da je telefonski broj formiran po *big-endian* principu (polazeći od viših cifara prvo se definiše kod zemlje, pa mrežne grupe, pa centrale, pa korisnika na centrali), a domensko ime po *little-endian* principu (najviši domen se nalazi na kraju punog imena domena, pa se ispred njega nalazi njegov poddomen, pa potom poddomen tog poddomena, itd.).

Na ovaj način, korisnik iz paketske mreže (tj. njegov terminal) vrši prevođenje telefonskog broja u kvalifikovano domensko ime, čime se omogućava da korisnik ili proksi server ili gejtkiper preko DNS upita saznaju lokaciju gejtveja preko koga se može stići do traženog broja tj. traženog korisnika iz fiksne telefonske mreže. Na sličan način, gejtvej primljeni traženi telefonski broj iz fiksne telefonske mreže može da prevede u kvalifikovano domensko ime (ili da u svojoj bazi podataka potraži SIP URI ili H.323 URI koji su registrovani pod tim telefonskim brojem) i time omogući proces uspostave poziva po H.323 ili SIP principima u paketskoj mreži. Telefonski brojevi prevedeni na opisani način u kvalifikovano domensko ime se čuvaju u DNS bazi u vidu NAPTR (*Naming Authority Pointer*) zapisa koji omogućavaju da se za dotični zapis vežu svi postojeći kontakti korisnika (SIP telefon, fiksni telefon, mejl, i dr.), pri čemu redosled kontakata u zapisu odgovara željama dotičnog korisnika kako da se kontakira (kojim redom da se pozivaju kontakti dok se ne dobije taj korisnik).

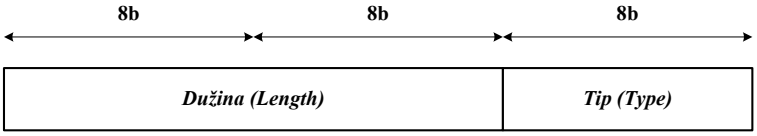
Drugi problem koji se sreće u mešovitom radu paketske mreže i mreže sa komutacijom kola je izbor gejtveja između ovih mreža različitog principa komutacije. Naime, najčešće prenos preko mreže na bazi komutacije kola značajno podiže cenu razgovora što se više resursa zauzme, pa je poželjno izabrati gejtvej koji će minimizovati zauzimanje resursa u mreži baziranoj na komutaciji kola tj. koji će biti što bliži korisniku iz te mreže. Za rešavanje ovog problema je razvijen protokol TRIP (*Telephony Routing Over IP*) za slučaj kada se poziv pokreće iz paketske mreže. TRIP predstavlja svojevrsni protokol rutiranja na osnovu kojeg se dobijaju tabele usmeravanja kojima se određuje ka kom gejtveju je najbolje proslediti signalizaciju i govorne pakete. Za pozive iz fiksne telefonske mreže postoji protokol CTRIP (*Circuit Telephony Routing Over IP*) koji rešava sličan problem, a to je formiranje tabela usmeravanja kojima se vrši određivanje gejtveja kojim se korisnik iz fiksne telefonske mreže treba povezati sa paketskom mrežom radi ostvarivanja poziva ka korisniku iz paketske mreže. Međutim, pošto se tipično koristi fiksno rutiranje u fiksnoj telefoniji ovaj problem nije toliko izražen, pogotovo ako se ima u vidu činjenica da je najčešće cilj što pre izaći na paketsku mrežu pa je samim tim poželjno izabrati najbliži gejtvej.

Na kraju postoji problem konverzije signalizacije i govornih signala. U okviru paketske mreže se koristi H.323 ili SIP signalizacija, a u okviru fiksne telefonske mreže postoji velik broj signalizacija, ali bi trebala dominantna da bude signalizacija No7 (ostale se koriste samo u slučaju starijih telefonskih centrala), pa je očigledno potrebna konverzija signalizacije iz jednog formata (SIP ili H.323) u drugi format (No7) i obrnuto. Takođe, u okviru paketske mreže se vrši prenos govornih signala unutar paketa, dok se u komutaciji kola paketi ne koriste. Otuda je neophodna konverzija i govornih signala (u opštem slučaju koverzija multimedijalnog sadržaja). Konverzija signalizacije se vrši upotrebom signalizacionih gejtveja (*SGW - Signaling Gateway*), a konverzija multimedijalnog korisnog sadržaja (tipično govornog signala) se vrši upotrebom

medija gejtveja (*MGW - Media Gateway*). Kontrolu rada SGW i MGW, vrši kontroler koji se naziva softsvič (*softswitch*), ali postoje i alternativni nazivi poput MGC (*Media Gateway Controller*), *Call Agent*, *Call Server* i dr.

10.3.1. TRIP

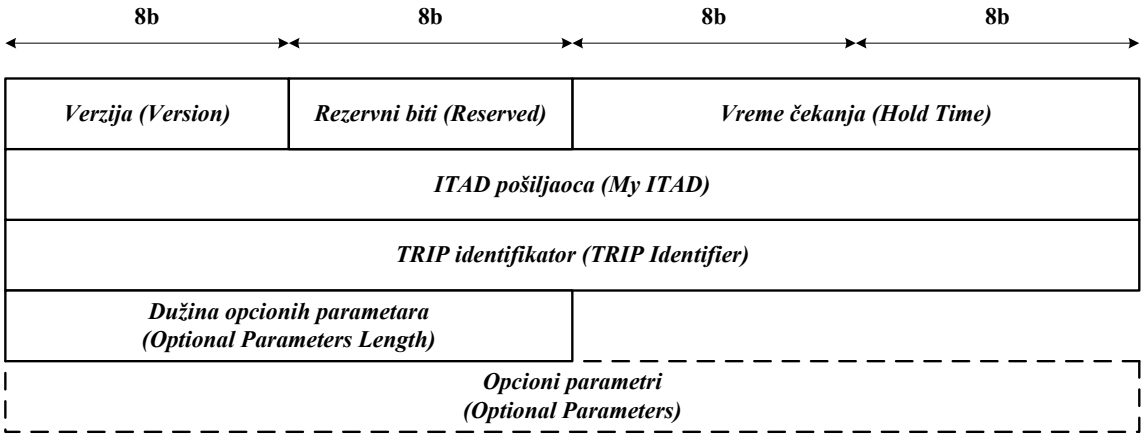
TRIP protokol je definisan u preporuci RFC 3219. Problem koji TRIP treba da reši jeste određivanje najoptimalnijeg gejtveja za izlaz na mrežu sa komutacijom kola tj. fiksnu telefonsku mrežu. Cilj je izaći u fiksnu telefonsku mrežu što bliže samom korisniku da bi poziv bio što ekonomičniji. Međutim, problem nije jednostavan jer postoje mnoga ograničenja i problemi, na primer, politike provajdera i njihovi međusobni dogovori oko oglašavanja svojih gejtveja prema fiksnoj telefonskoj mreži mogu da formiraju određena ograničenja u pristupima gejtvejima, takođe, problem je kreirati efikasno oglašavanje svih postojećih gejtveja pošto u opštem slučaju poziv ka pretplatniku iz fiksne telefonske mreže može da završi na bilo kom mestu na svetu (koje naravno ima fiksni telefonski priključak). Takođe, bitno je i koji tip signalizacije podržava gejtvej (SIP i/ili H.323), pa se za različiti tip korisnika (SIP ili H.323) može dobiti i različito rešenje, tj. izabrati različit gejtvej. Stoga su definisani tzv. lokacijski serveri koji čuvaju podatke o gejtvejima, odnosno o telefonskim brojevima (i rutama tj. putevima do njih). Ideja je da ovi lokacijski serveri imaju ulogu sličnu ruterima koji implementiraju i koriste BGP protokol za rutiranje između administrativnih domena (lokacijski server se još naziva i TRIP *speaker*, pa je očigledna paralela sa BGP *speaker* koji predstavljaju rutere koji koriste BGP protokol), pa je TRIP protokol zasnovan na principima BGP protokola. Umesto oglašavanja mreža na Internetu (odnosno destinacija sa stanovišta IP mrežnih adresa), lokacijski serveri oglašavaju destinacije sa stanovišta telefonskih adresa (oglašavaju se prefiksi telefonskih brojeva) i rute do tih destinacija (tačnije do gejtveja ka tim telefonskim brojevima). TRIP je zasnovan na BGP protokolu i zbog ostvarivanja dobre podrške za definisanje politika provajdera. Pošto TRIP preuzima filozofiju BGP protokola, definišu se i tzv. ITAD (*IP Telephony Administrative Domain*) domeni koji predstavljaju skup gejtveja, lokacijskih servera, i drugih uređaja vezanih za telefoniju u paketskim mrežama koji spadaju pod kontrolu istog administratora. Otuda se razlikuje interdomenska komunikacija između lokacijskih servera i intradomenska komunikacija između lokacijskih servera.



Slika 10.3.1.1. Zaglavlja TRIP poruke

Lokacijski serveri sa svojim susedima uspostavljaju TCP konekciju i potom razmenjuju TRIP poruke kojih ima 4 tipa (OPEN, NOTIFICATION, UPDATE, KEEPALIVE). Kao što vidimo, koriste se isti nazivi poruka kao kod BGP protokola (i uloge tih tipova poruka su slični ulogama iz BGP protokola). Poruke između lokacijskih servera različitih ITAD domena se razmenjuju po tačka-tačka principu, dok se unutar istog ITAD domena razmena vrši principom plavljenja (ova osobina je preuzeta iz OSPF protokola). Da bi se postigla bolja skalabilnost unutar ITAD domena, lokacijski serveri iz istog ITAD domena ne moraju da budu povezani svaki sa svakim (kao u BGP slučaju, mada se i tamo mogu koristiti alternatnivna rešenja poput konfederacija i reflektora ruta) već je dozvoljeno formiranje topologije povezanosti lokacijskih servera po principu formiranja topologije povezanosti rutera u OSPF protokolu. TRIP poruke se sastoje od zaglavlja i eventualnog korisnog dela.

Struktura TRIP zaglavlja je prikazana na slici 10.3.1.1. TRIP zaglavlje se sastoji od tri bajta. Prva dva bajta definišu dužinu TRIP poruke u bajtovima (računajući i TRIP zaglavlje i korisni deo TRIP poruke). Pri tome, minimalna dužina je 3 bajta (samo TRIP zaglavlje), a maksimalna dužina je 4096 bajtova. Treći bajt predstavlja tip poruke. Kao što je već napomenuto, postoje 4 tipa TRIP poruka (u zagradama pored naziva je data vrednost polja tip za dotičnu poruku): OPEN (1), UDPATE (2), KEEPALIVE (3), NOTIFICATION (4).

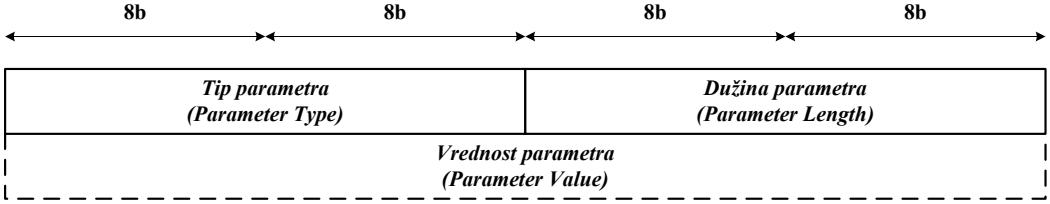


Slika 10.3.1.2. OPEN poruka

Struktura korisnog dela TRIP poruke za slučaj OPEN poruke je prikazana na slici 10.3.1.2. OPEN poruka se koristi za otvaranje sesije susedstva lokacijskih servera. Nakon što se otvori TCP veza, obe strane šalju OPEN poruku. Ukoliko je OPEN poruka prihvatljiva onda se ona potvrđuje slanjem KEEPALIVE poruke. Po prijemu KEEPALIVE poruke se smatra da je TRIP veza (susedstvo) otvorena i može da otpočne razmena UPDATE, KEEPALIVE i NOTIFICATION poruka. OPEN poruka se sastoji iz sledećih polja:

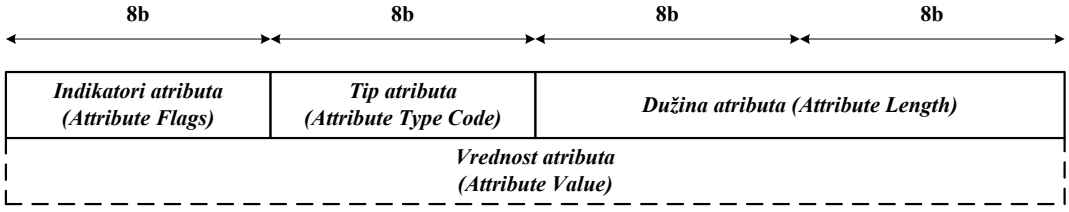
- Verzija - Polje dužine 1 bajt koje označava verziju TRIP protokola. Trenutna verzija je 1.
- Rezervni biti - Ovi biti su namenjeni za eventualnu buduću upotrebu.
- Vreme čekanja - Ovo šesnaestobitno polje definiše maksimalno vreme u sekundama koje sme da prođe između prijema dve susedne TRIP poruke (UPDATE ili KEEPALIVE, pošto se one šalju u regularnim situacijama). Po prijemu OPEN poruke, lokacijski server upoređuje vreme čekanja koje je primio od suseda, kao i svoje predloženo vreme čekanja (koje je i poslao u svojoj OPEN poruci) i za konačno vreme čekanja, koje će zaista i koristiti, bira manju od te dve vrednosti.
- ITAD pošiljaoca - Ovo 32-bitno polje definiše ITAD broj lokacijskog servera od koga je primljena OPEN poruka. ITAD broj unutar konfederacije ITAD domena koje međusobno povezuju svoje lokacijske servere ne sme da se ponavlja (ne sme više lokacijskih servera da ima isti ITAD broj). ITAD brojeve dodeljuje IANA organizacija.
- TRIP identifikator - Ovo 32-bitno polje predstavlja jedinstvenu identifikaciju lokacijskog servera unutar svog ITAD domena.

- Dužina opcionih parametara - Ovo šesnaestobitno polje definiše ukupnu dužinu opcionih parametara u bajtovima. Ako je vrednost ovog polja 0, tada opcioni parametri ne postoje u OPEN poruci.
- Opcioni parametri - Ovo polje sadrži jedan ili više opcionih parametara (ako opcioni parametri postoje u OPEN poruci). Opcioni parametri definišu skup mogućnosti lokacijskog servera. Format jednog opcionog parametra je prikazan na slici 10.3.1.3. Tip parametra određuje tip opcionog parametra. Dužina parametra određuje dužinu polja vrednost parametra u bajtovima. Polje vrednost parametra sadrži samu vrednost opcionog parametra. Tip 1 predstavlja opcioni parametar za opis 'tehničkih' mogućnosti lokacijskog servera. RFC 3219 definiše dve 'tehničke' mogućnosti lokacijskog servera. Mogućnost primopredaje definiše podržani mod slanja lokacijskog servera (može samo da šalje, može samo da prima, može i da šalje i da prima). Druga 'tehnička' mogućnost se odnosi na podršku tipovima adresa i protokola. Tipovi adresa koje predviđa TRIP su decimalni brojevi prosleđivanja, pentadecimalni brojevi prosleđivanja i E.164 brojevi (definicije ovih formata su date u RFC 3219). Tipovi protokola koje predviđa TRIP su SIP, H.323-H.225.0-Q.931 (tj. H.225.0 kontrola poziva), H.323-H.225.0-RAS (tj. H.225.0 RAS), H.323-H.225.0-Annex-G.



Slika 10.3.1.3. Struktura opcionog parametra

UPDATE poruka je poruka kojom lokacijski serveri razmenjuju svoje podatke o dostupnosti telefonskih brojeva tj. informacije o gejtvejima, i na osnovu kojih ažuriraju svoje baze podataka. Korisni deo TRIP poruke se, u slučaju UPDATE poruke, sastoji od niza atributa ruta, a struktura jednog atributa rute je prikazana na slici 10.3.1.4.



Slika 10.3.1.4. Struktura atributa rute

Atribut rute se sastoji od sledećih polja:

- Indikatori atributa - Ovi indikatori određuju procesiranje i pre svega prosleđivanje atributa. Svaki indikator je dužine jedan bit. Indikatori koji su trenutno definisani su:
    - *Well-Known Flag* - Određuje da li je atribut dobro poznat ili ne. Ako je atribut dobro poznat, tada lokacijski server mora da podržava njegovu

obradu, u suprotnom nije u obavezi da implementira podršku za dotični atribut. Vrednost 0 označava da je atribut dobro poznat.

- *Transitive Flag* - Ovaj indikator određuje da li se atribut, koji nije dobro poznat i pri tome nije podržan od strane lokacijskog servera koji ga je primio, prosleđuje dalje ili ne. Vrednost 1 označava da je atribut tranzitivan. Ako je atribut dobro poznat, ovaj indikator na predaji mora biti postavljen na 0, a na prijemu se ignoriše njegovo tumačenje.
- *Dependent Flag* - Ovaj indikator određuje za tranzitivne atribute da li je atribut zavisan (vrednost 1) ili ne (vrednost 0), što se koristi prilikom odluke da li da se nepodržani tranzitivni atribut prosledi dalje ili ne (nepodržani nezavisni tranzitivni atribut se uvek prosleđuje dalje, a prosleđivanje nepodržanog zavisnog tranzitivnog atributa zavisi od određenih uslova). Za dobro poznate atribute ili netranzitivne atribute vrednost ovog bita nije bitna, pa se na predaji postavlja na 0, a na prijemu se ne tumači.
- *Partial Flag* - Ovaj indikator određuje da li je atribut, koji nije dobro poznat, parcijalan (vrednost 1) ili kompletan (vrednost 0). U suštini parcijalan atribut signalizira da nisu svi lokacijski serveri na prethodnom delu puta UPDATE poruke razumeli i procesirali dotični atribut. Za dobro poznate atribute ili netranzitivne atribute vrednost ovog bita nije bitna, pa se na predaji postavlja na 0, a na prijemu se ne tumači.
- *Link-state Encapsulation Flag* - Ovaj indikator je relevantan samo za određene atribute (*ReachableRoutes* i *WithdrawnRoutes* atributi) i definiše način enkapsulacije oglašenih/povučenih ruta u tim atributima, tj. da li se koristi *link-state* enkapsulacija ili ne. Za atribute koji ne koriste ovaj indikator se ovaj bit na predaji postavlja na 0, a na prijemu se ne tumači. Atributi koji koriste *link-state* enkapsulaciju imaju dodatna dva polja koja se nalaze između dužine atributa i vrednosti atributa. To su polje TRIP identifikator izvorišta (*Originator TRIP Identifier*) i redni broj (*Sequence Number*) koji se koriste za kontrolu plavljenja (plavljenje može da se koristi samo u intradomenskoj komunikaciji).

Preostala tri bita ovog polja koja se ne koriste su postavljeni na 0.

- Tip atributa - Ovo osmobitno polje definiše tip atributa. Postoji više tipova atributa koji su veoma slični atributima koji se koriste u BGP protokolu. Neki od atributa su:
  - *WithdrawnRoutes* - Lista povučenih ruta (i destinacija).
  - *ReachableRoutes* - Lista oglašenih ruta (i destinacija).
  - *AdvertisementPath* - Ovaj atribut predstavlja putanju kojom je išlo dotično obaveštenje, pri čemu je putanja navedena u vidu niza ITAD domena kroz koje se prošlo. Koristi se za detekciju petlji.
  - *LocalPreference* - Ovaj atribut ima značaja u intradomenskoj komunikaciji i označava poželjni granični lokacijski server za određenu

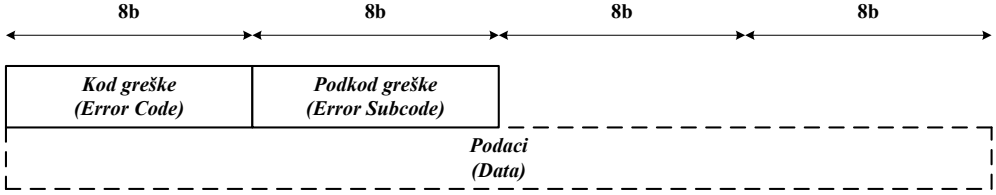
destinaciju (granični u smislu da se preko njega izlazi u drugi ITAD domen).

- Dužina atributa - Ovo polje predstavlja dužinu vrednosti atributa u bajtovima.
- Vrednost atributa - Ovo polje sadrži koristan sadržaj atributa.

KEEPALIVE poruke se sastoje samo od TRIP zaglavlja (nema korisnog dela). Koriste za održavanje susedstva između lokacijskih servera da znaju da je otvorena sesija (susedstvo) između njih i dalje u redu, odnosno aktivna.

NOTIFICATION poruke se koriste za obaveštavanje o greškama. Ako se prijavi greška vrši se i zatvaranje susedstva između dotičnih lokacijskih servera, pa se mora ponovo pokrenuti procedura otvaranja veze radi ponovnog uspostavljanja susedstva. Struktura ove poruke (deo koji ide iza TRIP zaglavlja) je data na slici 10.3.1.5. Kod i podkod greške označavaju tip greške koja se prijavljuje, a u podacima se nalaze detaljniji podaci o prijavljenoj grešci. Greške koje se mogu prijaviti su:

- Greške u zaglavlju TRIP poruke (nevalidna dužina poruke, nevalidan tip).
- Greške u OPEN poruci (nepodržana verzija, nepodržan opcioni parametar,...).
- Greške u UPDATE poruci (nevalidna dužina atributa, nevalidne vrednosti indikatora atributa,..).
- Isteklo vreme čekanja.
- Greška konačnog automata (TRIP protokol implementacija funkcioniše po principu konačnog automata zasnovanog na BGP konačnom automatu).
- Zatvaranje veze. U suštini ovaj tip greške i nije greška, već suprotna strana iz nekog razloga želi da zatvori vezu i raskine susedstvo.

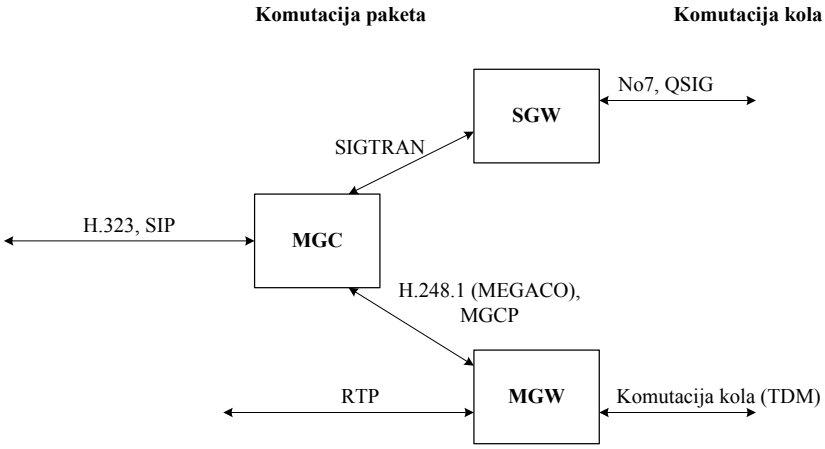


Slika 10.3.1.5. NOTIFICATION poruka

10.3.2. Gejtvej

Terminologija koja se koristi za gejtveje između mreže sa komutacijom kola i paketske mreže je veoma raznovrsna pa se dešava da se za istu funkcionalnost ili uređaj naiđe na nemali broj različitih naziva, a takođe da se za isti termin nađu različite definicije i tumačenja, pa to može da izazove određenu konfuziju prilikom proučavanja literature i proizvoda vezanih za ovu oblast. Gejtvej treba da izvrši dve osnovne funkcije – konverziju signalizacije i konverziju multimedijalnog sadržaja (tipično samo govornog sadržaja). Konverzija signalizacionog sadržaja se vrši u tzv. signalizacionim gejtvejima SGW (koristi se i oznaka SG). Međutim, SGW termin se koristi i za označavanje paketskog transporta (transport kroz paketsku mrežu) signalizacionih poruka iz mreže sa komutacijom kola (No7, QSIG signalizacije), pa u ovom slučaju SGW vrši samo prilagođenje signalizacionih poruka za prenos preko paketske mreže. Tada se u slučaju da te poruke završavaju u paketskoj mreži (jer se jedan od korisnika u vezi nalazi u paketskoj

mreži), konverzija u SIP ili H.323 signalizaciju (i obrnuto) vrši u nekom drugom uređaju, tipično u MGC-u. Konverzija multimedijalnog sadržaja se vrši u medija gejtvejima MGW (koristi se i oznaka MG). Kontrolu rada ova dva gejtveja vrši kontroler MGC koji se još naziva i softsvič da bi se naglasilo da je MGC implementiran softverski (takođe se koriste i termini server poziva (*call server*), kao i agent poziva (*call agent*) da bi se naglasilo da je tu smeštena inteligencija pri obradi poziva). MGC treba da upravlja signalizacionim gejtvejom (SGW) da bi se obezbedila pravilna razmena signalizacije u paketskoj mreži i mreži sa komutacijom kola, a i da bi dobio neophodne informacije za konfigurisanje MGW. Naime, MGW treba da se konfiguriše ne samo da bi se ispravno obavila konverzija multimedijalnog sadržaja, već i da bi se postiglo ispravno slanje i prijem multimedijalnog sadržaja u i iz paketske mreže i mreže bazirane na komutaciji kola, a takođe i ispravna komutacija multimedijalnog sadržaja iz paketske mreže u mrežu komutacije kola i obrnuto. Na primer, ako se koristi E1 link za povezivanje na fiksnu telefonsku mrežu, neophodno je znati u koji govorni kanal treba smeštati govorne odmerke dobijene konverzijom RTP paketa jedne veze, odnosno koje govorne odmerke treba uzimati da bi se od njih kreirali RTP paketi dotične veze. Takođe, bitno je da MGW zna i na koje IP adrese i transportne portove treba da šalje generisane RTP pakete, odnosno na kojim portovima prima RTP pakete. Očigledno, MGW radi svojevrsnu komutaciju jer RTP pakete jedne veze smešta u odgovarajući kanal na strani komutacije kola, i obrnuto, iz odgovarajućeg kanala na strani komutacije kola uzima odmerke i formira RTP pakete koje šalje na suprotnu stranu ka odgovarajućem korisniku iz paketske mreže. MGC koristi standardizovane protokole za komunikaciju i upravljanje SGW i MGW gejtvejima, kao što je prikazano na slici 10.3.2.1. Na slici je prikazana češća varijanta gde SGW vrši samo prilagođenje signalizacionih poruka i njihovo prosleđivanje ka MGC (u obrnutom smeru vrši prijem poruka i njihovu translaciju u originalan oblik namenjen za prenos kroz mrežu baziranu na komutaciji kola).



Slika 10.3.2.1. Generalna struktura gejtveja

SIGTRAN protokol, ustvari, predstavlja okvir i skup protokola za prenos No7 (ali i Q.931 i QSIG) signalizacije između SGW i MGC preko IP protokola. U RFC 2719 je predstavljen okvir za prenos signalizacionih poruka preko IP. SIGTRAN koristi SCTP protokol kao transportni protokol, a takođe koristi i adaptacione MTP slojeve No7 signalizacije kojima se omogućuje funkcionalnost drugog i trećeg MTP sloja u prenosu No7 signalizacionih poruka preko IP mreže. U ovom slučaju se No7 poruke prenose do MGC koji vrši na osnovu njih formiranje odgovarajućih SIP ili H.323 poruka (MGC radi, naravno, i konverziju u obrnutom

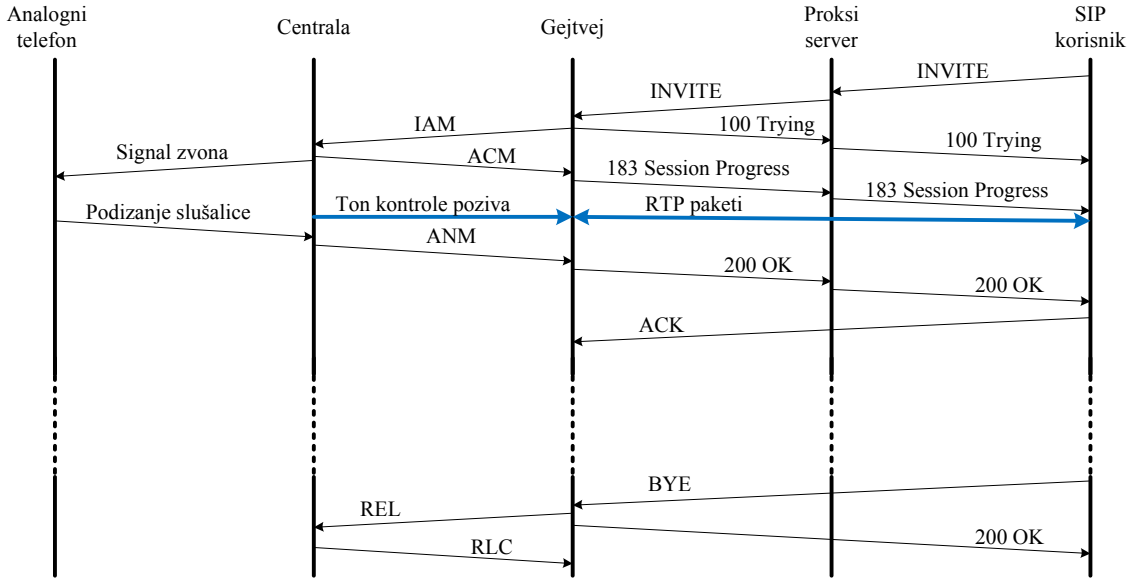
smeru). Kao što je rečeno SIGTRAN omogućava i prenos Q.931 i QSIG signalizacionih poruka preko IP.

Za povezivanje MGC i MGW se koristi H.248.1 protokol (*Gateway Control Protocol Version 1*) koji se u praksi još naziva i MEGACO protokol jer je H.248.1 protokol nastao kao rezultat udruženog rada ITU-T i IETF organizacije. MEGACO protokol koji je inkorporiran u H.248.1 protokol je definisan u RFC 3525, ali njegovom integracijom u H.248.1 standard, RFC 3525 je zvanično prestao da važi kao važeća preporuka. Kao protokol za povezivanje MGC i MGW se može koristiti i MGCP (*Media Gateway Control Protocol*) definisan u RFC 3435. Pri tome, MGCP i H.248.1 (MEGACO) nisu međusobno kompatibilni. Pošto je H.248.1 rezultat zajedničkog rada IETF i ITU-T, obe organizacije preporučuju upotrebu H.248.1 (MEGACO) protokola. U okviru ovog teksta nećemo ulaziti u detalje rada SIGTRAN, H.248.1 i MGCP protokola.

U samoj implementaciji gejtveja može doći do integracije pojedinih delova u jedinstvenu celinu. Na primer, MGW i SGW se mogu spojiti u zajedničku celinu jer se govorni kanali i signalizacioni kanali prenose istim linkom pa samim tim završavaju na istom mestu tj. uređaju. Takođe, u nekim implementacijama su MGC i MGW spojeni u istu celinu. Same implementacije prvenstveno zavise od odluka proizvođača, tako da u praksi postoje raznovrsna rešenja.

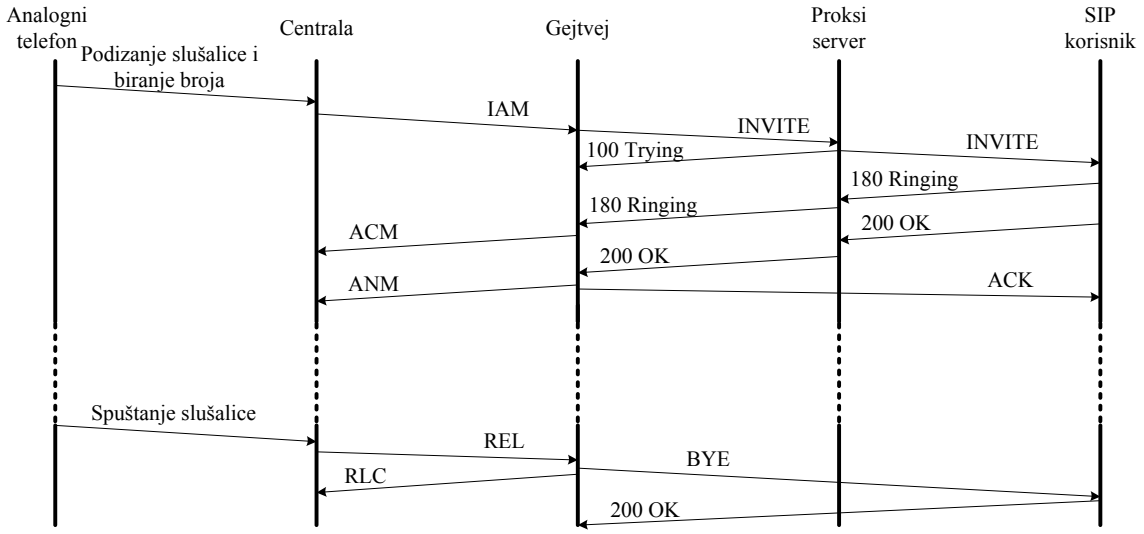
10.3.3. Primer uspostave veze između korisnika u različitim tipovima mreže

U okviru ove sekcije ćemo prikazati primere uspostave veze između H.323/SIP korisnika i korisnika u fiksnoj telefonskoj mreži. U primerima će biti pretpostavljena No7 signalizacija u okviru fiksne telefonske mreže, i takođe će se smatrati da se u uspostavi veze koristi samo jedna centrala (na koju je priključen korisnik koji komunicira sa korisnikom iz paketske mreže), ali princip razmene No7 signalizacije bi bio isti i za slučaj tranzita kroz više centrala kao što je pokazano u poglavlju 6. Takođe, u slučaju H.323/SIP signalizacije će biti pretpostavljena direktna razmena signalizacije H.323/SIP korisnika i gejtveja (sem inicijalne razmene preko gejtkipera/proksi servera). Slučajeve gde kompletna signalizacija prolazi kroz gejtkiper/proksi server je lako izvesti iz datih primera koristeći primere razmene H.323/SIP signalizacije koji su dati ranije u ovom poglavlju.



Slika 10.3.3.1. Poziv između SIP korisnika i korisnika iz fiksne telefonije - SIP korisnik inicijator

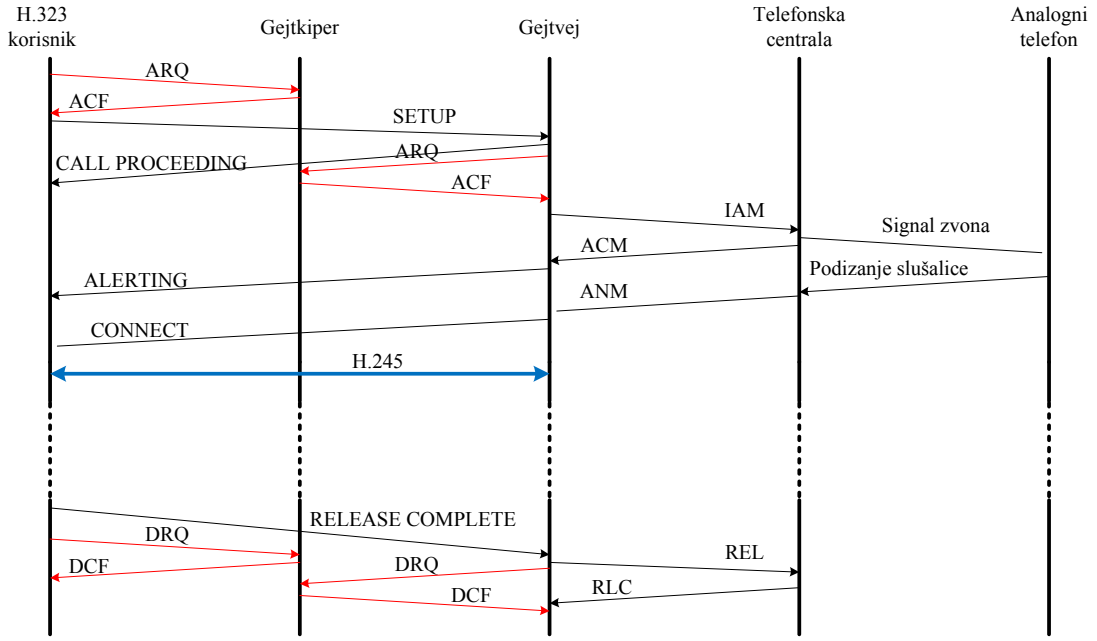
Na slici 10.3.3.1. je prikazan slučaj kada SIP korisnik naziva korisnika iz fiksne telefonske mreže. SIP korisnik generiše INVITE zahtev (birani telefonski broj je konvertovan ENUM postupkom u kvalifikovano domensko ime). Proksi server na osnovu konvertovanog biranog broja određuje (konsultujući lokacijski server ili DNS server) da poziv mora da se uputi odgovarajućem gejtveju, pa se INVITE zahtev upućuje gejtveju. Odgovori 100 označavaju SIP korisniku, odnosno proksi serveru da je proksi server, odnosno gejtvej primio INVITE zahtev i da ga procesira. Gejtvej šalje IAM poruku centrali sa ciframa traženog korisnika. Korisniku se pušta signal zvona i vraća se ACM poruka gejtveju. Gejtvej generiše poruku 183 proksi serveru, a ovaj je prosleđuje ka SIP korisniku. Mogla se koristiti i poruka 180 kojom bi SIP terminal generisao lokalni ton kontrole poziva pozivajućem korisniku. Međutim, odgovor 183 sadrži opis sesije tako da može da se uspostavi govorni put (multimedijalna sesija) u paketskoj mreži. Time se signalizira SIP terminalu da ne pušta lokalni ton zvona korisniku nego ton koji prima od gejtveja, a gejtvej, ustvari, prosleđuje ton kontrole poziva (samo u paketizovanom obliku) koji prima od centrale preko zauzetog govornog puta između centrale i gejtveja. Razlog za varijantu sa 183 odgovorom je taj što umesto tona kontrole poziva centrala može da pusti neko govorno obaveštenje (na primer, 'sačekajte trenutak' i sl.) kojim se dobija precizniji opis trenutnog stanja poziva. Kada se traženi korisnik odazove, centrala šalje ANM poruku. Gejtvej šalje odgovor 200 koji preko proksi servera stiže do SIP korisnika. U 200 odgovoru se daje isti opis sesije kao i u 183 odgovoru tako da uspostavljeni govorni put u paketskoj mreži ostaje nepromenjenih parametara prenosa. SIP korisnik šalje ACK odgovor direktno gejtveju i komunikacija može da krene. SIP korisnik raskida vezu slanjem BYE zahteva gejtveju. Gejtvej istovremeno šalje 200 odgovor SIP korisniku potvrđujući raskid veze, a takođe šalje REL poruku centrali koja je potvrđuje RLC porukom (u tom procesu je oslobođen zauzeti govorni put u fiksnoj telefonskoj mreži).



Slika 10.3.3.2. Poziv između SIP korisnika i korisnika iz fiksne telefonije - korisnik fiksne telefonije inicijator

U primeru sa slike 10.3.3.2 korisnik fiksne telefonije naziva SIP korisnika kome je dodeljen validan telefonski broj. Centrala na osnovu biranog broja utvrđuje da poziv treba da rutira ka gejtveju pa mu šalje IAM poruku sa ciframa biranog broja. Gejtvej kreira INVITE poruku koju šalje ka proksi serveru (telefonski broj je konvertovao ENUM postupkom u kvalifikovano domensko ime). Proksi server odgovorom 100 signalizira da je primio INVITE zahtevi da ga procesira. Proksi server vrši upit ili lokacijskom serveru ili DNS serveru (u

zavisnosti kako je konfigurisan za slučaj telefonskih brojeva konvertovanih u domensko ime ENUM postupkom) i dobija lokaciju traženog SIP korisnika kome prosleđuje INVITE poruku. SIP terminal odgovorom 180 signalizira 'zvonjenje' telefona. Proksi server prosleđuje ovaj odgovor gejtveju, koji potom generiše ACM poruku centrali da je pušten ton zvona SIP korisniku. Gejtvej u ovom momentu može da pusti ton kontrole poziva pozivajućem korisniku koji će u svojoj slušalici da čuje taj ton. Kada se korisnik odazove generisaće odgovor 200 koji će preko proksi servera stići do gejtveja. Ovim odgovorom je uspostavljena multimedijalna sesija u paketskoj mreži. Gejtvej generiše ANM odgovor centrali i ACK odgovor direktno ka SIP korisniku. Razgovor je uspostavljen. Kada pozivajući korisnik spusti slušalicu, centrala generiše REL poruku. Gejtvej istovremeno šalje RLC poruku centrali (govorni put se takođe oslobađa u fiksnoj telefonskoj mreži) i BYE poruku SIP korisniku. SIP korisnik odgovorom 200 potvrđuje BYE zahtev, tj. raskid veze.

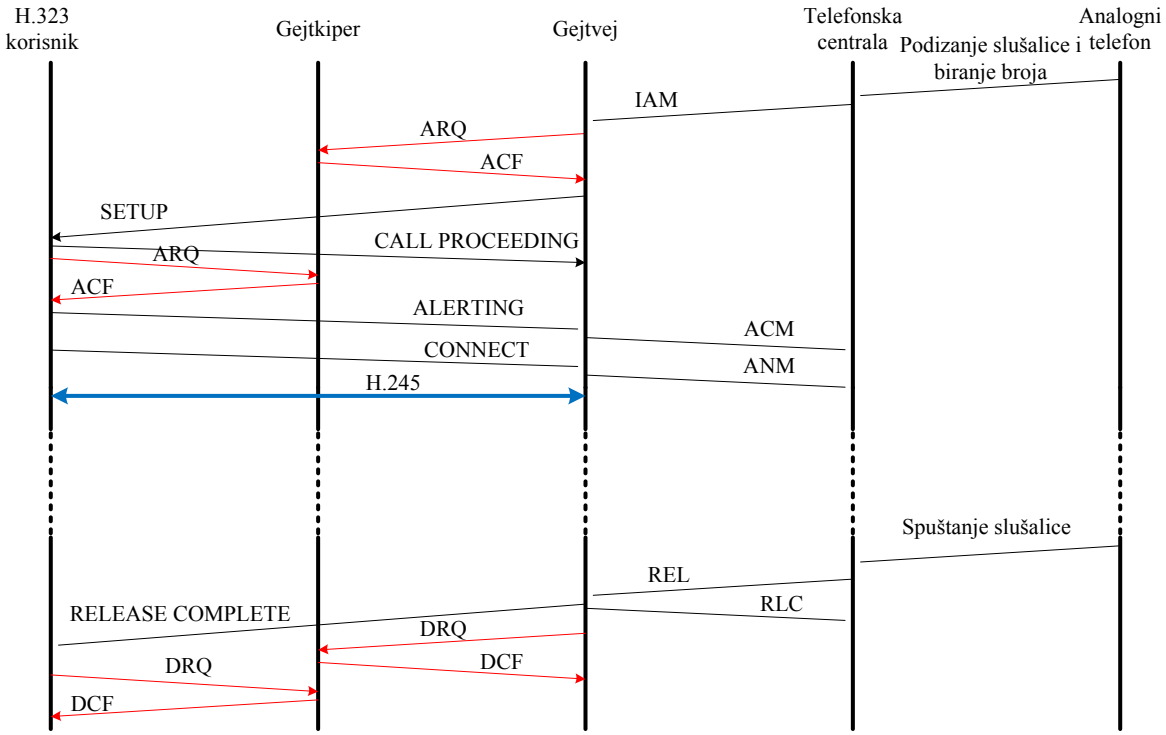


Slika 10.3.3.3. Poziv između H.323 korisnika i korisnika iz fiksne telefonije - H.323 korisnik inicijator

Na slici 10.3.3.3 je prikazana uspostava veze između H.323 korisnika i korisnika fiksne telefonije, gde je H.323 korisnik pozivajući korisnik. H.323 korisnik prvo traži dozvolu za uspostavom veze od gejtkipera, koji mu je odobrava i takođe mu prosleđuje adresu gejtveja (gejtkiper takođe vrši upit lokacijskom serveru ili DNS serveru za određivanje gejtveja na koji treba uputiti poziv). H.323 korisnik generiše SETUP poruku ka gejtveju, a gejtvej potvrđuje prijem poruke sa CALL PROCEEDING porukom. Gejtvej traži dozvolu od gejtkipera ARQ porukom i kada je dobije šalje IAM poruku centrali. Centrala šalje signal zvona traženom korisniku, a ACM poruku gejtveju. Gejtvej šalje ALERTING poruku H.323 korisniku čime se signalizira da traženom korisniku zvoni telefon. Kada se traženi korisnik odazove, centrala šalje ANM poruku gejtveju koji potom šalje CONNECT poruku H.323 terminalu. H.245 signalizacijom se uspostavlja multimedijalna sesija između H.323 terminala i gejtveja pa razgovor može da otpočne. H.323 terminal signalizira kraj veze slanjem RELEASE COMPLETE poruke gejtveju. Gejtvej šalje REL poruku centrali i takođe prijavljuje raskid veze gejtkiperu DRQ porukom. H.323 terminal takođe prijavljuje raskid veze gejtkiperu DRQ porukom. Centrala

vraća poruku RLC kao potvrdu raskida veze (govorni put u fiksnoj telefonskoj mreži je takođe oslobođen).

Na slici 10.3.3.4 je prikazana uspostava veze između H.323 korisnika i korisnika fiksne telefonije, gde je korisnik iz fiksne telefonije pozivajući korisnik. Korisnik podiže slušalicu i bira telefonski broj. Centrala na osnovu biranog broja utvrđuje da poziv treba da rutira ka gejtveju pa mu šalje IAM poruku sa ciframa biranog broja. Gejtvej prvo traži dozvolu od gejtkipera ARQ porukom (u okviru koje se nalazi konvertovan telefonski broj ENUM postupkom). Gejtkiper odobrava vezu ACF porukom u koju smešta lokaciju traženog H.323 korisnika. Gejtvej šalje SETUP poruku H.323 korisniku, koji na nju odgovara CALL PROCEEDING porukom čime signalizira prijem SETUP poruke i njeno procesiranje. H.323 korisnik traži dozvolu od gejtkipera i kada je dobije šalje ALERTING poruku gejtveju čime signalizira 'zvonjenje' telefona H.323 korisnika. Gejtvej obaveštava centralu ACM porukom (gejtvej može da generiše ton kontrole poziva koji bi se slao pozivajućem korisniku). Kada se H.323 korisnik odazove, H.323 terminal šalje CONNECT poruku gejtveju, a gejtvej šalje ANM poruku centrali. Razmenom H.245 signalizacije kreira se govorni put (multimedijalna sesija) kroz paketsku mrežu i razgovor može da krene. Kada pozivajući korisnik spusti slušalicu, centrala šalje REL poruku gejtveju. Gejtvej istovremeno šalje RLC poruku centrali i RELEASE COMPLETE poruku H.323 korisniku. Gejtvej i H.323 korisnik DRQ porukom prijavljuju gejtkiperu kraj veze.



Slika 10.3.3.4. Poziv između H.323 korisnika i korisnika iz fiksne telefonije - korisnik fiksne telefonije inicijator