UNIVERZA V LJUBLJANI
Fakulteta za elektrotehniko

Damjan Jelovčan

VPELJAVA PROTOKOLA SIP V KONVERGENČNA TELEKOMUNIKACIJSKA OMREŽJA

MAGISTRSKO DELO

Mentor: prof. dr. Janez Bešter

Ljubljana, 2006

ZAHVALA

Zahvaljujem se vsem, ki so mi pomagali in me vzpodbujali pri izdelavi magistrske naloge.

Najprej se zahvaljujem svoji družini, očetu Vinkotu, materi Anici, bratu Igorju ter sestri Andreji, ki so mi stali ob strani med pripravami in pisanjem magistrske naloge.

Zahvaljujem se sodelavcem v podjetjih Iskratel, d.o.o., in Siemens AG, ki so mi omogočili, da sem se seznanil s tem zanimivim področjem in mi nudili potrebne informacije.

Posebej pa se zahvaljujem mentorju prof. dr. Janezu Beštru za usmerjanje in vso pomoč.

KAZALO

SLIKE:

TABELE:

1. Povzetek

V zadnjih desetletjih so telekomunikacije eno izmed najhitreje razvijajočih se področij. Kar se nam je še pred desetletjem zdelo skoraj nemogoče, se danes pravzaprav dogaja. Govorne komunikacije se namreč selijo iz dobro uveljavljenih in priznanih tradicionalnih, povezavno orientiranih omrežij v konvergenčna, paketno orientirana omrežja, ki so osnovana na internetnem protokolu. Prednosti, ki jih ta migracija prinaša, so v največji meri pisane na kožo upravljavcem omrežij in ponudnikom storitev. Poleg prednosti pa naletimo tudi na probleme, ki nastanejo ravno zaradi osnovnih lastnosti paketnih omrežij. Seveda ne smemo pozabiti tudi na končne uporabnike, ki pričakujejo vedno nove in nove storitve, pri čemer morata varnost in kvaliteta storitev ostati na približno istem nivoju.

Magistrsko delo predstavlja trenutno stanje na področju integracije in uveljavljanja protokola za vzpostavljanje sej (SIP – *Session Initiation Protocol*) v konvergenčna omrežja. Protokol SIP namreč zagotavlja vzpostavitev govornih in video komunikacij, prenos hipnih sporočil, ugotavljanje prisotnosti itd. Od začetne uporabe v internetni telefoniji se je razširil na veliko novih področij. Njegova funkcionalnost se zato precej hitro spreminja v skladu z novimi zahtevami, kar pa dejansko pomeni tudi povečanje kompleksnosti samega protokola. Delo je tako razdeljeno na štiri glavne dele. Prvi del je namenjen opisu signalizacijskega protokola SIP. V naslednjem delu se spoznamo s konvergenčnimi omrežji in komunikacijami ter procesom integracije protokola SIP. Nato so izpostavljeni še najbolj pereči problemi, ki nastopijo pri vpeljavi protokola. Zadnji del pa je namenjen praktičnemu primeru.

Za samo razumevanje dela je na prvem mestu potrebno razumevanje osnov samega protokola SIP. S temi osnovami se spoznamo takoj na začetku, kjer so za lažje razumevanje pripravljeni tudi nekateri najosnovnejši dialogi. Nato se spoznamo s ključnimi elementi protokola, z različnimi entitetami (različni uporabniški agenti in strežniki), osnovnimi termini (dialog, transakcija, seja) in glavnimi protokolnimi sporočili, ki so razdeljena v dve skupini: v skupino zahtev in skupino odgovorov. Posebno mesto je namenjeno tudi opisu protokola za opis seje (SDP – *Session Description Protocol*), ki je namenjen prenosu informacij o medijskih tokovih. Konec

prvega dela je namenjen predstavitvi najpogostejših oz. najpomembnejših SIP scenarijev.

V drugem delu so predstavljeni razlogi za razvoj in nadgradnjo komunikacijskih omrežij s treh različnih vidikov: poslovnega, uporabniškega ter informacijskega. Nato je opisan evolucijski potek razvoja komunikacijskih omrežij: od omrežij z ločeno infrastrukturo do konvergenčnih omrežij in naprej do konvergenčnih komunikacij. Sledi predstavitev nekaj konkretnih primerov konvergenčnih komunikacij in razlogov zakaj se protokol SIP temu tako dobro prilagaja. Opisan je tudi postopek same integracije oz. vpeljave protokola SIP v konvergenčna omrežja.

Tretji del naloge je namenjen obravnavi raznovrstnih problemov, ki predstavljajo največje težave pri uveljavitvi protokola SIP in konvergenčnih sistemov osnovanih na paketnih omrežjih, katerih osnova je internetni protokol (IP – *Internet Protocol*). Kot prvi je predstavljen problem kvalitete storitev. Tu se najprej spoznamo z osnovnimi dejavniki kvalitete, kot so: zakasnitev, trepetanje, izguba paketov in izločanje odmeva. Nato je predstavljenih nekaj načinov za zagotavljanje kvalitete, nazadnje pa se dotaknemo še zanesljivosti sistemov.

Kot drugi problem je predstavljena varnost. Najprej je pojem varnosti opredeljen kot zagotavljanje celovitosti (zasebnost, verodostojnost in avtentičnost), ki jo je mogoče zagotoviti z uporabo ustreznih protokolov in šifrirnih postopkov. Predstavljenih je tudi nekaj najpogostejših varnostnih problemov, ki so specifični predvsem za IP okolje. Nazadnje pa je predstavljenih nekaj najaktualnejših protokolov za povečevanje varnosti ter kako je za varnost poskrbljeno v okviru protokola SIP.

Na koncu tretjega dela se spoznamo še s problemom prehoda požarnih zidov in naprav, katerih naloga je prevajanje omrežnih naslovov (NAT – *Network Address Translation*).

Zadnji del je namenjen predvsem predstavitvi rezultatov in projekta, ki smo ga v okviru Siemensa izvedli za nizozemskega telekomunikacijskega operaterja KPN. Najprej sta predstavljeni dve Siemensovi rešitvi konvergenčnih sistemov, osnovanih na protokolu SIP, za katere se je KPN odločil in tudi podpisal pogodbo. Nato so predstavljeni osnovni gradniki takega omrežja in njihov varnostni koncept. Na koncu

pa je priloženih še nekaj diagramov poteka klicev določenih storitev, ki jih je KPN zahteval.

Ključne besede: *SIP, SDP, VoIP, IP telefonija, konvergenčna omrežja, konvergenčne komunikacije, varnost, kvaliteta storitve, QoS, NAT, požarna pregrada, kriptiranje.*

Abstract:

In the last few decades telecommunications have become one of the fastest growing areas. What was almost impossible one decade ago is actually happening today. Voice communications are moving from traditional, well established and acknowledged, connection oriented networks towards converged, packet oriented networks based on internet protocol. The ones who gain most advantages from this migration are network operators and service providers. Besides advantages, there are also problems arising from the basic characteristics of packet networks. Of course we cannot forget the end subscribers who are always expecting new and new services provided that security and quality of service remain approximately on the same level as before.

The present M.A. thesis presents the present status of integration and asserting of the session initiation protocol (SIP) into converged networks. SIP enables the establishment of voice and video communications, transmission of instant messages (IM), transmission of presence status, etc. From the first usage in internet telephony it has spread to many new areas. This is the reason why its functionality is changing very fast in accordance with new requests. This actually increases the complexity of the protocol. The thesis is divided into four main parts. The first one focuses on the description of the SIP. In the next part we get acquainted with converged networks and converged communications and also with the process of SIP integration. Then the most important problems appearing because of the integration are exposed. The last part is intended for a practical example.

For the understanding of the thesis in the first place, it is necessary to understand the SIP protocol itself. As it is important to understand the basics already at the beginning, some of the most fundamental dialogs are presented. It follows an

explanation of key elements of SIP, different entities (different user agents and servers), basic terms (dialog, transaction, session) and main protocol messages, which are divided into two groups: group of requests and group of responses. A special place is dedicated to a describing the session description protocol (SDP), which is intended for transmission of information about media flows. At the end of the first part some of the most frequent or most important SIP scenarios are presented.

In the second part are some reasons for development and upgrade of communication networks are presented from three different points of view: business, user and information technology (IT) imperative. Then the evolution of IT infrastructures is described, from networks with separate infrastructure to converged networks and further to converged communications. This is followed by some concrete examples of converged communications and reasons for the flexibility of SIP. There is also a description of the integration procedure or introduction of SIP into converged networks.

The third part is intended for dealing with various problems representing the biggest difficulties in introducing or asserting of SIP and converged systems based on packet networks based on the internet protocol (IP). As the first problem quality of service is presented. First of all, we get to know the basic factors of quality, such as delay, jitter, packet loss and echo cancellation. Then some methods for assuring quality are presented, at last reliability of the systems is mentioned shortly.

Security is presented as the second problem. First the term of security is defined as integrity (privacy, credibility and authenticity) which can be achieved with proper use of communication protocols and cryptographic algorithms. Some of the most frequent security problems specific for IP environment are also presented. Finally, some of the latest protocols for increasing security and ways of handling security issues within SIP are described.

At the end of the third part the problem of traversal of firewalls and devices for network address translation (NAT) is looked into.

The last part is mostly intended for presenting the results and project which was realized in the frame of Siemens for the Dutch telecommunication operator KPN. First of all, two Siemens' solutions for converged systems based on SIP are presented.

They were chosen and contracted by KPN. Then basic parts of those networks and their security concept are shown. At the end some call flows requested by KPN are added.

Keywords: *SIP, SDP, VoIP, IP telephony, converged networks, converged communications, security, quality of service, QoS, NAT, firewall, encryption.*

2. Uvod

Internet nam zagotavlja nešteto načinov za enostavnejše in bogatejše komunikacije med ljudmi. Lahko bi rekli, da nam po eni strani izboljšuje celo življenje, saj nam ponuja mnogo stvari, med drugimi tudi znižanje stroškov, povečanje učinkovitosti in izboljšavo odnosa stranka – ponudnik. Prav tako pa je internet eden od vzrokov oz. povodov za združevanje različnih in do pred kratkim nezdružljivih komunikacijskih omrežij.

Že od začetka interneta nas je motilo dejstvo, da potrebujemo več vzporednih telekomunikacijskih omrežij, kot sta npr. omrežje za prenos govora – javno komutirano telefonsko omrežje (PSTN – *Public Switched Telephone Network*) in omrežje za prenos podatkov – paketno IP omrežje. Z obratovanjem večih omrežij tako povečujemo stroške za inštalacijo, vzdrževanje, nadgrajevanje, nadzorovanje itd.

IP telefonija nam ponuja prav to – združitev dveh popolnoma različnih omrežij v eno. Ker pa so trendi pravzaprav taki, da bo prenos podatkov slej ko prej izpodrinil govor, je bila najboljša rešitev prenos govora v omrežje IP. IP standard je postal "de facto" standard za vsa podatkovna omrežja. Prav zato in pa zaradi njegove univerzalne prisotnosti v osebnih računalnikih (PC – *Personal Computer*), strežnikih in delovnih postajah je bil tudi izbran protokol za IP telefonijo, kljub temu, da za to ni najbolj primeren.

Spremembe, ki jih je povzročil internet, nam pravzaprav pomagajo slediti poti, ki nam jo narekujejo proizvajalci telekomunikacijske opreme. Toda kljub temu še vedno ostaja dvom, saj smo kljub vsemu kar se dogaja okoli tega, npr. zlivanje telekomunikacijskih omrežij, prenosu videa in govora preko IP-ja, IP telefoniji itd., še vedno precej zbegani. Koliko IP-ja sploh potrebujemo? Kje vse pri svojem delu in kdaj ga potrebujemo? Ali bi lahko delali brez tega? Bomo morali vso dosedanjo opremo zamenjati z novo in začeti na novo?

Postavlja se nam mnogo vprašanj, vendar eno je gotovo: IP tehnologija se bo nadaljevala, mi pa moramo vse skupaj vsaj razumeti in se na to tudi pripraviti, saj

prenos govornih podatkov preko omrežja IP (VoIP – *Voice over IP*) omogoča govorne storitve po konkurenčnih cenah, hkrati pa neposredna dostopnost omrežja IP omogoča ponujanje razširjenega nabora aplikacij oz. njihovo lažjo integracijo s podatkovnimi storitvami.

Omenjene prednosti so povod vse večjemu razmahu tehnologij VoIP; z večanjem števila uporabnikov pa narašča tudi število potencialnih napadov in vdorov, kar narekuje potrebo po implementaciji novih pristopov za zagotavljanje varnosti pri govorni komunikaciji v omrežjih IP.

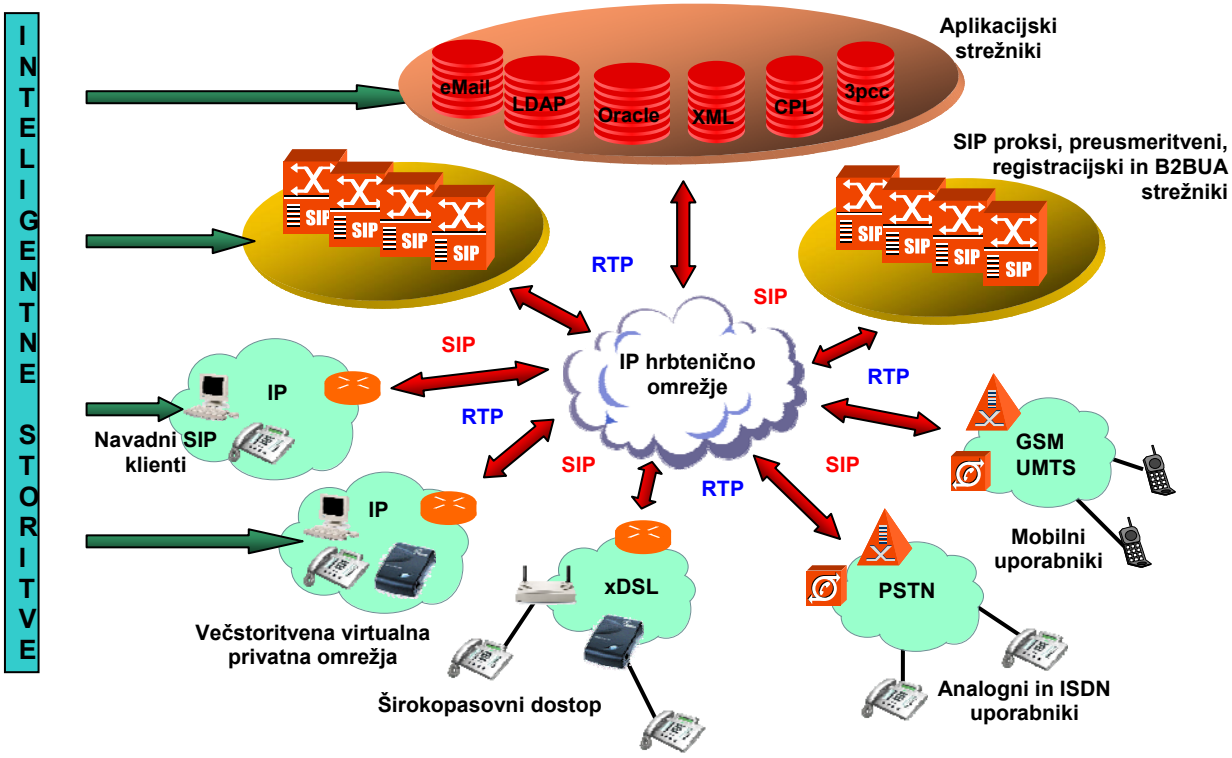
Kot je značilno za vse tehnologije v razvoju, se tudi pri pisanju standardov za VoIP pojavljajo različni predlogi. Starejši protokol H.323, ki ga je razvilo mednarodno telekomunikacijsko združenje (ITU – *International Telecommunications Union*) [ITU_00], se počasi že umika. Novejši protokol SIP, ki ga je razvila delovna skupina za internetsko inženirstvo (IETF – *Internet Engineering Task Force*) [IETF], pa počasi pridobiva na veljavi. Od začetne uporabe v internetni telefoniji se je razširil na veliko novih področij. Dejansko je uporabljen v sklopu prenosa govora, videa, hipnih sporočil (IM – *Instant Messages*), prisotnosti (angl. *presence*), avdio-video konferenčnih zvez in multimedijskega sodelovanja med uporabniki (RTC – *Real Time Collaboration*). Njegova funkcionalnost se hitro spreminja v skladu z novimi potrebami in zahtevami, tako da bo verjetno postal vodilni protokol pri povezovanju končnih točk, še vedno pa je precej nejasno ali bo uspel zagotoviti nov model arhitekture in aplikacij v IP telefonskem omrežju.

SIP je postal razširjen standardni mehanizem, ki z uporabo večih, od medijev neodvisnih načinov, zagotavlja praktičen način integracije storitev različnih omrežij. Protokol tako postaja pomemben del tako korporacijskih kot brezžičnih omrežij novih generacij (NGN – *Next Generation Networks*).

Zadnje čase se vedno bolj uveljavljajo ne samo konvergenčna omrežja, temveč tudi konvergenčne komunikacije kot celota. Konvergenčne komunikacije izboljšujejo poslovne in privatne komunikacije in sicer s pomočjo združevanja različnih in do pred kratkim nezdružljivih sporočilnih sistemov in modelov (npr. govor, video, hipna sporočila, prisotnost …) s podatkovnimi aplikacijami in orodji. Pravzaprav je njihovo bistvo modularnost, ki omogoča postavitev omrežnih komponent in aplikacij na

širokem izboru različnih sistemov. Modularnost tako prinaša možnost izvedbe storitev v večih različnih konfiguracijah in lažjo implementacijo v večproizvajalsko okolje, kar posledično prinaša večjo fleksibilnost in cenovno učinkovitost.

Zaradi svoje odprte zasnove, ki določa osnovne funkcije potrebne za interoperabilnost, vendar še vedno dovolj prostora za implementacijo lastnih rešitev, se protokol SIP izvrstno ujema s konceptom konvergenčnih komunikacij, saj omogoča bogate komunikacije na različnih tipih medijev in med opremo različnih proizvajalcev. In ravno z vpeljavo protokola SIP v konvergenčna omrežja naredimo najpomembnejši korak v smeri konvergenčnih komunikacij (Slika 1), saj je to protokol, ki omogoča enostavno integracijo z ostalimi storitvami svetovnega spleta (elektronska in glasovna pošta, konferenčne avdio in video zveze …). Naš namen je takorekoč nadomestiti množico protokolov, ki so dandanes nujno potrebni za komunikacijo med posameznimi segmenti konvergenčnih omrežjih, s protokolom SIP.



Slika 1: Vpeljava protokola SIP v konvergenčno omrežje

Znanost in razvoj lahko spreminjata vse. Upam, da bo tudi to magistrsko delo prispevalo k temu in pomagalo pri kakršnihkoli odločitvah, ki jih ponujajo sodobni telekomunikacijski sistemi in omrežja.

3. Protokol SIP

Protokol SIP je signalizacijski oz. kontrolni protokol za vzpostavljanje, spreminjanje in zaključevanje multimedijskih sej z enim ali več udeleženci. Primeri sej so npr. internetna telefonija, multimedijska konferenca in druge podobne aplikacije, ki vključujejo avdio, video in podatke.

Začetek protokola sega v leto 1996, ko je bil le-ta razvit v sklopu akademskega projekta za nadzor razširjanja na več končnih točk (angl. *multicast media distribution*) kot eno izmed orodij, ki jih je uporabljalo hrbtenično omrežje z oddajanjem večim prejemnikom (MBONE – *Multicast Backbone*). Zasnovan je bil na preprostih, tekstovnih in razširljivih objektih, po vzoru protokola za prenos elektronske pošte (SMTP – *Simple Mail Transfer Protocol*). Ob povečanem zanimanju za telefonijo preko internetnega omrežja je organizacija IETF v marcu 1999 začetno delo vključila v standard RFC 2543 [RFC2543]. Nezdružljivost opreme različnih proizvajalcev je odpravil nov osnovni standard za SIP RFC 3261 [RFC3261], izdan leta 2002, ki je razširil prvotno priporočilo ter izboljšal področje razširljivosti in varnosti.

Pri delu znotraj IETF delovnih skupin, odgovornih za različna področja povezana s protokolom SIP, so aktivno sodelovali tudi večji proizvajalci komunikacijske opreme, kot so Cisco, Nokia, Microsoft in Avaya, ki so veliko pripomogli k uspešnemu razvoju tehnologije. Danes razvija različne SIP produkte vse več proizvajalcev, tako da je na to temo napisanih več kot dvajset priporočil in sto osnutkov [Cumming_03].

Glede na svoje lastnosti SIP postaja pomemben člen konvergenčnih komunikacij, kjer je poudarek na povečanju poslovno-operativnih sposobnosti končnih uporabnikov. Njegovo vlogo lahko primerjamo z vlogo protokola za prenos hiperteksta (HTTP – *HyperText Transfer Protocol*) v svetovnem spletu, saj uporabnikom omogoča transparentnost komunikacijske infrastrukture in omogoča dostop do različnih načinov komuniciranja. Z uporabo enoličnega identifikatorja virov (URI – *Unified Resource Identifier*) omogoča obravnavo zahteve za komunikacijo na enak način kot protokol HTTP, kar predstavlja naravno izbiro za uporabo pri komunikacijskih storitvah in korporacijskih aplikacijah.

Kot je razvidno iz imena protokola, je glavna naloga SIP-a vzpostavitev sej med uporabniki. Poleg tega opravlja tudi zaključevanje sej in spremembe parametrov sej. Vzpostavitev seje je tudi najtežji del, saj zahteva ugotavljanje trenutne lokacije klicanega uporabnika. Klicani uporabnik je lahko v določenem trenutku prisoten na eni izmed večih lokacij. Lahko ima SIP telefon (ali računalnik) doma in drug SIP telefon (ali računalnik) v službi. V tem primeru morata oba telefona (ali računalnika) naenkrat zvoniti. Uporabnik pa je lahko tudi mobilen, kar je bilo tudi upoštevano pri snovanju tega protokola.

Ko je klicani uporabnik lociran, lahko SIP opravi svojo naslednjo nalogo. Klicani uporabnik mora prejeti opis seje, h kateri ga vabi pobudnik seje. Za opis seje je uporabljen poseben protokol SDP, ki ga protokol SIP prenese do klicanega uporabnika.

Klicani uporabnik se potem odloči, ali bo povabilo sprejel, ali ne. Če klic sprejme, postane seja aktivna. Med njenim potekom lahko katerikoli uporabnik (kličoči ali klicani) spremeni njene parametre, tako da pošlje svojemu sogovorniku nov opis seje, ki ga ta lahko zopet sprejme ali zavrne.

3.1. Osnove protokola SIP

Protokol SIP originalno izhaja iz RFC 2543 [RFC2543]. Kasneje je bil ta standard posodobljen in izdan kot RFC 3261 [RFC3261], ki danes velja za osnovni standard protokola SIP. Poleg tega osnovnega standarda je bilo do danes objavljenih še veliko število podpornih standardov, ki opisujejo in dopolnjujejo protokol SIP in njegove različne interakcije [Tabela 1]. Spodnja tabela vsebuje večino teh standardov, vsi ostali pa so dostopni na naslovu http://www1.cs.columbia.edu/sip/drafts.html.

Standard	*Naslov*
RFC 3261	SIP:Session Initiation Protocol (obsoletes RFC2543)
RFC 3262	Reliability of Provisional Responses in SIP
RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method
RFC 4028	Session Timers in the Session Initiation Protocol (SIP)
RFC 3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)
RFC 3325	Private Extensions to SIP for Asserted Identity within Trusted Networks
RFC 3204	MIME media types for ISUP and QSIG Objects
RFC 3372	Session Initiation Protocol for Telephones (SIP-T): Context and Architectures

RFC 3398	ISUP to SIP Mapping
RFC 2976	The SIP INFO Method
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication
RFC 3428	SIP Extension for Instant Messaging
RFC 3515	The Session Initiation Protocol (SIP) Refer Method
RFC 3665	Session Initiation Protocol (SIP) Basic Call Flow Examples
RFC 3666	Session Initiation Protocol (SIP) PSTN Call Flows
RFC 3725	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol
RFC 2327	SDP: Session Description Protocol
RFC 3407	Session Description Protocol (SDP) Simple Capability Declaration
RFC 3551	RTP Profile for Audio and Video Conferences with Minimal Control
RFC 3555	MIME Type Registration of RTP Payload Formats
RFC 3824	Using E.164 numbers with the Session Initiation Protocol (SIP)
RFC 3840	Indicating User Agent Capabilities in SIP
RFC 3841	Caller Preferences for the Session Initiation Protocol (SIP)
RFC 3842	A Message Summary and Message Waiting Indication Event Package for SIP
RFC 3856	A Presence Event Package for the Session Initiation Protocol (SIP)
RFC 3857	A Watcher Information Event Template-Package for SIP
RFC 3891	The Session Initiation Protocol (SIP) "Replaces" Header
RFC 3892	The Session Initiation Protocol (SIP) Referred-By Mechanism
RFC 3966	The tel URI for Telephone Numbers
Q.1912.5	ITU Recommendation Q.1912.5: Interworking between SIP and BICC/ISUP

Tabela 1: Standardi, povezani s protokolom SIP

Protokol SIP opišemo kot protokol aplikacijskega sloja referenčnega modela za medsebojno povezovanje odprtih sistemov (OSI – *Open Systems Interconnection*), ki v prvi vrsti skrbi za vzpostavitev, spreminjanje in prekinitev komunikacijskih sej. SIP omogoča precej več kot samo vzpostavitev telefonskih klicev. Njegova razširljiva osnova omogoča tako pošiljanje hipnih sporočil preko tekstovnih kanalov, kot tudi mehanizem naročanja oz. objavljanja informacije o prisotnosti ali dostopnosti. Po vzoru modela HTTP, jedro protokola tvori izmenjava tekstovnih zahtev (angl. *request*) in odgovorov (angl. *response*), direktno med končnimi točkami (angl. *peer-to-peer*) [Hiti_05].

Sporočila SIP so sorodna zahtevam oz. odgovorom HTTP in se prenašajo preko protokolov transportne ravnine: uporabniški datagramski protokol (UDP – *User Datagram Protocol*), protokol za krmiljenje pretoka (TCP – *Transfer Control Protocol*) ali prenosni protokol z nadzorovanim pretokom (SCTP – *Stream Control Transfer Protocol*). Sporočila SIP v svoji glavi (angl. *header*) nosijo informacijo o posamezni komunikacijski seji (naslovnik, pošiljatelj …), v uporabniškem delu sporočila pa najpogosteje prenašajo informacijo SDP, potrebno za vzpostavitev medijskih kanalov

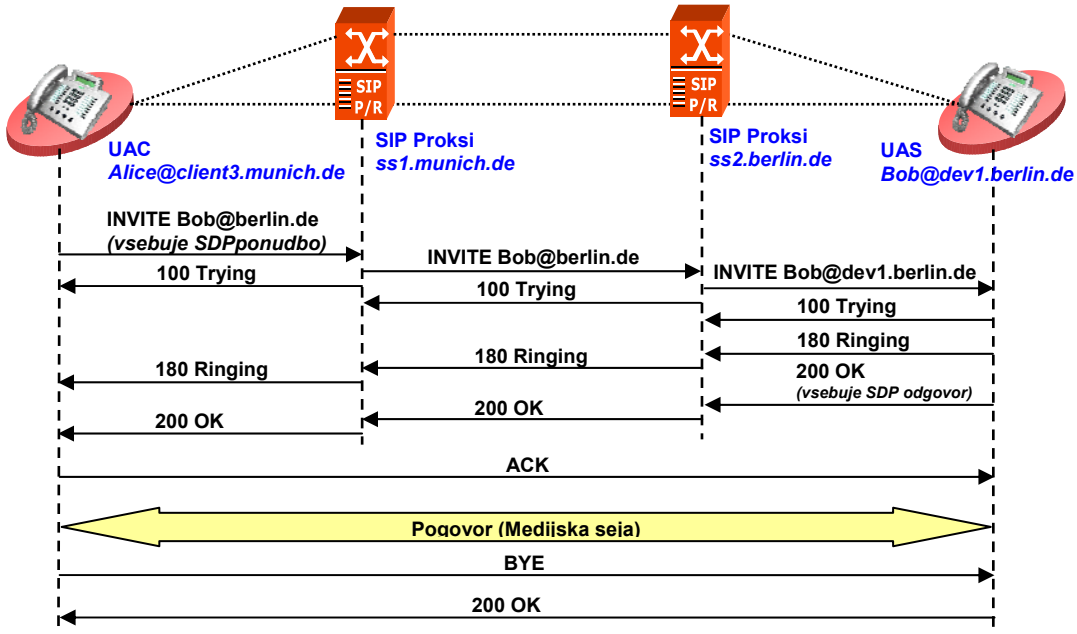
(tip medija, št. UDP vrat …). Tu pa se lahko prenaša tudi vsebina elektronskega sporočila, slika, ISDN uporabniški del (ISUP – *ISDN User Part*) …

Vzpostavitev signalizacijske seje lahko poteka preko različnih strežnikov SIP (proksi, preusmeritveni ali B2BUA – *Back to Back User Agent*) ali direktno, medtem ko se govorna povezava vzpostavi direktno med končnima točkama s pomočjo protokola za prenos v realnem času (RTP – *Real Time Protocol*).

3.1.1. Pregled delovanja

Najprej si poglejmo osnovno delovanje protokola SIP na preprostem primeru, kjer so prikazane njegove osnovne funkcije: lociranje končne točke, želja po vzpostavitvi komunikacije, pogajanje za osnovne parametre seje ter podiranje vzpostavljene zveze.

Spodnja slika [Slika 2] prikazuje osnovni potek sporočil SIP med dvema uporabnikoma. Prikazana sta tudi dva SIP proksi strežnika, ki pomagata pri sami vzpostavitvi seje. Zaradi tipične razvrstitve, ki je prikazana z geometrijsko obliko pikčastih črt, se na ta primer velikokrat nanašajo kot na SIP trapezoid.



Slika 2: Primer vzpostavitve SIP klica

Alice kliče Boba z uporabo njegove SIP identitete, imenovane SIP URI. V našem primeru je to Bob@berlin.de, kjer je berlin.de Bobova domena. SIP prav tako omogoča varen prenos z uporabo SIPS URI-ja. Klic, vzpostavljen na podlagi SIPS URI-ja, zagotavlja varen in kriptiran transport sporočil imenovan varnost transportnega sloja (TLS – *Transport Layer Security*).

SIP je osnovan na HTTP transakcijskem modelu zahteva/odgovor. Vsaka transakcija je sestavljena iz zahteve, ki vsebuje določeno metodo ali funkcijo ter vsaj enega odgovora. V našem primeru transakcijo začne uporabniški klient (UAC – *User Agent Client*) Alice, ko pošlje zahtevo INVITE za vzpostavitev komunikacijske seje, ki poleg naslovne informacije v uporabniškem delu sporočila vsebuje tudi informacijo (SDP) o vrsti ter načinu vzpostavitve medijskega kanala. Zahteva je naslovljena na Bobov SIP URI naslov.

Ker pa Alice ne pozna fizične lokacije Boba ali njegovega proksi strežnika, zahtevo INVITE naslovi na strežnik SIP v svoji domeni. Naslov tega strežnika mora biti predhodno ročno nastavljen ali pa se za to uporabi strežnik, ki skrbi za dinamično konfiguriranje gostiteljskih računalnikov (DHCP – *Dynamic Host Configuration Protocol*).

SIP proksi strežnik sprejme zahtevo INVITE, na katero najprej odgovori s 100 Trying, kar pomeni, da je bila zahteva sprejeta in v imenu pošiljatelja posredovana naprej. V primeru, da strežnik ne pozna naslova, kamor naj bi zahtevo preusmeril, lahko uporabi domenski strežnik (DNS – *Domain Name System*), ki na poizvedbo odgovori z IP naslovom.

Zahteva se nato preko prvega SIP proksi strežnika (ss1.munich.de) prenese do drugega SIP proksi strežnika (ss2.berlin.de), kjer se v lokacijski podatkovni bazi poišče IP naslov zahtevanega uporabnika. Nato se zahteva pošlje do končne entitete SIP, kjer uporabniški strežnik (UAS – *User Agent Server*) preveri zmožnost sprejetja klica.

Terminal prične zvoniti in izvornemu uporabniškemu agentu se preko istih dveh strežnikov SIP najprej pošlje informacijo o zvonjenju (180 Ringing), nato pa še informacijo (200 OK), da je klicani uporabnik Bob klic tudi sprejel. To sporočilo SIP vsebuje tudi informacijo o vrsti seje, ki jo je Bob zmožen vzpostaviti. Če Bob klica ne

bi želel sprejeti ali če bi bil zaseden, bi se namesto potrditve poslal odziv napake, zaradi katerega se seja ne bi vzpostavila.

Po vzpostavitvi seje se mora poslati potrditveno sporočilo ACK. Ker sedaj Alice in Bob poznata pravi naslov drug drugega, se to in tudi vsa naslednja sporočila lahko pošiljajo direktno med njima. Proksi strežnika se sedaj ne potrebujeta več.

V kolikor želi kateri od agentov spremeniti parametre vzpostavljene medijske seje, lahko med pogovorom pošlje novo zahtevo INVITE z novimi parametri, ki jih lahko agent na drugi strani sprejme (npr. 200 OK) ali pa zavrže, tako da odgovori z napako (npr. 488 Not Acceptable Here). Ne glede na odgovor nove zahteve, to ne vpliva na trenutno sejo, saj ta ostane nespremenjena, če pogajanje ni uspelo. V nasprotnem primeru se vzpostavi nova seja (npr. video klic).

Seja se konča tako, da ena izmed strani (v našem primeru Alice) pošlje sporočilo BYE, ki ga druga stran potrdi s sporočilom 200 OK. Sporočili se prav tako pošljeta direktno med uporabnikoma.

3.1.2. Entitete protokola SIP

V sklopu SIP priporočila je definiranih več entitet, ki skrbijo za uspešno vzpostavljanje komunikacijskih sej in izvajanje storitev. Kljub temu, da SIP zagovarja koncept porazdeljenosti, naštete entitete največkrat niso izvedene kot samostojne naprave. Tako običajno preusmeritveni (angl. *redirect server*) kot tudi SIP proksi (angl. *SIP proxy server*) strežnik vsebujeta registracijsko komponento (angl. *registrar server*), kar jima omogoča preusmerjanje zahtev na naslov, kjer se uporabnik trenutno nahaja.

1. Uporabniški agenti (UA – *User Agents*) so končne točke, ki med seboj komunicirajo preko protokola SIP. Končne točke so lahko odjemalci (UAC – *User Agent Client*), ki generirajo nove SIP zahteve ali strežniki (UAS – *User Agent Server*), ki odgovarjajo (potrjujejo, zavračajo in preusmerjajo) na prejete zahteve. V praksi so končne točke kombinacija obeh entitet, kajti vloga (odjemalec ali strežnik) končne točke ostaja nespremenjena samo znotraj ene transakcije. Lahko se spremeni pri vsaki nadaljnji transakciji, ki jih je znotraj enega dialoga lahko več.

2. SIP proksi strežnik (angl. *SIP proxy server*) je naprava, ki sodeluje pri izmenjavi signalizacijskih sporočil med končnimi točkami. Deluje kot strežnik in odjemalec z namenom pošiljanja zahtev namesto končnega uporabnika. Strežnik predvsem usmerja SIP zahteve proti končni destinaciji. Zahtevam lahko dodaja ali briše določene parametre (Via, Record-Route …), lahko jih zavrača, ne sme pa pozitivno odgovarjati na njih (potrjevanje je prepuščeno končnim točkam) oz. generirati novih zahtev. Njegova naloga je tudi izvajanje politike (angl. *policy*), ki jo zahteva določen operater. Nepoznanih sporočil SIP strežnik ne sme zavrniti oz. spremeniti, temveč jih mora poslati nespremenjene na ustrezno končno destinacijo. Ta način omogoča vpeljavo novih storitev le z nadgradnjo končnih točk.

3. Preusmeritveni strežnik (angl. *redirect server*) je strežniški uporabniški agent (UAS), ki na prejete zahteve odgovarja s 3xx odzivi. Zahteve za vzpostavitev seje preusmeri na ustrezno končno točko in ji doda pravilen naslov.

4. Registracijski strežnik (angl. *registrar server*) je prav tako strežniški uporabniški agent (UAS), ki obdeluje samo zahteve za registracijo končnih točk (REGISTER). Prejete informacije shrani v podatkovno bazo domene, ki jo nadzira. SIP končne točke dinamično pošiljajo zahteve za registracijo in na ta način prijavijo svojo lokacijo ali več lokacij, tako da strežnik SIP potem ve kam naj zahtevo za vzpostavitev seje preusmeri.

5. B2BUA (angl. *Back to Back User Agent*) je naprava, ki je zelo podobna SIP proksi strežniku, vendar s to pomembno razliko, da zahteve lahko tudi sam generira. Prav zaradi tega lahko zagotavlja vpeljavo nekaterih novih storitev, ki potrebujejo za delovanje centralen strežnik. Tak primer so različne uporabniške storitve, ki izhajajo iz sveta časovnega multipleksa (TDM – *Time Division Multiplex*). Lahko pa so to tudi povsem nove storitve, kot sta enkripcija poslanih sporočil in avtentikacija posameznih udeležencev.

3.1.3. Sporočila protokola SIP

SIP je tekstovno orientiran protokol, ki uporablja znakovni nabor UTF-8 (ref. RFC 2279). Kot smo že povedali, v protokolu SIP obstajata dve vrsti sporočil (angl. *messages*). Odjemalci generirajo ***zahteve*** (angl. *requests*), strežniki pa odgovarjajo z ***odzivi*** (angl. *responses*). Vsako sporočilo (zahteva ali odziv) ima naslednjo obliko:

SPOROČILO = ZAČETNA VRSTICA
ENA ALI VEČ GLAV SPOROČILA
CLRF (prazna vrstica)
UPORABNIŠKI DEL SPOROČILA

Iz začetne vrstice lahko razberemo ali gre za zahtevo ali odziv. Sledi eno ali več glav sporočila. Zadnji glavi sledi prazna vrstica. Uporabniški del sporočila je opcijski in npr. vsebuje opis seje po specifikaciji SDP. Primer sporočila SIP je podan na spodnji sliki [Slika 3]. Gre za zahtevo INVITE po vzpostavitvi seje.

```
INVITE sip:+49671000101@218.1.98.116;user=phone SIP/2.0
Via: SIP/2.0/UDP 172.18.84.30:5060;branch=z9hG4bK05246976440000000001.
From: <sip:+492002059@172.18.84.30;user=phone>;tag=3e5f33cf-00c5-ac12541e
To: <sip:+49671000101@218.1.98.116;user=phone>
Call-ID: 3E5F33CF-00000001@h13pm-03
CSeq: 1 INVITE
Accept: application/SDP, application/ISUP, multipart/mixed, application/vnd.siemens.key-event
Contact: <sip:+492002059@172.18.84.30;user=phone>
MIME-Version: 1.0
Supported: timer
Supported: 100rel
Max-Forwards: 70
Session-Expires: 1800
Allow: ACK, INFO, BYE, CANCEL, INVITE, OPTIONS, NOTIFY, PRACK
Content-Type: application/SDP
Content-Length: 267
```

Zahteva INVITE s pripadajočimi glavami

```
v=0
o=hiQ9200/CN0 156762230 156762230 IN IP4 172.18.84.30
s=Phone Call via hiQ9200 SIPCA
c=IN IP4 172.18.61.50
t=0 0
m=audio 5212 RTP/AVP 8 2
a=rtpmap:8 PCMA/8000
a=rtpmap:2 G726-32/8000
```

Uporabniški del sporočila SIP (npr. seja SDP)

Slika 3: Primer sporočila SIP za vzpostavitev seje

3.1.3.1. Zahteve

Začetna vrstica zahteve je sestavljena po naslednjem pravilu:

ZAČETNA VRSTICA ZAHTEVE = OZNAKA METODE SP URI ZAHTEVE SP VERZIJA PROTOKOLA SIP CRLF

Začetna vrstica se torej začne z oznako zahteve ali metode (angl. *method*) in predstavlja eno izmed vseh možnih vrst zahtev. SP (angl. *space*) pomeni presledek. URI zahteve (angl. r*equest-URI*) je naslov uporabnika, na katerega je zahteva naslovljena. Za razliko od glave "To", lahko proksi strežniki to vrednost spremenijo. Trenutna verzija protokola je SIP/2.0.

Osnovni nabor metod definiranih v SIP priporočilu je sledeč:

- ***INVITE*** – Ta metoda nakazuje, da je klicani uporabnik povabljen k seji. Uporabniški del sporočila vsebuje opis seje. Kličoči uporabnik v povabilu navede tudi vrsto seje (avdio ali video ali oboje), ki jo želi vzpostaviti ter vse potrebne parametre (video in avdio kodek, video resolucija …). Uspešen odziv na to zahtevo (odziv 200 OK) vsebuje vrsto seje in pripadajoče atribute, ki jih lahko klicani uporabnik sprejme. Na tak način uporabniki pri vzpostavitvi seje prepoznajo zmožnosti drug drugega.
- ***ACK*** – Ta metoda je uporabljena v povezavi z metodo INVITE. Ko odjemalec prejme končni odziv na zahtevo INVITE, to potrdi še z zahtevo ACK. Končni odzivi so vsi odzivi, katerih kode se ne začnejo z 1xx. V uporabniškem delu zahteve ACK lahko odjemalec poda še dokončen opis seje, ki naj jo uporabi klicani uporabnik. Če tega opisa ni, se uporabi opis seje, ki je bil podan s predhodno zahtevo INVITE.
- ***OPTIONS*** – S pomočjo te metode se zbira informacije o zmožnostih uporabniških agentov in omrežnih strežnikov.
- ***BYE*** – Kličoči ali klicani uporabniški agenti lahko uporabijo to metodo kadar želijo končati klic.
- ***CANCEL*** – Ta zahteva se uporablja za preklic predhodne zahteve, na katero še ni bilo končnega odziva.
- ***REGISTER*** – Ta zahteva omogoča odjemalcu, da obvesti proksi ali preusmeritveni strežnik o svojem naslovu (naslovih), kjer je dosegljiv.

Poleg osnovnih metod RFC priporočila določajo še naslednje metode:

- ***PRACK*** (angl. *Provisional Response ACK*) – se uporablja za začasno potrjevanje metode INVITE na podlagi sprejetega odziva 1xx (npr. če želimo prenašati podatke po govornem kanalu pred dejansko vzpostavitvijo zveze (preden klicani uporabnik pošlje 200 OK),
- ***UPDATE*** – se uporablja za posodobitev parametrov seje,
- ***REFER*** – se uporablja za prenos kontaktnih podatkov tretje osebe (npr. pri predaji klica),
- ***INFO*** – se uporablja za prenos informacij med klicem,
- ***NOTIFY*** – se uporablja za prenos informacij o spremembi stanj,
- ***MESSAGE*** – se uporablja za prenos hipnih sporočil,
- ***SUBSCRIBE*** – se uporablja za pridobivanje informacij o trenutnem stanju oddaljenih vozlišč (npr. pri uporabi različnih storitev, na katere je posamezen uporabnik naročen – prevzem klica znotraj skupine).

3.1.3.2. Odzivi

Ko strežnik sprejme zahtevo, nanjo odgovori z odzivom, ki opisuje (ne)uspešnost klica oz. status strežnika. Začetna vrstica sporočila ima naslednjo obliko:

ZAČETNA VRSTICA ODZIVA = VERZIJO PROTOKOLA SP KODA STATUSA SP BESEDNI OPIS STATUSA CRLF

Verzija protokola je prav tako kot pri zahtevi enaka SIP/2.0. Koda statusa (angl. *status code*) je trimestno število in določa vrsto odziva. Odzivi, ki se začnejo z 1xx, so ***začasni*** (angl. *provisional response*), vsi ostali odzivi pa so ***končni*** (angl. *final response*). Začasni odzivi opisujejo le napredek klica in ne predstavljajo končnega odgovora na zahtevo.

Tudi odzivi strežnika SIP na zgoraj navedene metode so podobni tistim pri protokolu HTTP in jih lahko razdelimo v naslednje skupine:

- ***1xx*** – obvestila,

Koda statusa	Besedni opis
100	Trying
180	Ringing
181	Call Is Being Forwarded
182	Queued
183	Session in Progress

Tabela 2: Odzivi – obvestila

- ***2xx*** – potrditve,

Koda statusa	Besedni opis
200	Ok
202	Accepted

Tabela 3: Odzivi – potrditve

- ***3xx*** – preusmeritve,

Koda statusa	Besedni opis
300	Multiple Choices
301	Moved Permanently
302	Moved Temporarily
303	See Other
305	Use Proxy
380	Alternative Service

Tabela 4: Odzivi – preusmeritve

- ***4xx*** – napake na strani odjemalca,

Koda statusa	Besedni opis
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
413	Request Entity Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Unsupported URI Scheme
420	Bad Extension
421	Extension Required
422	Session Interval Too Small

423	Interval Too Brief
480	Temporarily Unavailable
481	Call/Transaction Does Not Exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete
485	Ambiguous
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
489	Bad Event
491	Request Pending
493	Undecipherable

Tabela 5: Odzivi – napake na strani odjemalca

- ***5xx*** – napake na strani strežnika,

Koda statusa	*Besedni opis*
500	Server Internal Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Server Time-out
505	Version Not Supported
513	Message Too Large

Tabela 6: Odzivi – napake na strani strežnika

- ***6xx*** – globalne napake.

Koda statusa	*Besedni opis*
600	Busy Everywhere
603	Decline
604	Does Not Exist Anywhere
606	Not Acceptable

Tabela 7: Odzivi – globalne napake

3.1.3.3. Glave sporočil

Glave so v sporočilih uporabljene za opis kličočega uporabnika, opis klicanega uporabnika, tip in dolžino vsebovanega sporočila in podobno. Vse informacije o glavah, ki jih podpira protokol SIP, ter njihovo povezanost s posameznimi zahtevami, so razvidne iz spodnje tabele [Tabela 8].

Sintaksa SIP glav naj bi upoštevala naslednje pravilo:

GLAVA = IME GLAVE : SP VREDNOST *(;IME PARAMETRA = VREDNOST)

Tako lahko vsaka glava poleg svoje osnovne vrednosti vsebuje še več dodatnih parametrov, ki še bolj natančno opisujejo samo glavo. Ti parametri so med sabo ločeni s podpičji.

Ime glave	*Uporaba*	*Proksi*	*ACK*	*BYE*	*CAN*	*INV*	*OPT*	*REG*
Accept	R		-	o	-	o	m*	o
Accept	2xx		-	-	-	o	m*	o
Accept	415		-	c	-	c	c	c
Accept-Encoding	R		-	o	-	o	o	o
Accept-Encoding	2xx		-	-	-	o	m*	o
Accept-Encoding	415		-	c	-	c	c	c
Accept-Language	R		-	o	-	o	o	o
Accept-Language	2xx		-	-	-	o	m*	o
Accept-Language	415		-	c	-	c	c	c
Alert-Info	R	ar	-	-	-	o	-	-
Alert-Info	180	ar	-	-	-	o	-	-
Allow	R		-	o	-	o	o	o
Allow	2xx		-	o	-	m*	m*	o
Allow	r		-	o	-	o	o	o
Allow	405		-	m	-	m	m	m
Authentication-Info	2xx		-	o	-	o	o	o
Authorization	R		o	o	o	o	o	o
Call-ID	c	r	m	m	m	m	m	m
Call-Info		ar	-	-	-	o	o	o
Contact	R		o	-	-	m	o	o
Contact	1xx		-	-	-	o	-	-
Contact	2xx		-	-	-	m	o	o
Contact	3xx	d	-	o	-	o	o	o
Contact	485		-	o	-	o	o	o
Content-Disposition			o	o	-	o	o	o
Content-Encoding			o	o	-	o	o	o
Content-Language			o	o	-	o	o	o
Content-Length		ar	t	t	t	t	t	t
Content-Type			*	*	-	*	*	*
CSeq	c	r	m	m	m	m	m	m
Date		a	o	o	o	o	o	o
Error-Info	300-699	a	-	o	o	o	o	o
Expires			-	-	-	o	-	o
From	c	r	m	m	m	m	m	m
In-Reply-To	R		-	-	-	o	-	-
Max-Forwards	R	amr	m	m	m	m	m	m
Min-Expires	423		-	-	-	-	-	m
Min-SE	R	amr	-	-	-	o	-	-
Min-SE	422		-	-	-	m	-	-
MIME-Version			o	o	-	o	o	o
Organization		ar	-	-	-	o	o	o
Priority	R	ar	-	-	-	o	-	-
Proxy-Authenticate	407	ar	-	m	-	m	m	m
Proxy-Authenticate	401	ar	-	o	o	o	o	o
Proxy-Authorization	R	dr	o	o	-	o	o	o
Proxy-Require	R	ar	-	o	-	o	o	o
Record-Route	R	ar	o	o	o	o	o	-
Record-Route	2xx,18x	mr	-	o	o	o	o	-
Reply-To			-	-	-	o	-	-
Require		ar	-	c	-	c	c	c

Ime glave	*Uporaba*	*Proksi*	*ACK*	*BYE*	*CAN*	*INV*	*OPT*	*REG*
Retry-After	404,413		-	o	o	o	o	o
	480,486		-	o	o	o	o	o
	500,503		-	o	o	o	o	o
	600,603		-	o	o	o	o	o
Route	R	adr	c	c	c	c	c	c
Server	r		-	o	o	o	o	o
Session-Expires	R	amr	-	-	-	o	-	-
Session-Expires	2xx	ar	--	-	-	o	-	-
Subject	R		-	-	-	o	-	-
Supported	R		-	o	o	m*	o	o
Supported	2xx		-	o	o	m*	m*	o
Timestamp			o	o	o	o	o	o
To	c(1)	r	m	m	m	m	m	m
Unsupported	420		-	m	-	m	m	m
User-Agent			o	o	o	o	o	o
Via	R	amr	m	m	m	m	m	m
Via	rc	dr	m	m	m	m	m	m
Warning	r		-	o	o	o	o	o
WWW-Authenticate	401	ar	-	m	-	m	m	m
WWW-Authenticate	407	ar	-	o	-	o	o	o

Tabela 8: Pregled glav v protokolu SIP

Stolpec ***UPORABA*** vsebuje informacijo o tem, kje se določena glava lahko uporablja. Možne vrednosti so sledeče:

- ***R***: glava se lahko nahaja samo v zahtevah;
- ***r***: glava se lahko nahaja samo v odzivih;
- ***2xx,4xx, itd.***: numerična vrednost ali niz vrednosti se nanaša na odziv oz. odzive, kjer se glava lahko uporablja;
- ***c***: glava se kopira iz zahtev v odzive;
- če polje ne vsebuje nobene vrednosti to pomeni, da je glava lahko prisotna tako v zahtevah kot tudi v odzivih.

Stolpec ***PROKSI*** opisuje operacije, ki jih proksi strežnik lahko izvrši nad določeno glavo:

- ***a***: proksi strežnik lahko glavo doda ali poveže;
- ***m***: proksi strežnik lahko spremeni vrednost glave;
- ***d***: proksi strežnik lahko zbriše vrednost glave;
- ***r***: proksi strežnik mora biti sposoben prebrati vrednost glave, zato to polje ne sme biti kriptirano.

Naslednjih šest stolpcev ponazarja prisotnost določene glave v zahtevi ali odzivu na zahtevo:

- ***c***: pogojno, zahteva za glavo je odvisna od celotnega sporočila SIP;
- ***m***: glava je obvezna;
- ***m****: glava naj bi se poslala, vendar mora biti klient ali strežnik pripravljen sprejeti sporočilo tudi brez nje;
- ***o***: glava ni obvezna;
- ***t***: glava naj bi se poslala, vendar mora biti klient ali strežnik pripravljen sprejeti sporočilo tudi brez nje. V primeru uporabe povezavno orientiranega protokola, kot je TCP, se glava mora poslati;
- *******: glava je zahtevana, če telo vsebovanega sporočila ni prazno;
- **-**: glava se ne uporablja.

Sedaj pa si natančneje poglejmo pomen nekaterih pomembnejših oz. največkrat uporabljenih glav.

- ***Glava Call-ID*** predstavlja edinstven identifikator skupine zaporednih sporočil. Njena vrednost mora biti ista za vse zahteve in odzive znotraj istega dialoga. Njeno vrednost določi UAC in mora biti edinstvena. To pomeni, da mora imeti vsak uporabniški agent vgrajen način, s katerim zagotovi, da ustvarjenega identifikatorja klica ne bo ustvaril noben drug agent. Z uporabo naključnih kriptografskih identifikatorjev povečamo varnost z vidika kraje seje (angl. *session hijacking*) ter zmanjšamo verjetnost nenamernih kolizij.

  Primer:

  Call-ID: 0881020211-8237898029811211-11-75168013

- ***Glava CSeq*** predstavlja mehanizem za identifikacijo in razvrščanje posameznih transakcij znotraj dialoga. Sestavljena je iz zaporedne številke in metode. Ujemati se mora s poslano zahtevo. Njena vrednost je za vse zahteve, razen zahteve REGISTER, izven dialoga popolnoma poljubna. Lahko je izražena kot 32-bitno nepredznačeno celo število in mora biti manjša od 2^{31}. Znotraj dialoga pa se mora njena vrednost povečevati z vsako nadaljnjo transakcijo.

Primer:

CSeq: 16 INVITE

- ***Glava Via*** označuje protokol, njegovo verzijo in transportni mehanizem, ki ga transakcija uporablja. Poleg tega vsebuje tudi lokacijo oz. zaporedni spisek lokacij, preko katerih naj bi se odziv tudi poslal. Temu pa mora biti dodan še parameter imenovan branch, katerega vrednost mora biti glede na kraj in čas edinstvena. Izjemi tega pravila sta zahtevi CANCEL in ACK, ki se pošljeta na katerikoli odziv, razen na odzive 2xx. Zahteva CANCEL ima v tem primeru enako vrednost kot predhodna zahteva, ki jo preklicuje. Zahteva ACK pa isto vrednost kot parameter branch znotraj zahteve INVITE, ki jo potrjuje. Skladno s priporočilom [RFC3261] se mora njena vrednost začeti z "**z9hG4bK**".

  Primer:

  Via: SIP/2.0/UDP 172.18.1.102:5060;branch=z9hG4bKSNCLLC1121189447

- ***Glava Contact*** vsebuje SIP ali SIPS URI, ki se lahko uporabi kot kontaktni naslov za vse nadaljnje zahteve uporabniških agentov. Glava mora biti vedno prisotna v vseh zahtevah, katerih posledica je lahko vzpostavitev dialoga.

  Primer:

  Contact: <sip:0102230208@172.18.1.102:5060;transport=udp>

- ***Glava To/From*** predstavlja predvsem logičen naslov prejemnika/pošiljatelja zahteve, ki je ali pa tudi ni končni prejemnik. Načeloma naj bi vsebovala SIP ali SIPS URI, vendar lahko uporablja tudi druge URI sheme (npr. URL; RFC 2806). Njena vrednost se lahko uporabi za prikaz številke. Poleg tega vsebuje še dodatno označbo, parameter imenovan tag, ki se uporablja za identifikacijo dialoga.

  Primer:

  To: <sip:0942016@172.18.1.102 ;user=phone>;tag=1119872580-2723301120144910-11
  From: "0102230208" <sip:0102230208@172.18.1.102>;
  tag=siemens-sx551-1.33a-929444224-feab70ef-939796913

- ***Glavo Record-Route*** v zahteve prvotno vstavljajo proksi strežniki. Njen namen je prisiliti vse nadaljnje zahteve znotraj enega dialoga, da uporabljajo specifično oz. natančno določeno pot preko enega ali več proksi strežnikov. Uporablja se lahko z namenom centraliziranega obračunavanja stroškov.

  Primer:

  Record-Route: <sip: ss2.berlin.de;lr>

3.1.3.4. Enolični identifikator virov SIP in SIPS

Enolični identifikator virov (URI – *Uniform Resource Indicator*) SIP in SIPS enolično označujeta komunikacijski vir. Gre za enotno označevanje SIP komunikacijskih virov. Prav tako kot URI, se SIP ali SIPS URI lahko uporablja na spletnih straneh, v elektronskih sporočilih, tiskani literaturi itd. Vsebuje namreč dovolj informacij, da se lahko vzpostavi in vzdržuje komunikacijska seja s tem virom, ki je lahko:

- uporabnik spletnih storitev,
- večlinijski IP telefon,
- poštni predal sporočilnega sistema,
- PSTN številka,
- skupina (npr. servis ali prodaja) v neki organizaciji.

SIPS URI pa zagotavlja, da se bo povezava do komunikacijskega vira vzpostavila na varen način. To pomeni, da se bo za povezavo med UA odjemalcem in domeno, ki je lastnica URI-ja, uporabil varen transportni način imenovan TLS. Od tam naprej se bo za komunikacijo uporabil varnostni mehanizem, ki je odvisen od politike posamezne domene.

SIP in SIPS shema sledita priporočilu RFC 2396 [RFC2396]. Sama sintaksa je naslednja:

sip:uporabnik:geslo@odjemalec:vrata;uri-parametri?glave

Za SIPS je namesto "sip:" uporabljen "sips:" Primeri naslovov so lahko:

- sip:logonder@iskratel.si
- sip:+49102230022@176.7.6.1:5060;tranpsort=tcp;user=phone
- sips:logonder@iskratel.si?subject=project%20x&priority=urgent

3.1.3.5. Označbe

Parameter za označbo (*tag*) se uporablja v glavah To in From. Njegov namen je pomoč pri identifikaciji posameznega dialoga, ki je natančno določen z identifikacijo klica (glava Call-ID) ter označbo v glavi To in From.

Označbe morajo biti edinstvene v globalnem pomenu in kriptografsko naključne z vsaj 32 bitno naključnostjo.

Poleg ravnokar omenjenih obveznih označb se v SIP-u uporabljajo tudi neobvezne označbe. Te edinstveno označujejo neobvezne podaljške v SIP-u. Uporabljajo pa se v glavah Require, Proxy-Require, Supported in Unsupported kot neobvezen parameter.

3.1.4. Osnovni termini protokola SIP

Za lažje razumevanje si najprej razjasnimo nekaj osnovnih pojmov protokola SIP, kot so dialog, transakcija in seja. Poglejmo, kako so ti pojmi med seboj prepleteni in kakšna je pravzaprav razlika med njimi.

3.1.4.1. Dialog

Dialog je razmerje točka – točka med dvema uporabniškima agentoma, ki traja nekaj časa. Olajšuje tudi razvrščanje sporočil med dvema agentoma in zagotavlja ustrezno usmerjanje zahtev med njima. Pravzaprav nam predstavlja neko zvezo znotraj katere obdelujemo sporočila SIP [Slika 4].

Vsak dialog je natančno določen z identifikacijo klica (polje Call-ID), lokalno (angl. *local tag*) in oddaljeno označbo (angl. *remote tag*). Za prenos označb sta uporabljeni

glavi To in From, ki pa se spreminjata glede na dejstvo, kateri agent pošlje zahtevo oz. glede na to ali je uporabniški agent klient ali strežnik. Prav zaradi tega je identifikacija dialoga za vsakega uporabniškega agenta drugačna:

- ***UAC***: Lokalna označba = označba v glavi FROM sporočila INVITE
  Oddaljena označba = označba v glavi TO sporočila INVITE

- ***UAS***: Lokalna označba = označba v glavi TO sporočila INVITE
  Oddaljena označba = označba v glavi FROM sporočila INVITE

Vsak dialog mora vsebovati vse potrebne informacije o samem stanju, zato da se prenos sporočil znotraj dialoga nadaljuje. Te informacije so naslednje:

- identifikacija dialoga,
- lokalna/oddaljena sekvenčna številka,
- lokalni/oddaljeni URI,
- oddaljeni cilj in
- pot, po kateri se sporočila prenašajo (glava oz. glave Record-Route, ki določajo celotno pot sporočila oz. vse strežnike preko katerih mora sporočilo potovati).

Dialog se vzpostavi samo na podlagi uspešnega odziva na določene zahteve. V primeru zahteve INVITE se bo dialog vzpostavil samo, če bo odziv 2xx ali 101 – 199, in če polje TO znotraj odziva vsebuje potrebno označbo (parameter tag). Dialog vzpostavljen na podlagi začasnega odziva (1xx) se imenuje začetni dialog (angl. *early dialog*). Njegov status se spremeni z začetnega v potrjenega (angl. *confirmed*) na podlagi 2xx odziva. Za katerikoli drugi odziv ali če odziva sploh ni, se tak dialog zaključi. Vsak uspešno vzpostavljeni dialog se zaključi v trenutku, ko katerikoli agent pošlje zahtevo BYE.

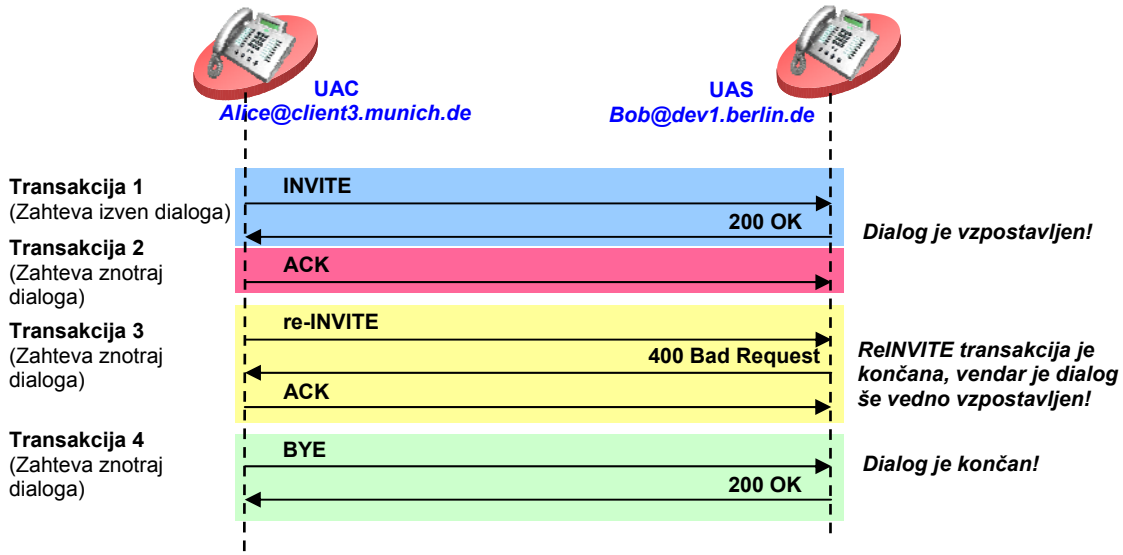
V primeru, da uporabniški agent prejme več 2xx odzivov od različnih agentov, za vsak odziv vzpostavi svoj dialog. Vsi ustvarjeni dialogi pa so del istega klica.

3.1.4.2. Transakcija

SIP je transakcijski protokol, kar pomeni, da interakcijo med dvema uporabniškima agentoma sestavlja izmenjava zaporednih ter med seboj neodvisnih sporočil. Sama SIP transakcija je tako sestavljena iz posamezne zahteve in vseh odzivov na to zahtevo. Ti odzivi lahko vsebujejo enega ali več začasnih odzivov in enega ali več končnih odzivov. V primeru transakcije, kjer je prvotna zahteva sporočilo INVITE, ta prav tako vključuje zahtevo ACK, vendar samo v primeru, da ne gre za 2xx odziv. Če pa je odziv na zahtevo iz razreda 2xx, potrditev ACK ne šteje kot del iste transakcije.

Razlog za to delitev izvira iz dejstva, da je pravilen in zanesljiv prenos vseh odzivov 200 (OK) na originalno zahtevo INVITE izrednega pomena. Da se odziv 200 (OK) res pravilno prenese od UAS do UAC, poskrbita oba uporabniška agenta. Naloga UAC-ja je potrjevanje sprejema s samostojno zahtevo ACK. Naloga UAS-a pa, da ponovi prenos odziva 200 (OK), če je to potrebno. Ker zahtevo ACK pošilja samo UAC, je razumljivo smatrana za svojo transakcijo.

Kako sta med seboj povezana dialog in transakcija je lepo razvidno tudi iz spodnje slike [Slika 4].



Slika 4: Razmerje med dialogom in transakcijo

3.1.4.3. Seja

Termin seja se nanaša na podatkovni kanal ali kanale, ki se vzpostavijo med uporabniškimi agenti. Po teh kanalih se potem lahko prenaša različne informacije, kot je avdio signal, video slika, igre itd. Multimedijska seja je izraz za več pošiljateljev, prejemnikov in podatkovnih tokov med njimi. Primer multimedijske seje je multimedijska konferenca [RFC2327]. V okviru protokola SIP je za opis sej uporabljen protokol SDP.

Seja med dvema uporabniškima entitetama se vzpostavi vzporedno z dialogom. To pomeni, da se vzpostavi samo na podlagi uspešnega odziva (npr. potrditve 200 OK) na poslano zahtevo INVITE. Seja pa se lahko vzpostavi že v času začetnega dialoga. Pogoj za vzpostavitev je namreč uspešna izmenjava opisa seje. Prav tako kot dialog, se tudi vsaka uspešno vzpostavljena seja zaključi v trenutku, ko katerikoli agent pošlje zahtevo BYE.

Seja je lahko sestavljena iz ene ali več RTP sej. To pomeni, da če uporabniški agent prejme več 2xx odzivov od različnih agentov, za vsak posamezen odziv vzpostavi svojo RTP sejo. Vse ustvarjene RTP seje pa so del ene seje.

3.1.5. Protokol SDP

SIP seja se lahko vzpostavi samo v primeru uspešne izmenjave njenega opisa. Za izmenjavo opisov seje protokol SIP uporablja model ponudba – odgovor (angl. *offer – answer*) [RFC3264]. Eden izmed uporabniških agentov najprej pošlje ponudbo, ki lahko vključuje več medijskih tokov (angl. *media stream*). Drugi agent mu vrne odgovor, ki mora vsebovati točno toliko medijskih tokov kot ponudba. Lahko pa ponudbo tudi zavrne. Uporabniški agent ima tudi možnost, da kadarkoli pošlje drugemu novo ponudbo, ki lahko spremeni trenutno sejo.

Za opis seje je tako uporabljen protokol za opis seje (SDP – *Session Description Protocol*, [RFC2327]), ki je že v osnovi namenjen prenosu informacij o medijskih tokovih v multimedijskih sejah. Prvotno je bil namenjen za uporabo v internetu, vendar je vseeno dovolj splošen, da se lahko uporablja tudi v drugačnih omrežjih in okoljih (npr. SIP).

3.1.5.1. Struktura protokola SDP

Naloga protokola SDP je komunikacija z namenom vzdrževanja trenutno aktivnih sej. Poleg tega mora prenašati ustrezne informacije, tako da omogoča priključevanje in udeležbo novih uporabnikov v seji. Struktura SDP opisa seje mora zato vsebovati:

- ime seje in njen namen;
- čas, ko je seja aktivna;
- medije, ki so vključeni v sejo;
- informacije, ki so potrebne za sprejem teh medijev (naslovi, številke vrat, oblika podatkov …).

Poleg naštetega so v opisu lahko podane tudi informacije o pasovni širini, ki naj bo uporabljena za sejo in kontaktne informacije o osebi, ki je odgovorna za sejo.

Za opis medijev protokol SDP vsebuje:

- tipe medijev (video, avdio itd.),
- transportni protokol (RTP/UDP/IP, H320 itd.),
- format medija (H.261 video, MPEG video, G729 avdio itd.),
- oddaljeni naslov in vrata kamor naj se mediji pošiljajo.

Protokol SDP se lahko uporablja za prenos informacij o javni in prav tako privatni seji. V primeru privatne seje, ki je seveda kriptirana, protokol SDP poskrbi za prenos potrebnih enkripcijskih ključev za dekodiranje vsakega posameznega medija. Poleg tega mora vsebovati tudi dovolj informacij, da se lahko natančno določi, kateri medij pripada kateri enkripcijski shemi.

Opis seje po specifikaciji SDP je sestavljen iz več vrstic v obliki ***<tip>=<vrednost>***. Polje <tip> je vedno sestavljeno iz enega znaka. Polje <vrednost> pa je vrstica besedila, katere struktura je odvisna od polja <tip>.

Zgradbo opisa seje prikazuje tabela [Tabela 9]. Vrstni red vrstic je točno določen. Opcijske vrstice so označene z zvezdico.

<tip>		<vrednost>
v		Verzija protokola SDP
o		Vsebuje ime pobudnika seje, unikatno številko seje, zaporedno številko opisa, tip omrežja, tip omrežnega naslova in naslov
s		Ime seje
i	*	Informacije o seji
u	*	URI, kjer so dostopne dodatne informacije o seji
e	*	Elektronski naslov osebe, ki je odgovorna za sejo
p	*	Telefonska številka osebe, ki je odgovorna za sejo
c	*	Vsebuje tip omrežja, tip naslova in naslov za določeno povezavo (če te vrstice ni, mora biti prisotna v vsakem opisu podatkov – glej spodnjo tabelo)
b	*	Informacije o pasovni širini
		EDEN ALI VEČ OPISOV ČASOVNIH PARAMETROV (glej spodnjo tabelo)
z	*	Za nastavitve časovnih con
k	*	Šifrirni ključ
a	*	Atributi seje
	*	OPISI PODATKOV (glej spodnjo tabelo)

Tabela 9: Vrstni red vrstic v opisu seje

<tip>		<vrednost>
t		Vsebuje informacije o začetku in koncu seje
r	*	Vsebuje periodo ponavljanja sej

Tabela 10: Vrstice za opis časovnih parametrov

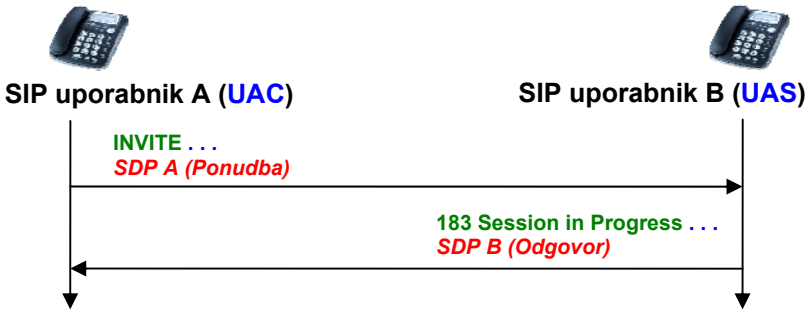
<tip>		<vrednost>
m	*	Določa tip podatkov, številko ponornih vrat, vrsto transportnega protokola in obliko podatkov
i	*	Informacije o določenem tipu podatkov
c	*	Informacije o povezavi za določen tip podatkov
b	*	Informacije o pasovni širini
k	*	Šifrirni ključ
a	*	Razni atributi

Tabela 11: Vrstice za opis oblike podatkov v bodoči seji

3.1.5.2. Načini izmenjave opisa SDP

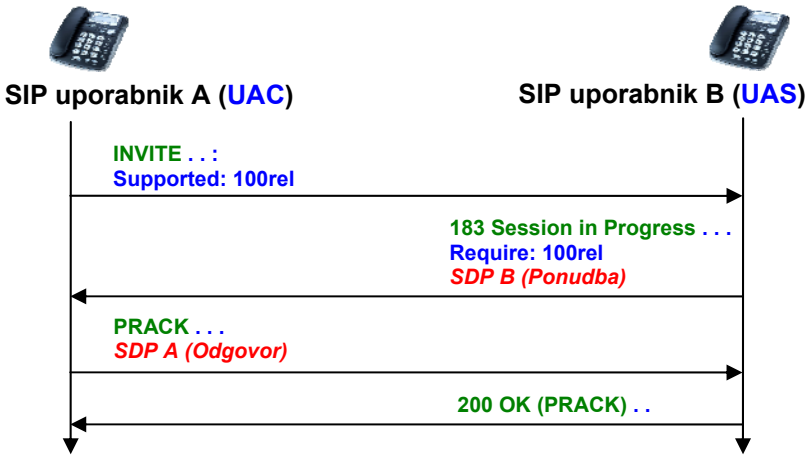
Za uspešno zaključen cikel ponudba – odgovor v okviru protokola SIP obstaja več možnosti.

1. Ponudba SDP se pošlje v zahtevi INVITE, odgovor pa v odzivu 18x (npr. Ringing) in/ali potrditvi 200 (npr. OK) na to zahtevo [Slika 5].
2. Zahteva INVITE ne vsebuje ponudbe. Vsebuje jo odziv 200 OK, odgovor pa je vsebovan v zahtevi ACK.



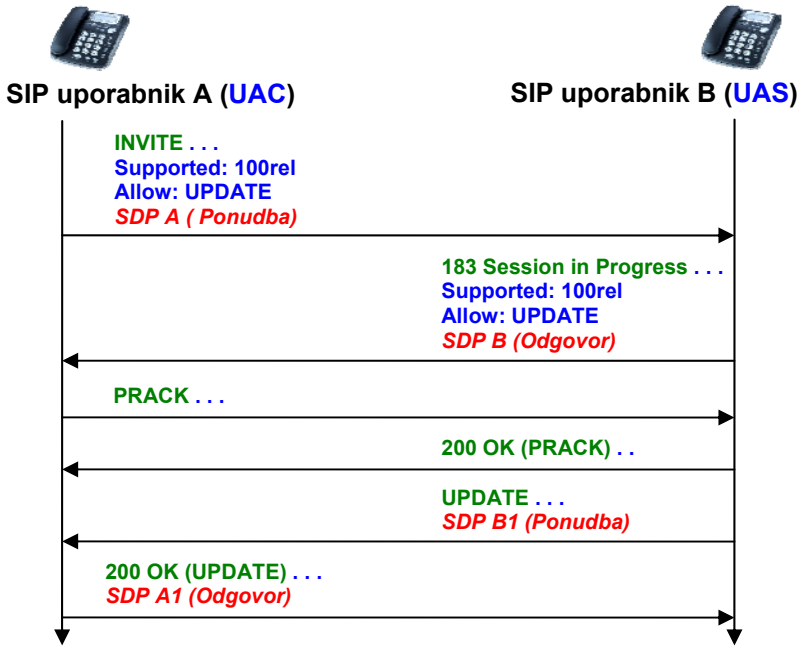
Slika 5: Osnovna izmenjava opisa SDP

3. Ponudba SDP je vsebovana v odzivu 18x na zahtevo INVITE, odgovor pa v naslednji zahtevi PRACK. Celoten potek je lepo razviden iz spodnje slike [Slika 6]. Uporabnik A najprej pošlje zahtevo INVITE, iz katere je razvidno, da podpira PRACK (prisotnost glave Supported: 100rel). Nato uporabnik B v sporočilu Session in Progress (183) pošlje ponudbo SDP. Poleg tega pa zahteva od strani A začasno potrjevanje – PRACK, v katerem je potem vsebovan odgovor SDP.



Slika 6: Izmenjava opisa SDP s pomočjo zahteve PRACK

4. Ponudba SDP je vsebovana v zahtevi PRACK, odgovor pa v odzivu 200 OK na to zahtevo.
5. Ponudba SDP je vsebovana v zahtevi UPDATE, odgovor pa v odzivu 200 OK na to zahtevo [Slika 7].

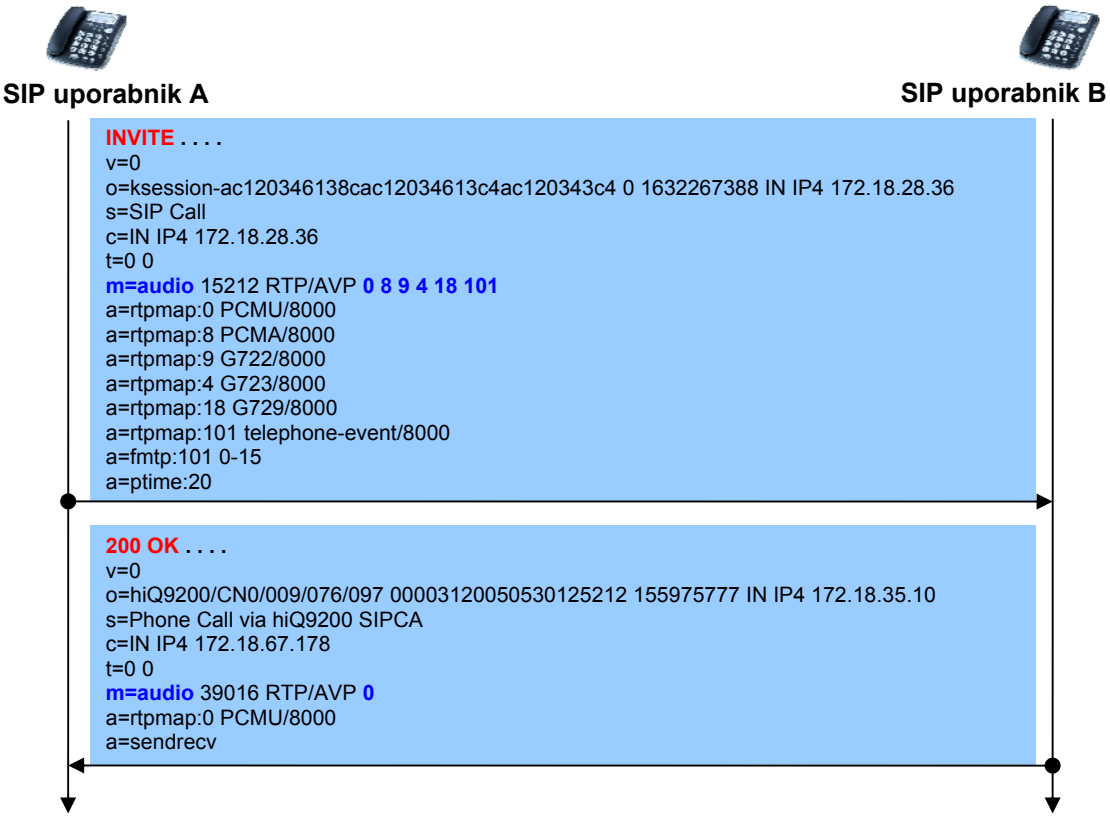


Slika 7: Izmenjava opisa SDP s pomočjo zahteve UPDATE

Katera od zgoraj navedenih možnosti se bo uporabila je odvisno predvsem od tega za kakšno vrsto storitve gre. Najpogosteje pa se uporablja kar prva.

3.1.5.3. Primera izmenjave opisa SDP za avdio in video klic

Najprej si poglejmo najosnovnejši primer izmenjave opisa seje za avdio klic [Slika 8]. Ponudba SDP v zahtevi INVITE vsebuje en medijski tok (angl. *media stream*) s spiskom šestih različnih kodekov, ki jih podpira stran A. Prioriteta kodekov si sledi po vrstnem redu. To pomeni, da ima npr. kodek 0 (PCMU ali G.711 μ – zakon) prednost pred kodekom 8 (PCMA ali G.711 A – zakon), kodek 8 pa pred kodekom 9. Za števila od 0 do 100 je preslikava (število – kodek) že fiksno določena, za števila večje od 100 pa je ta preslikava poljubna in se lahko za vsak klic spreminja.

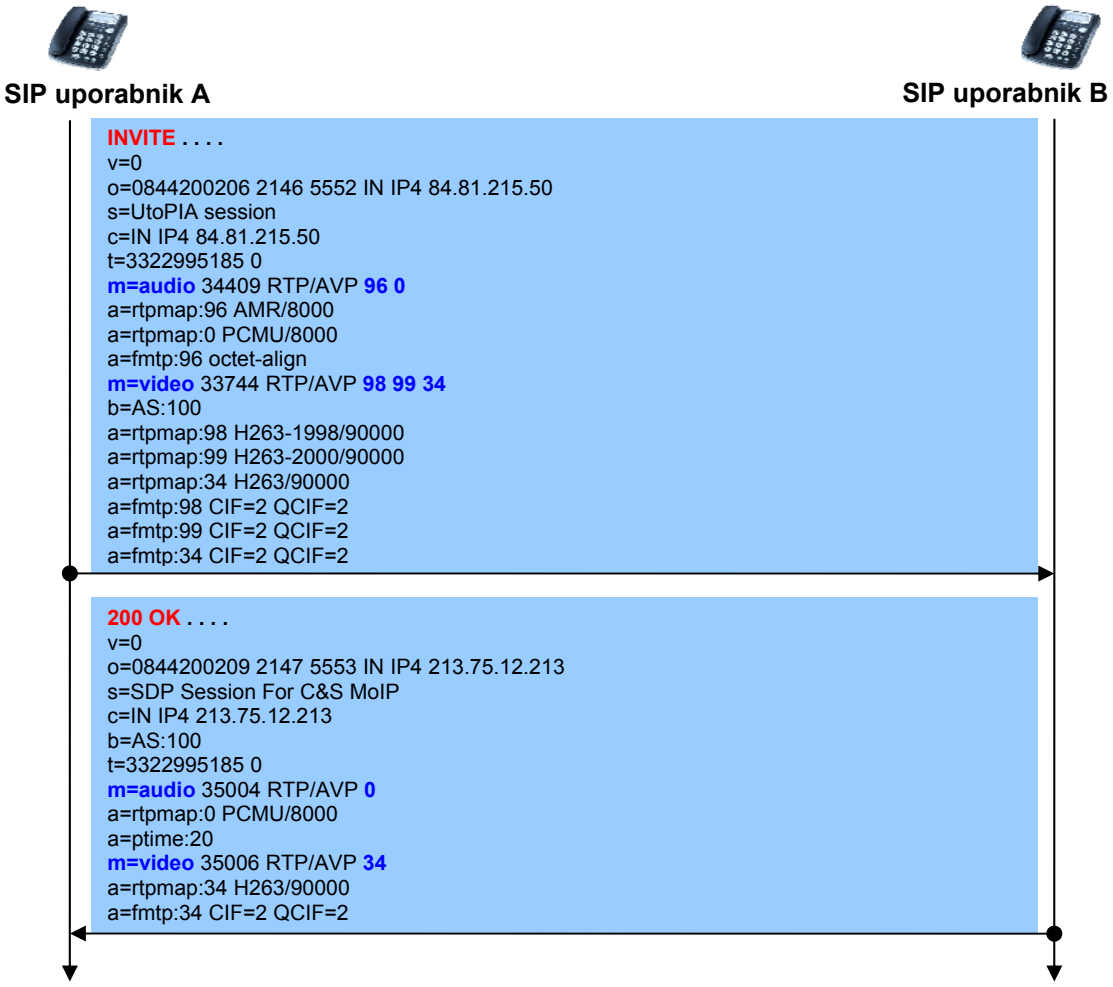


Slika 8: Primer izmenjave opisa SDP za avdio klic

Odgovor je vsebovan v potrditvi OK, ki mora vedno vsebovati opise za vse medijske tokove prejete v ponudbi. Vsak tak medijski tok pa mora vsebovati vsaj en pripadajoči kodek. V našem primeru stran B izbere prvi kodek, kar pomeni, da bosta tekom celotne seje oba uporabnika uporabljala samo kodek G.711 μ – zakon.

V primeru video klica ponudba vsebuje vsaj dva medijska tokova [Slika 9]. Avdio in video medijski tok, ki oba vsebujeta svoj nabor kodekov in potrebnih parametrov. Pri video kodekih je dodana še video resolucija in gostota slik (angl. *frame rate*).

Odgovor SDP v našem primeru vsebuje en kodek za vsak medijski tok. To pomeni, da bosta za prenos govora uporabljala kodek G.711 μ – zakon, za prenos slike pa H.263.



Slika 9: Primer izmenjave opisa SDP za video klic

3.2. Tipični scenariji SIP

3.2.1. Registracija uporabnikov

Protokol SIP ponuja zmožnost odkrivanja (angl. *discovery*). Če želi uporabnik vzpostaviti sejo z drugim uporabnikom, mora protokol SIP odkriti trenutnega gostitelja ali gostitelje (angl. *host*), preko katerih lahko doseže želenega uporabnika. Ta proces odkrivanja je dosežen z uporabo SIP omrežnih elementov, kot sta SIP proksi ali preusmeritveni strežnik. Njuna naloga je, da sprejmeta zahtevo in se na podlagi informacij o lokaciji posameznega uporabnika odločita kam bosta zahtevo poslala. Za shranjevanje informacij o lokaciji uporabnika je potrebna registracijska enota, ki je največkrat že kar sestavni del strežnika SIP. V nasprotnem primeru mora SIP proksi ali preusmeritveni strežnik izvesti poizvedbo na oddaljenem registracijskem strežniku.

To je prepuščeno kateremu drugemu protokolu (npr. protokolu, ki določa dostop do imenika (LDAP – *Lightweight Directory Access Protocol*); RFC 1777), kajti protokol SIP ne določa izvedbe registracijskega strežnika.

Naloga registracijske enote je, da SIP ali SIPS URI (npr. Bob@berlin.de) poveže z enim ali več identifikatorji, ki uporabnika opisujejo bolj natančno (npr. Bob@dev1.berlin.de).

Obstaja več načinov kako se ustvari podatkovna baza lokacijskega strežnika. Ena možnost je, da vse povezave vpisujemo ročno, vendar SIP zagotavlja povsem dinamičen mehanizem imenovan registracija. Sama registracija tako ustvarja povezave med ustrezno domeno ter dejanskimi naslovi uporabnikov, ki so vsebovani v glavi Contact. Ko proksi strežnik določene domene prejme zahtevo, kjer se vsaj en zapis ujema s poljem Request-URI, bo to zahtevo že lahko posredoval končnemu uporabniku ali uporabnikom.

Uporabnik se registrira tako, da pošlje registracijskemu strežniku zahtevo REGISTER [Slika 10] s svojimi kontaktnimi podatki (telefonska številka, IP naslov, vrata (angl. *port*) in transportni protokol (UDP ali TCP)). Poleg tega mora v svoji zahtevi določiti tudi časovni interval, v katerem bo uporabnik registracijo osvežil. V primeru, da registracijski strežnik v tem intervalu ne prejme ponovnega sporočila REGISTER, se uporabnik izbriše iz domenske podatkovne baze in od tega trenutka naprej uporabnik ni več dosegljiv.

Poleg tega se zahteva REGISTER uporablja tudi za poizvedbo trenutnih povezav in brisanje le-teh (časovni interval se nastavi na 0).

```
REGISTER sip:172.50.67.102:5060 SIP/2.0
Via: SIP/2.0/UDP 172.50.10.2:5060;branch=z9hG4bKc0f8ebb7d
Max-Forwards: 70
Content-Length: 0
To: line60002p <sip:02802600002@172.50.67.102:5060>
From: line60002p <sip:02802600002@172.50.67.102:5060>;tag= 42721c5e-15c1f-ac14640
Call-ID: 18145b915537ad06c81a090350a8e515@172.50.67.102
CSeq: 1919952650 REGISTER
Contact: line60002p <sip:02802600002@172.50.10.2:5060; transport=udp>;expires=3600
User-Agent: optiPoint 400 standard
```

Slika 10: Primer zahteve REGISTER

Iz primera na sliki lahko razberemo, da je v začetni vrstici zahteve IP naslov strežnika SIP (sip:172.50.60.102:5060), kamor je zahteva tudi naslovljena. Iz glave Contact pa lahko razberemo logično ime uporabnika (line60002p), ki se prikaže na prikazovalniku samega terminala, njegovo dejansko ime (02802600002) in naslov (172.50.10.2:5060), transportni mehanizem, ki ga uporablja (UDP), ter življenjski čas same registracije (3600 s). Registracijska enota na to zahtevo naredi vpis v svojo podatkovno bazo, ki bi izgledal nekako takole:

02802600002@172.50.60.102:5060 = 02802600002@172.50.10.2:5060

Uporabniki imajo na voljo tri načine kako določiti naslov strežnika SIP, kamor se nato pošlje zahteva REGISTER. Ena možnost je, da se naslov strežnika SIP nastavi ročno. Druga možnost je, da se uporabi normalni mehanizem iskanja lokacije strežnika SIP. Npr. uporabnik sip:Bob@berlin.de naslovi zahtevo na sip:berlin.de. Zadnja možnost pa je pošiljanje zahtev na več naslovov hkrati (angl. *multicast*). V tem primeru se sporočilo REGISTER pošlje na dobro znani (angl. *well-known*) naslov strežnika SIP. Za IP verzijo štiri (IPv4 – *IP version 4*) je to sip.mcast.net (224.0.1.75), za IP verzijo šest (IPv6 – *IP version 6*) pa zaenkrat še ni določen.

3.2.2. Povpraševanje po zmožnostih

Protokol SIP omogoča tudi, da uporabniški agenti povprašujejo druge agente ali proksi strežnike po njihovih zmožnostih. V ta namen se uporablja metoda OPTIONS, na podlagi katere lahko vsak uporabnik poskuša pridobiti informacije o metodah, različnih tipih vsebine, podaljških (angl. *extension*), kodekih itd., ki jih druga stran podpira in to brez kakršnegakoli vzpostavljanja seje. To pomeni, da lahko uporabnik še pred vzpostavljanjem seje preveri, če druga stran npr. podpira določene kodeke, ki so bistveni za realizacijo same seje.

S pomočjo spreminjanja vrednosti glave Max-Forwards in pošiljanjem zaporednih zahtev OPTIONS, lahko uporabnik preveri zmožnosti vsakega skoka posebej (angl. *hop*). Funkcionalnost je zelo podobna funkcionalnosti "trace route", ki je verjetno poznana marsikomu.

Primer zahteve OPTIONS je lepo razviden iz spodnje slike [Slika 11]. Iz začetne vrstice je lepo razvidno, da je zahteva namenjena končnemu uporabniku (carol@chicago.com). Prav tako zahteva vsebuje glavo Accept, ki označuje, kakšno naj bo telo sporočila, ki ga UAC pričakuje v odgovoru. Najpogosteje se na tem mestu uporablja format, ki je uporabljen za opis medijev (application/sdp).

```
OPTIONS sip:carol@chicago.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKhjhs8ass877
Max-Forwards: 70
To: <sip:carol@chicago.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 63104 OPTIONS
Contact: <sip:alice@pc33.atlanta.com>
Accept: application/sdp
Content-Length: 0
```

Slika 11: Primer zahteve OPTIONS

Odziv na zahtevo 200 OK [Slika 12] naj bi vedno vseboval metode (Allow: INVITE, ACK, CANCEL, OPTIONS, BEY), tip telesa (Accept: application/sdp), zgoščevalno metodo (Accept-Encoding: gzip), jezik (Accepted-Language) in podaljšek, ki ga uporabnik podpira. Poleg tega naj bi vseboval tudi telo sporočila, ki pa v spodnjem primeru ni prikazan.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKhjhs8ass877;received=192.0.2.4
To: <sip:carol@chicago.com>;tag=93810874
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 63104 OPTIONS
Contact: <sip:carol@chicago.com>
Contact: <mailto:carol@chicago.com>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
Accept: application/sdp
Accept-Encoding: gzip
Accept-Language: en
Supported: foo
Content-Type: application/sdp
Content-Length: 274
```

Slika 12: Primer potrditve zahteve OPTIONS

3.2.3. Usmerjanje zahtev in odzivov

Protokol SIP v osnovi ponuja poseben način usmerjanja zahtev in odzivov. Glede na to, da na začetku uporabniški agent pozna samo naslov svojega strežnika SIP, zahtevo za vzpostavitev seje pošlje prav njemu. Poleg ostalih glav, ki so v zahtevi

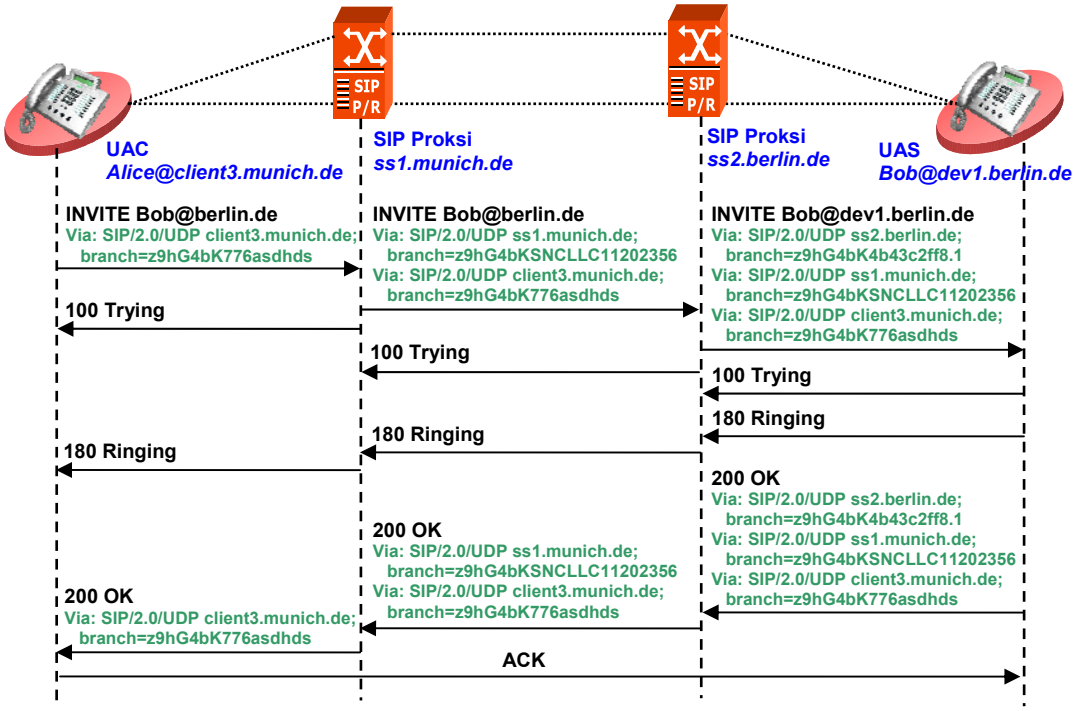
nujno potrebne, že sam uporabnik doda glavo Via. Njena vrednost je sestavljena iz naslova uporabnika, ki se ji na koncu doda še enoličen parameter branch. To pomeni, da se vrednost izračunanega parametra razlikuje za vse različne instance zahtev.

Proksi strežnik sprejme zahtevo in najprej preveri, če prejete zahteve ni sprejel že pred tem. To stori na podlagi vseh glav Via, ki so že vsebovane v zahtevi. Če je katera izmed njih njegova lastna, to pomeni, da je to zahtevo enkrat že obdeloval. Glede na parameter branch pa lahko določi ali gre za zanko ali spiralo. V prvem primeru zahtevo zavrne z odzivom 482 Loop Detected, v drugem pa nadaljuje z obdelavo, tako da pred že obstoječo glavo Via doda še svojo in zahtevo pošlje naprej. Ista procedura se izvede v vseh strežnikih preko katerih zahteva potuje, vse dokler zahteva ne pride do končnega uporabnika.

V primeru, da UAS želi vzpostaviti sejo, pošlje nazaj proti UAC-ju potrditev 200 OK. Za ta odziv je značilno, da opravi povsem enako pot kot pred tem zahteva. To pa zato, ker preden UAS odpošlje svoj odziv, vse glave Via, prejete v zahtevi, v istem vrstnem redu prekopira v odziv. Ko SIP proksi strežnik prejme tak odziv, najprej pogleda v glavo Via, zbriše svoj vpis in pošlje odziv na naslov, ki je vpisan v naslednji glavi Via. S tem se skrajša tudi čas obdelave odziva, saj v tem primeru ni več potrebno obremenjevati registracijskega strežnika, ker odziv s sabo nosi vse potrebne informacije za pravilno usmeritev.

Od trenutka, ko uporabnik prejme odziv od klicanega uporabnika, dobi tudi njegov pravi naslov. To pomeni, da za vse nadaljnje zahteve lahko uporablja direktno pot in ne potrebuje več ne proksi, ne preusmeritvenega in ne registracijskega strežnika. Prva taka zahteva je že metoda ACK, s katero se potrjuje originalna zahteva INVITE.

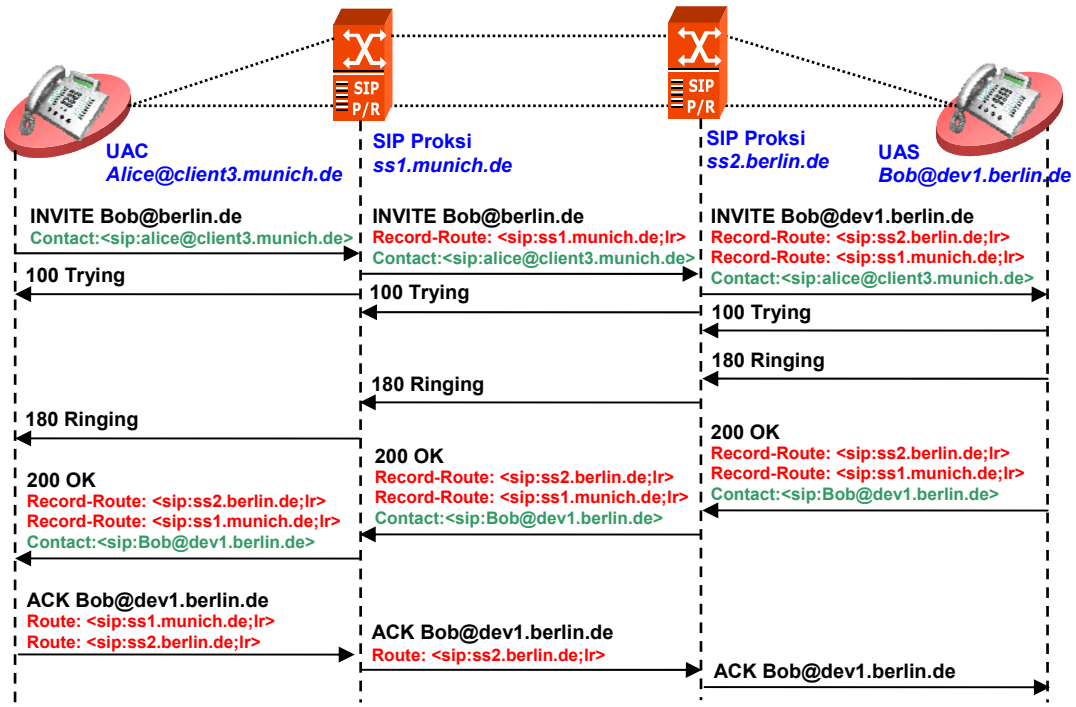
Z drugimi besedami se vse zahteve, ki so poslane znotraj vzpostavljenega dialoga, pošiljajo direktno od enega proti drugemu uporabniku. Vse druge zahteve, poslane izven dialogov, pa morajo prečkati strežnike SIP. Ravno zaradi takega pristopa je SIP bolj skalabilen, saj strežnike SIP obremenjuje manjše število sporočil [Slika 13].



Slika 13: Usmerjanje na podlagi glave Via

V nekaterih situacijah pa SIP proksi strežnik mora ostati na poti vseh sporočil. Tak primer je, če proksi nadzoruje omrežni element, ki dela preslikavo IP številk (NAT) ali če je uporabljen za tarifiranje storitev. V ta namen SIP ponuja poseben mehanizem (angl. *loose routing*, [RFC3261]).

Vsak SIP proksi strežnik, ki želi ostati na poti sporočil, v prejeto zahtevo, poleg glave Via, doda še posebno glavo imenovano Record-route, ki vsebuje naslov strežnika. Če v zahtevi ta glava že obstaja, mora strežnik glavo dodati pred že obstoječo. V primeru, da uporabnik na drugi strani želi vzpostaviti sejo, pošlje v odzivu 200 OK vse glave Record-Route, v istem vrstnem redu, kot jih je prejel v zahtevi. Sedaj imata oba uporabnika vse informacije o poti, ki ji morajo slediti vse nadaljnje zahteve znotraj ravnokar vzpostavljenega dialoga. Tako bosta oba uporabnika lahko v vse nadaljnje zahteve v pravem vrstnem redu dodajala glave Route. Ko strežnik sprejme tako zahtevo, najprej zbriše prvo glavo Route. Nato prebere naslednjo in zahtevo usmeri na ravnokar prebrani naslov.



Slika 14: Usmerjanje na podlagi glave Route

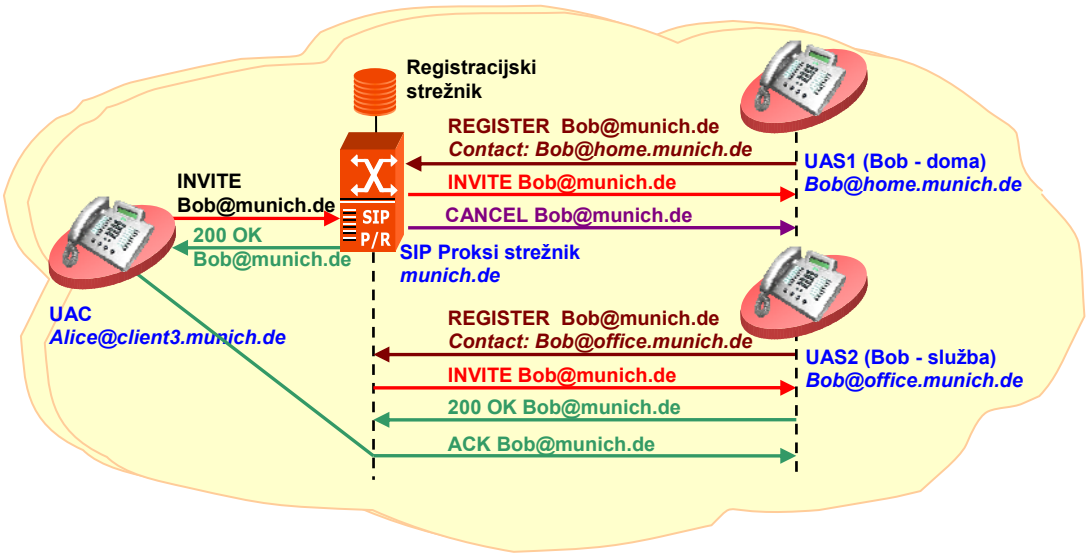
3.2.4. Razcep sporočil SIP

Protokol SIP ima že v sami osnovi vgrajene določene mehanizme, zaradi katerih je lahko protokol še bolj zanimiv za končne uporabnike. Eden izmed takih mehanizmov je razcep sporočil (angl. *SIP forking*).

Če na primer želimo biti ves čas dostopni in se selimo z ene lokacije na drugo, obstaja več možnosti. Najlažja možnost bi verjetno bila, da si kupimo mobilni telefon, vendar vedno to ni mogoče. V tem primeru lahko uporabimo eno izmed množice storitev, ki jih ponujajo telekomunikacijski operaterji. Od najpreprostejše preusmeritve pa vse do storitev, ki jih ponujajo inteligentna omrežja (IN – *Intelligent Network*). Lahko pa svojim potencialnim sogovornikom posredujemo celotni spisek telefonskih številk na katerih bomo dosegljivi in upamo, da ne bodo obupali preden nas dobijo. Za tako preprosto stvar takšna rešitev problema povzroči kar precej komplikacij.

Sedaj pa poglejmo, kako bi takšno situacijo rešili s pomočjo protokola SIP. Kot smo že povedali v poglavju 3.2.1 (Registracija uporabnikov), se lahko vsak uporabnik prijavi oz. registrira z istim uporabniškim imenom z večih različnih lokacij. To pomeni, da ima lahko registracijski strežnik v nekem trenutku za določeno osebo lahko več

kontaktnih naslovov. Če v tem trenutku nekdo želi vzpostaviti sejo s to osebo, potem se bo zahteva INVITE razcepila v več vzporednih vej in začelo bo zvoniti več uporabniških agentov [Slika 15]. Glede na to, da isti uporabnik fizično ne more biti na dveh različnih lokacijah, bo sejo lahko vzpostavil samo z ene lokacije. Proksi strežnik pa bo poskrbel, da se bodo vse na pol vzpostavljene vzporedne seje pravilno zaključile.



Slika 15: Razcep sporočil SIP

3.2.5. Osveževanje seje

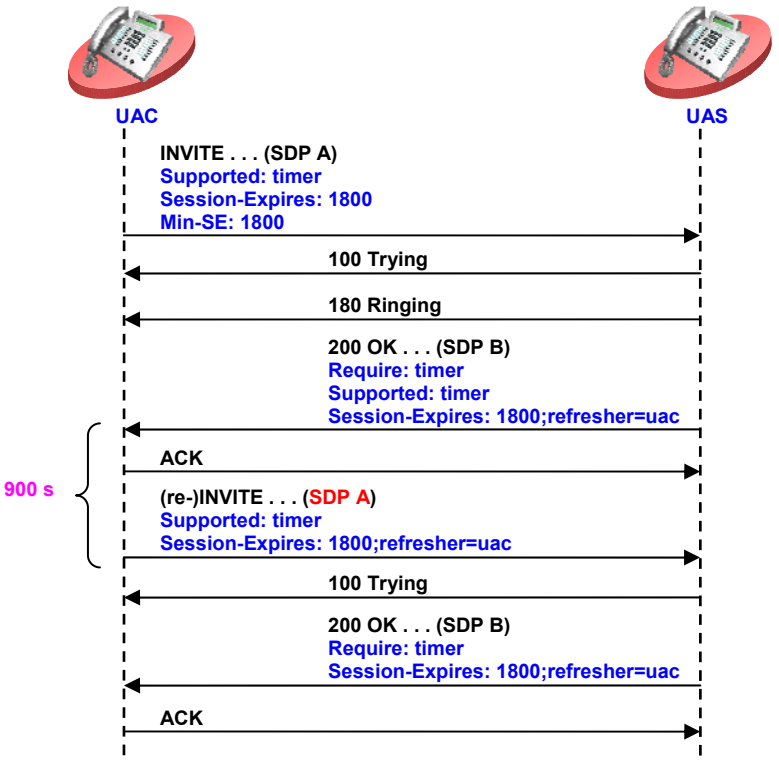
Sam protokol SIP ne vsebuje nobenega mehanizma za ugotavljanje ali je vzpostavljena seja še aktivna ali ne. Čeprav uporabniški agenti to lahko ugotovijo na podlagi specifičnih parametrov seje, proksi strežniki tega niso sposobni. Rezultat tega je, da strežnik SIP ne bo mogel vedno zagotovo vedeti ali je določena seja še živa ali ne. Ko na primer uporabniški agent pošlje zahtevo BYE in se ta zaradi omrežnih problemov izgubi, strežnik SIP ne bo vedel, da se je seja končala. Zato bo v nedogled vzdrževal stanje te seje, čeprav ne obstaja več.

Podobno se lahko zgodi, če imamo v omrežju napravo NAT, ki vsebuje tudi prehod na aplikacijskem nivoju (ALG – *Application Level Gateway*). Ta ohranja stanje seje, in ko je le-ta končana, je potrebno sprostiti vse vire vezane nanjo. Če ta omrežni element ne prejme sporočila BYE, ki sproži sproščanje virov, lahko pride do potencialne zapore strežbe (DoS – *Denial of Service*).

Iz tega razloga, se je originalnemu SIP standardu dodal še en podaljšek standarda imenovan RFC 4028 [RFC4028], ki opisuje celoten mehanizem. Njegovo bistvo je v tem, da uporabniški agenti po uspešno vzpostavljeni seji začnejo s periodičnim pošiljanjem zahtev INVITE ali UPDATE. Interval osveževanja je določen na podlagi pogajanj. Če agent ni poslal zahteve za osveževanje ali če ni prejel odgovora na poslano zahtevo, se predpostavlja, da je seja končana. Zato v tem primeru pošlje še sporočilo BYE, na podlagi katerega konča vzpostavljeni dialog, SIP proksi pa sprosti vire, zasežene s to sejo.

Poglejmo si konkreten primer, kako to osveževanje izgleda v praksi [Slika 16]. Z vzpostavitvijo seje prične UAC, tako da pošlje zahtevo INVITE, v katero poleg osnovnih informacij, ki so potrebne za vzpostavitev seje, vključi še informacijo, da podpira mehanizem osveževanja seje (Supported: timer). Poleg tega UAC določi še minimalni (Min-SE: 1800) in želeni (Session-Expires: 1800) časovni interval osveževanja, ki je v našem primeru enak.

Ko se UAS odloči, da bo sprejel ponujeno sejo, pošlje proti UAC-ju odziv 200 OK, v katerega doda informacijo, da tudi on podpira osveževanje (Supported: timer). Ker je UAC zahteval osveževanje, se v odziv vključi tudi ta informacija (Required: timer). Poleg tega se mora še odločiti, kakšen bo interval osveževanja. Izbere se lahko katerikoli interval, dokler je ta večji od minimalnega intervala prejetega v zahtevi (Min-SE: 1800), lahko pa je enak predlaganemu. V našem primeru bo interval dolg kar predlaganih 1800 s. Najmanjši interval osveževanja, ki ga podpira priporočilo pa je 90 s.



Slika 16: Osveževanje seje

Nazadnje mora UAS določiti še kdo bo osveževanje kontroliral. Glede na to, da UAC ni poslal nobenega predloga in podpira osveževanje, ima možnost izbire ali bo to opravljal sam ali pa bo nalogo prepustil pobudniku seje, kar v našem primeru tudi naredi. V drugih primerih pa se lahko UAS odloča o kontrolorju na podlagi spodnje tabele [Tabela 12].

Ali UAC podpira RFC 4028?	*Kontrolor osveževanja v zahtevi*	*Kontrolor osveževanja v odzivu*
Ne	-	UAS
Ne	UAC	Se ne uporablja
Ne	UAS	Se ne uporablja
Da	-	UAS ali UAC
Da	UAC	UAC
Da	UAS	UAS

Tabela 12: Določanje kontrolorja osveževanja [RFC4028]

Kontrolor osveževanja nato začne s štetjem časa. Po preteku polovice določenega maksimalnega intervala osveževanja (900 s) kontrolor pošlje drugi strani zahtevo INVITE ali UPDATE. Če se za osveževanje uporablja metoda INVITE, potem mora

le-ta vsebovati opis SDP, ki mora biti popolnoma enak zadnjemu poslanemu. Če pa je uporabljena metoda UPDATE, se opisa SDP ne pošilja.

Seveda je potrebno pri vsakem ciklu osveževanja ponoviti pogajanje o intervalu in kontrolorju osveževanja. Najenostavneje je, če ti parametri ostanejo ves čas seje nespremenjeni, lahko pa se z vsakim ciklom spremenijo. Kako to poteka v realnosti je popolnoma odvisno od implementacije samega priporočila.

4. Konvergenčna omrežja in komunikacije

V času konvergenčnih omrežij tako podjetja kot tudi že nekateri telekomunikacijski operaterji postavljajo lastna omrežja IP kot skupno infrastrukturo za prenos govora in podatkov. Takšno omrežje mora zagotavljati ustrezno kvaliteto storitev, kot tudi zanesljivost za uporabnike kritičnih poslovnih in komunikacijskih aplikacij v realnem času. Zaradi vse večje porazdeljenosti večjih podjetij in povečanih zahtev po naprednih aplikacijah za dosego večje učinkovitosti, se vedno bolj uveljavljajo ne samo konvergenčna omrežja, temveč tudi konvergenčne komunikacije.

4.1. Potrebe razvijajočih se komunikacijskih omrežij

Potrebe po konvergenčnih omrežjih in komunikacijah lahko združimo v tri skupine ali vidike [Avaya_04].

1. Poslovni vidik

Dandanes so podjetja dobesedno izzvana, da simultano nadzorujejo stroške in rast dohodkov z načelom narediti več z manj (angl. *to do more with less*). Izboljševanje povezav do svojih strank in večanje produktivnosti svojih uslužbencev postajata vse večja in pomembnejša dejavnika med konkurenco. Poleg tega povečan nivo nevarnosti in groženj zahteva še bolj natančno planiranje poslov, njihovo nadaljevanje ter iskanje novih tržnih niš.

2. Uporabniški vidik

Razvijanje komunikacijskih rešitev, ki ne izboljšujejo uporabniških zmožnosti oz. ne rešujejo njihovih problemov, ne prinaša ravno svetle prihodnosti. Uporabniki se bodo verjetno branili prehoda na nove aplikacije ali učenja novih aplikacijskih vmesnikov, če ti ne bodo vsebovali dodatnih funkcionalnosti ali boljše produktivnosti. Poleg tega pa morajo biti tudi enostavni za uporabo. Rešitve morajo tako vsebovati in omogočati virtualnim in mobilnim uporabnikom delo od kjerkoli ter enostaven dostop do kakršnihkoli informacij in omrežij podjetja. Uporabniku morajo ne glede na

uporabljeno napravo dati konsistenten občutek ter mu pomagati do večje učinkovitosti pri opravljanju vsakodnevnih kompleksnih nalog.

3. Informacijski vidik

Ta vidik zahteva rešitve, ki so dovolj fleksibilne za prilagajanje poslovnih modelov v primeru sprememb političnih in ekonomskih razmer. Te rešitve naj bi dovoljevale centralizirano in porazdeljeno konfiguriranje in administriranje ter nadzor in upravljanje vse končnih točk. Prav tako morajo zagotavljati zaščito investicije z možnostjo dobre integracije v obstoječo infrastrukturo ter dobro možnostjo za kasnejše dograjevanje in spreminjanje.

4.2. Evolucija informacijske infrastrukture

Evolucijo infrastrukture informacijske tehnologije (IT – *Information Technology*) bi lahko razdelili na tri faze [Avaya_04]. Podjetja ali telekomunikacijski operaterji imajo tako možnost postopnega razvoja delov omrežja glede na poslovne potrebe, kar dejansko pomeni obratovanje omrežja v več različnih fazah hkrati.

Za prvo, tradicionalno fazo je značilno, da imamo ločeni infrastrukturi za govor in podatke. Za govor uporabljamo TDM, za podatke pa omrežje IP. V naslednji fazi, fazi konvergenčnih omrežij poskrbimo za izgradnjo ali nadgradnjo omrežja IP kot skupne infrastrukture za prenos govora in podatkov. Na tem mestu moramo poskrbeti oz. povečati kvaliteto storitev ter zanesljivost časovno in operacijsko kritičnih poslovnih in komunikacijskih aplikacij.

S povečevanjem porazdeljenosti ter širitvijo storitev, ki narekujejo povečevanje uporabniških zmožnosti, pridemo do tretje faze imenovane konvergenčne komunikacije. Njeno bistvo se skriva v povečani fleksibilnosti in cenovni učinkovitosti, ki ju dosežemo z modularizacijo komponent in aplikacij. Bolj ko je rešitev modularna, lažje jo je integrirati v večproizvajalsko okolje, poleg tega pa jo je mogoče postaviti v večjem številu različnih okolij.

4.3. Protokol SIP in konvergenčne komunikacije

Večina starih telefonskih naprav so neumne končne točke brez spomina ali vgrajenega procesorja. To pomeni, da mora biti vsa logika implementirana znotraj TDM stikal. V času konvergenčnih omrežij in komunikacij pa končne točke vsebujejo procesorje ter spomin in s tem se inteligenca, ki je bila prej centralizirana, porazdeli po celem omrežju. Protokol SIP je tako signalni protokol, ki poskrbi za komunikacijsko povezavo med temi pametnimi končnimi točkami. Kot smo že povedali, se uporablja za vzpostavitev običajnih ali konferenčnih, govornih ali video sej, prenos informacij o prisotnosti in lokaciji, multimedijsko sodelovanje med uporabniki oz. prenos hipnih sporočil med večimi končnimi točkami.

Protokolu SIP bi lahko rekli kar katalizator naslednje stopnje odprtih komunikacij preko omrežja IP. Je interoperabilni protokol v večproizvajalskem okolju, ki odpira nove možnosti za večjo prilagodljivost sistemov in omrežja z večimi storitvami. Ravno to omogoča strankam, da izmed vseh proizvajalcev in ponudnikov izberejo najprimernejšega in tako zgradijo konvergenčno komunikacijsko omrežje.

Uporabnik z večimi napravami, kot so mobilni telefon, namizni telefon, dlančnik in osebni računalnik, se lahko popolnoma zanese na protokol SIP, ki poskrbi za dobro integracijo teh entitet in s tem poveča uporabnikovo učinkovitost in produktivnost. Protokol SIP se od podobnih komunikacijskih protokolov razlikuje v široki podpori industrije, ki protokolni sklad vgrajuje že v vse mogoče naprave in aparate.

Poleg bogatega nabora različnih medijskih sej in informacij, ki jih je sposoben prenašati, protokol SIP ponuja še naslednje prednosti [Intel_06]:

- ***Konvergenčna omrežja***

Z uporabo enega hrbteničnega omrežja za prenos govora, videa in podatkov zmanjšujemo stroške, poenostavljamo nadzor in upravljanje. S tem naredimo še en pomemben korak v smeri konvergenčnih komunikacij.

- ***Mobilnost***

Protokol SIP uporabnikom omogoča predstavljanje z logično identiteto ne glede na napravo, ki jo trenutno uporablja ali njeno fizično lokacijo. To uporabnikom omogoča prehajanje oz. preklapljanje med različnimi napravami ali lokacijami, medtem pa so

še vedno dosegljivi na enem in istem logičnem naslovu. Uporabnikom tako ni potrebno vrteti številnih telefonskih številk.

- ***Povečana kvaliteta govora***

Tradicionalna telefonska omrežja prenašajo samo 4 kHz del celotnega frekvenčnega pasu človeškega govora, ki se razteza nekje od 80 Hz in vse do 15 kHz. To je seveda razlog, da je človeški glas preko telefona drugačen. V nasprotju s tem lahko protokol SIP uporablja širokopasovni kodek, ki zajema širši frekvenčni pas (npr. od 50 Hz do 7 kHz) in s tem omogoča prenos govora z minimalnimi spremembami.

- ***Integrirana prisotnost***

Komunikacijska seja se največkrat vzpostavlja na podlagi uporabnikove dostopnosti in želje po komunikaciji. Na podlagi objavljene informacije o prisotnosti uporabnika se lahko določi ustrezen tip seje (npr. med sestankom bo uporabnik raje uporabljal IM, kot pa govor, ki bi motil ostale udeležence).

Sedaj pa si poglejmo še nekaj najpomembnejših storitev, ki predstavljajo konvergenčne komunikacije [Hiti_05].

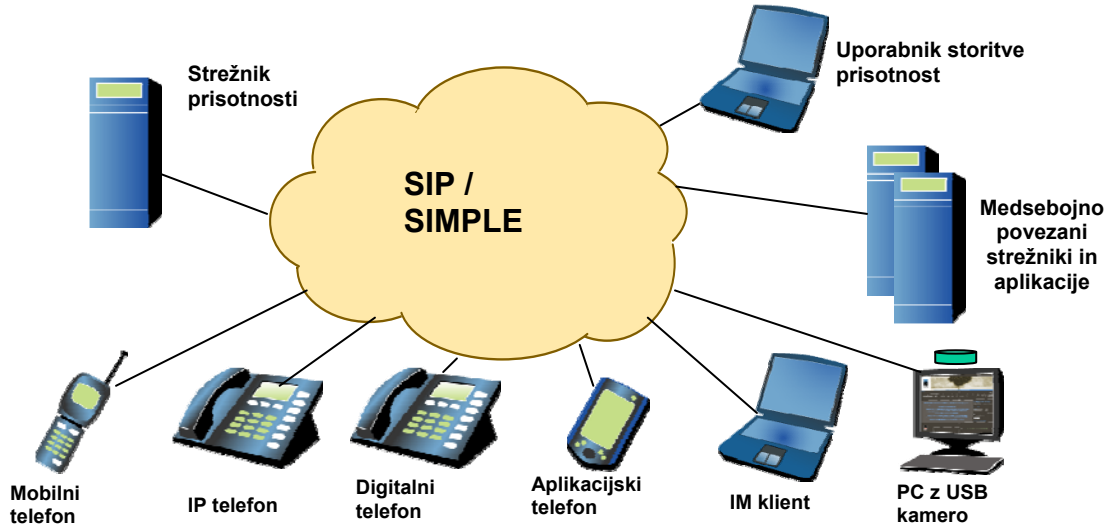
4.3.1. Storitev prisotnosti

Storitev prisotnosti omogoča objavo svojega stanja o prisotnosti (nedosegljiv, v pisarni, izven pisarne, dosegljiv na mobilni telefon …) ter naročanje na informacije o stanju prisotnosti drugih naročnikov. V tem primeru dobimo sporočilo o kakršnikoli spremembi stanja prisotnosti opazovanega naročnika. Omenjena storitev je izvedena z uporabo mehanizmov spremljanja dogodkov in obveščanja, ki so določeni v priporočilu RFC 3265 [RFC3265]. Pomemben koncept predstavlja tudi strežnik prisotnosti (angl. *presence server*), ki zbira podatke o stanju prisotnosti naročnikov in omogoča, da se uporabniki naročijo na te informacije. Na ta način povečamo zmogljivost in razširljivost sistema, saj končne točke pošljejo informacijo o svojem stanje le strežniku, in ne vsem na ta podatek naročenim končnim točkam. Storitev prisotnosti postane močno orodje predvsem v kombinaciji s telefonskimi klici oz. hipnimi sporočili, saj lahko znatno poveča dosegljivost uporabnikov ter učinkovitejšo izrabo časa v delovnem procesu (npr. strežnik SIP v kombinaciji s strežnikom prisotnosti preusmerja klice na mobilni telefon, ko uporabnika ni v pisarni).

Kljub prednostim pa lahko predvsem socialni dejavniki omejijo uporabo prisotnosti. Postavlja se namreč vprašanje ali bomo izpadli nevljudni, če kljub temu, da bomo imeli objavljeno stanje dosegljivosti, ne bomo odgovarjali na posamezne klice. Drugo vprašanje je ali bomo zaradi objave svoje prisotnosti prejeli več klicev in s tem posledično več motenj delovnega procesa ali bomo prihranili več časa s tem, da bomo uporabnike klicali le, ko bodo dosegljivi. Pri nadaljnjem razvoju te storitve bo potrebno nameniti še precej pozornosti zasebnosti in varnosti, saj mora biti informacija o prisotnosti dosegljiva le upravičenim uporabnikom in nikakor ne sme postati predmet zlorabe.

4.3.2. Storitev hipnih sporočil

Storitev hipnih sporočil omogoča pošiljanje kratkih sporočil med končnimi točkami. Sam prenos sporočil je podoben prenosu elektronske pošte, vendar pa je za uporabnika to povsem nekaj drugega, saj gre običajno za kratke stavke ali sporočila, ki jih izmenjujemo z uporabnikom. Običajno se uporabljajo v povezavi s telefonskim klicem (npr. sklic konferenčne zveze), lahko pa tudi samostojno po vzoru drugih pogovornih programov (npr. Yahoo, AOL, MSN …). Posebna delovna skupina znotraj SIP foruma, imenovana SIMPLE (*SIP Instant Messaging and Presence Leveraging Extensions*), skrbi za razvoj hipnih sporočil in storitve prisotnosti oz. določa način njihove uporabe [Slika 17]. Pravzaprav SIMPLE omogoča protokolu SIP še večjo privlačnost za konvergenčne komunikacije.



Slika 17: Primer konvergenčne komunikacije [Lazar_06]

Podobno kot pri vzpostavitvi ostalih SIP sej, se tudi tu za pridobitev pravilnega naslova uporabnika uporabi registracijski strežnik, nato pa se sporočilo (angl. *message*) prenese preko ustreznih strežnikov SIP do končne točke. Možna sta dva načina prenosa hipnih sporočil in sicer neodvisen prenos sporočil (angl. *page mode*) ter prenos sporočil znotraj seje (angl. *session mode*). Pri prvem gre za prenos vsakega sporočila popolnoma neodvisno od drugih, kar pomeni, da lahko vsako sporočilo potuje do končnega cilja po različnih poteh. V tem primeru vmesne SIP entitete ne poznajo povezave med posameznimi sporočili. Pri prenosu sporočil znotraj seje poteka komunikacija podobno kot pri navadnem telefonskem pogovoru. Razlika je samo v tem, da se za medijski kanal namesto protokola RTP uporabi protokol za prenos sporočil znotraj vzpostavljene seje (MSRP – *Message Session Relay Protocol*). Za prenos manjše količine informacij je primernejši prvi način. Način seje pa je ustreznejši, ko gre za večje izmenjave sporočil ali celo datotek, saj se le-ta prenašajo direktno med končnima točkama in ne obremenjujejo vmesnih strežnikov SIP.

4.3.3. Storitev multimedijskega sodelovanja

Eden izmed najpomembnejših konceptov konvergenčnih komunikacij je nedvoumno multimedijsko sodelovanje (angl. *multimedia collaboration*), ki znotraj ene aplikacije oz. portala združuje govor in video. Poleg tega omogoča avdio, video in spletne konferenčne zveze, skupno sledenje in spreminjanje dokumentov, hipna sporočila, prisotnost, elektronsko in govorno pošto, združeno sporočanje (angl. *unified messaging*), pretvorbo teksta v govor (angl. *text to speech*) in obratno (angl. *speech to text*), ter tako uporabnikom omogoča in zagotavlja učinkovitejše delo in izrabo časa. Multimedijsko sodelovanje omogoča uporabnikom nadzor nad dokumenti, viri in delovnimi procesi in v korporacijska omrežja vpeljuje nov koncept dela. Večji proizvajalci, kot so Microsoft (RTC – *Real Time Collaboration*), Siemens (*OpenScape*) in IBM (*Domino Collaboration Server*), so svoje rešitve razvili na podlagi SIP protokola, vendar imajo kljub oglaševanju standardnih rešitev, večino storitev izdelanih na podlagi lastnih, nestandardnih rešitev.

Multimedijsko sodelovanje bo v naslednjih letih najverjetneje doživelo razcvet, saj bo podjetjem omogočilo hitrejše odzive na spremembe in učinkovitejše razpolaganje z

zaposlenimi, viri in podatki. Kljub temu bo tudi na tem področju potrebno posebno pozornost nameniti varnosti in zasebnosti ter tudi večji standardizaciji rešitev.

4.4. Integracija infrastrukture

Pred enim desetletjem je svetovni splet (WWW – *World Wide Web*) uporabil protokol HTTP in s tem omogočil brskalnikom dostop do katerekoli spletne strani znotraj interneta. Protokol SIP uporablja podobno psihologijo, saj najprej poskrbi za dogovor o medijih, ki se bodo uporabili. SIP obljublja, da bo imel na komunikacijske rešitve vsaj tak vpliv, kot ga je imel svetovni splet na informacijski dostop.

Vpeljava protokola SIP oz. njegova integracija v konvergenčna omrežja je načeloma najenostavnejša za manjša podjetja, ki svojo infrastrukturo šele postavljajo ali načrtujejo. Prav tako je integracija protokola SIP relativno enostavna tudi za nove telekomunikacijske ponudnike, ki želijo na trg prodreti z novimi tehnologijami in ne potrebujejo nekakšnih vmesnih rešitev, s katerimi bi želeli obdržati že obstoječe stranke, ki slonijo na starejših tehnologijah in ne bi želele preiti na nove. Vendar tudi za velika podjetja ali večje telekomunikacijske operaterje, ki že imajo zgrajeno svoje hrbtenično omrežje ali še vedno ponujajo TDM priključke, obstajajo dobre rešitve. Edina slabost take vpeljave je čas, ki je potreben za vse skupaj, saj se je tega potrebno lotiti postopoma, po predhodno natančno določenih korakih. Tak evolucijski pristop tudi ščiti investicije v trenutno infrastrukturo. Vse to pa ima na drugi strani za posledico mešanico večih različnih protokolov, ki bodo morali v takih sistemih nekaj časa delovati vzporedno.

Na prvem mestu je tako priprava in postavitev dobro načrtovanega hrbteničnega omrežja, ki bo imelo primerne kapacitete za načrtovane storitve in s tem posledično zagotovljeno dobro kvaliteto teh storitev. To je osnovni predpogoj za dobro delovanje sistema, in če temu delu ne posvetimo dovolj časa, lahko kasneje pride do velikih problemov, ki so rešljivi, vendar cenovno izredno dragi.

Naslednja zadeva je postavitev nujno potrebnih SIP entitet ali strežnikov. V prvi vrsti sta to registracijski in SIP proksi strežnik, ki sta osnova celotnega SIP sistema. Od njune izbire je kasneje odvisno koliko dodatnega vložka bo potrebno za nadgrajevanje sistema ali za implementacijo povsem nove storitve. Lahko pa

namesto teh dveh strežnikov izberemo B2BUA strežnik, ki je načeloma dražji, vendar ima največkrat registracijsko in preusmeritveno komponento že implementirano. Poleg tega pa vsebuje oz. ima že implementirane marsikatere storitve, ki bi jih ali jih bomo kasneje želeli v svojem sistemu, tako da nam taka izbira lahko prihrani marsikateri tolar.

Seveda se pri postopnem prehodu skorajda ne moremo izogniti prehodom, ki bodo povezovali starejše sisteme (npr. TDM) z novejšimi in s tem pripomogli k gladkemu prehodu na konvergenčna omrežja in nato naprej na konvergenčne komunikacije. Zavedati pa se moramo, da se s tem precej poveča kompleksnost celotnega omrežja. Prehod je seveda nujen tudi v vsakem drugem primeru, ko želimo novonastajajočemu sistemu priključiti sistem, ki ne uporablja ali ne pozna protokola SIP (npr. globalni sistem za mobilne komunikacije (GSM – *Global System for Mobile Communications*), univerzalni mobilni telekomunikacijski sistem (UMTS – *Universal Mobile Telecommunications System)* ali sistem H323).

Sedaj imamo osnovno SIP okolje pripravljeno. Odločiti se moramo samo še katere oz. kakšne SIP kliente bomo ponudili končnim uporabnikom. Bo to navadni telefonski aparat z implementiranim SIP protokolom ali naprava z integriranim dostopom (IAD – *Integrated Access Device*)? Mogoče pa bo to prehod na strani uporabnika (CPG – *Customer Premises Gateway*) ali pa samo aplikacija, ki bo tekla na osebnem računalniku ali kaki drugi napravi. Odločitev je povsem odvisna od ponudnika storitev, vendar se moramo zavedati, da imajo nekateri klienti vgrajene več drugi pa manj logike in spomina. To pa sta dva dejavnika, ki pri implementaciji določenih storitev (npr. avdio in video konferenca) igrata pomembno vlogo. Odločitev ali novo storitev implementirati centralizirano ali porazdeljeno je namreč odvisna tudi od zmožnosti samih SIP klientov.

Glede na to, da je sistem že od samega začetka zasnovan popolnoma modularno, nam implementacija oz. dodajanje novih storitev ne sme povzročati prevelikih problemov. Če npr. želimo svojim uporabnikom ponuditi storitev prisotnosti, potem v obstoječi sitem samo dodamo strežnik prisotnosti (Presence Server). Nato še na SIP proksi ali B2BUA strežniku spremenimo oz. dodamo ustrezne nastavitve, ki omogočajo potrebno medsebojno komunikacijo. S tem je nova storitev implementirana.

Na enak način se v sistem dodajajo nove storitve (npr. razni nadzorni in upravljavski portali za navadne uporabnike, podjetja, poslovnih skupin ali posebnih skupin uporabnikov, ki so znotraj navideznih zasebnih omrežij, zasnovanih na javnih telefonskih centralah (CENTREX – *Central Exchange*)), vendar na žalost ni vedno tako enostavno, predvsem zaradi rešitev, ki še niso standardizirane in se tako od proizvajalca do proizvajalca lahko precej razlikujejo in jih zato zaenkrat še ne moremo medsebojno povezovati. Zavedati pa se moramo tudi tega, da je teh interoperabilnih problemov z vsakim dnem manj.

Pri vsem skupaj pa ne smemo pozabiti tudi na varnost samih uporabnikov, njihovih informacij ter celotnega sistema. Zato je potrebno v to arhitekturo na ustrezna mesta dodati še požarne zidove, uvesti uporabo navideznih omrežij in glede na stopnjo zahtevane varnosti uvesti tudi enkripcijo.

Vse skupaj se verjetno sliši precej preprosto in enostavno, vendar v realnosti na žalost ni vedno tako. Pri sami vpeljavi ali integraciji največkrat naletimo na množico zahtev in problemov, ki se na prvi pogled zdijo nerešljivi, vendar natančnejša analiza prinese sprejemljive rešitve, ki v končni fazi pomenijo implementacijo dodatne strojne in programske opreme. S ključnimi problemi se bomo bolj natančno soočili v naslednjem poglavju.

5. Problemi pri integraciji

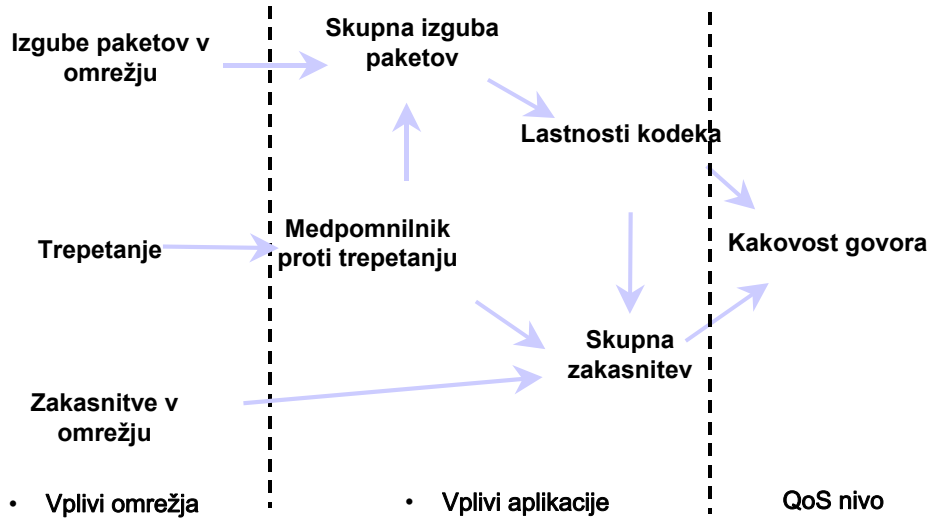
Prenos govornih komunikacij preko paketnih IP omrežij je eden izmed najpomembnejših trendov v telekomunikacijah. Prav tako kot ostale nove tehnologije s seboj prinaša poleg novih priložnosti, kot so znižanje cen in stroškov, precej več fleksibilnosti ter več različnih storitev, tudi precej novih problemov. Bistvo teh problemov je ravno v dejstvu, da se arhitektura govornih komunikacij osnovanih na omrežju IP preveč razlikuje od tradicionalnih omrežij. Poleg tega že samo omrežje IP s seboj prinaša celo vrsto problemov, ki so jih doslej reševali predvsem z vidika prenosa podatkov in ne govora. Zato je izrednega pomena, da se teh problemov pravilno in čim prej lotimo, če ne želimo, da bi to negativno vplivalo na nadaljnji razvoj in vpeljavo novodobnih storitev, predvsem pa pričakovanj, ki jih protokol SIP, kot osnovni protokol konvergenčnih omrežij, tudi ponuja.

5.1. Zagotavljanje kvalitete storitev

Kvaliteta storitev (QoS – *Quality of Service*) oz. izpolnjevanje dogovora o njihovem nivoju (SLA – *Service Level Agreement*) je ena izmed izredno pomembnih stvari pri prenosu govora preko paketnih omrežij in uveljavitvi konvergenčnih omrežij. Kajti ne glede na vse prihranke in prednosti, ki jih taka omrežja ponujajo, bi bila dodana vrednost izredno majhna ali celo negativna, če kvaliteta storitev ne bi bila vsaj primerljiva s tradicionalnimi telefonskimi omrežji. Poudariti pa moramo, da kakršnekoli implementacije varnostnih mehanizmov že v sami osnovi zmanjšujejo kvaliteto, saj vnašajo še dodatne zakasnitve, trepetanje in izgube paketov. Poleg tega pa je večina storitev časovno kritičnih, kar pomeni, da že nekaj izgubljenih paketov lahko pomeni občutne motnje ali celo izpad storitve. Ravno to je tudi vzrok, da marsikateri že implementirani varnostni mehanizem v paketnem omrežju, tu ni primeren. Na kakovost storitve tako vplivajo naslednji dejavniki:

- ***zakasnitev***, t.j. čas med oddajo in sprejemom paketa;
- ***trepetanje***, t.j. variacija zakasnitve;
- ***zahteve za pasovno širino***;

- ***zmožnosti strojne opreme*** za kodiranje, prenos in dekodiranje govornega signala v vsakem elementu omrežja;
- ***število napačno prenesenih paketov***.



Slika 18: Dejavniki, ki vplivajo na kakovost storitve

Splošne zahteve omrežij za prenos VoIP so trepetanje pod 10 ms (običajno pod 5 ms) in izguba paketov do 10^{-4}.

5.1.1. Zakasnitve

Zakasnitev (angl. *latency*) predstavlja čas, ki je potreben, da govor pride od izvora do ponora. V priporočilu ITU-T G.114 [ITU_G114] je zgornja meja pri prenosu v eno smer nekje do 150 ms. Vse zakasnitve do 400 ms so uporabne samo pogojno; recimo v primeru, da uporabnik ve, da gre za prenos preko satelitov. Za komercialno uporabo omenjajo mejo nekje pri 290 ms. Zakasnitve večje od 400 ms so največkrat nesprejemljive, razen v posebnih primerih, ko ne gre drugače. Recimo pri dvojnih satelitskih ali dolgih mednarodnih povezavah, kjer smo s predpostavko, da druge možnosti ni, pripravljeni sprejeti tudi večje zakasnitve.

Prenos časovno kritičnih podatkov tako ne sme presegati zgornje meje zakasnitve, t.j. 150 ms, če želimo, da je kvaliteta primerljiva s tradicionalnimi omrežji. Ta meja pa nam žal ne dopušča velikih napak pri prenosu. Največje zakasnitve nastajajo pri

kodiranju, paketizaciji, prenosu, čakanju v vrstah in raznih medpomnilnikih ter izvajanju varnostnih algoritmov [Tabela 13]. To na primer pomeni, da manjše ko imamo izgube pri prenosu in čakanju v vrstah, boljše varnostne mehanizme (večje zakasnitve) lahko implementiramo, ne da bi s tem kakorkoli škodovali sami kvaliteti storitev.

Izvor zakasnitve (G.729)	*Zakasnitev (ms)*
Jemanje vzorca	0,1
Kodiranje (zakasnitev algoritma + zakasnitev obdelave)	17,5
Paketizacija	20
Izhodna čakalna vrsta	0,5
Prenos do hrbteničnega omrežja	10
Zakasnitve hrbteničnega omrežja	X
Prenos iz hrbteničnega omrežja	10
Vhodna čakalna vrsta	0,5
Izenačevalnik trepetanja	60
Dekodiranje	2
Zakasnitev predvajanja	0,5
Vsota:	121,1+X

Tabela 13: Primer zakasnitev pri prehodu skozi omrežje [SecCon_05]

Zakasnitve v omrežjih VoIP so precej večje kot pri klasičnem TDM klicu, predvsem zaradi konceptualnih razlogov. Ker želimo omrežje IP izkoriščati čim bolj ekonomično, se informacija, ki jo dobimo vsakih 125 µs ne pošlje takoj, ampak se akumulira nekaj milisekund (angl. *packetizing period*), potem pa se pošlje vse skupaj v obliki IP paketa. Teoretično je možno zmanjšati zakasnitev na nekaj milisekund, vendar s tem zapravljamo pasovno širino hrbteničnega omrežja in izrabljamo preveč procesorske moči.

Zavedati se moramo, da se zakasnitve spreminjajo povsem dinamično, saj so odvisne od dolžine posameznega paketa, od števila prehodov (požarne stene, NAT-i, usmerjevalniki …), od uporabljenega kodeka, nastavitve izenačevalnika trepetanja [Tabela 14], trenutnih razmer omrežja itd.

Kodek	*Paketizacijski čas minimalen/uporabljen*	*Pogled naprej*	*Povprečna zakasnitev med obema koncema*
G.711	125 µs/10 ms	0	< 60 ms
G.726	125 µs/10 ms	0	< 60 ms
G.729A	10 ms/10 ms	5 ms	< 70 ms
G.723.1	30 ms/30 ms	7.5 ms	< 90 ms

Tabela 14: Zakasnitve različnih kodekov

5.1.2. Trepetanje

Trepetanje je neenakomerna zakasnitev paketov (angl. *jitter*). Ta varianca zakasnitve se pojavi zaradi različnih poti paketov RTP ali sprememb na omrežnem nivoju. Treba jo je odpraviti z vmesnim pomnilnikom, ki zadržuje pakete dlje kot predvidevamo, da bo največja varianca zakasnitve. To zadrževanje paketov vpliva na skupno zakasnitev in ne bi smelo biti preveliko. Možno je tudi, da se dolžina medpomnilnika dinamično spreminja glede na ugotovljeno trenutno trepetanje. Pri določanju trepetanja si pomagamo s podatki iz protokola RTP in protokola za nadzor prenosa v realnem času (RTCP – *Real Time Transport Control Protocol*). Velikost medpomnilnika naj bo taka, da lahko pokrijemo trepetanje do 200 ms. Paketi z večjimi zakasnitvami so odvrženi.

5.1.3. Izgube paketov

Za izgube paketov RTP so krive preobremenitve, prevelike zakasnitve na poti ali okvare vsebine paketov. Pri zaznavanju izgubljenih paketov pomaga zaporedna številka, ki je vključena v paket RTP. Izgubljene pakete lahko nadomestimo na več različnih načinov. Najlažje je, če jih nadomestimo s tišino ali s ponavljanjem zadnjega paketa. Poleg tega lahko paket ustvarimo umetno, na podlagi matematičnih algoritmov (interpolacija) ali uporabimo dodaten mehanizem za vnaprejšnje popravljanje napak pri prenosu (FEC – *Forward Error Correction*). Vsak paket vsebuje približno 10 do 50 byteov koristne vsebine, t.j. 12,5 do 62,5 ms govora. Izguba paketa tako pomeni izgubo fonema, kar vpliva na razumljivost, še posebej, če je takih izgub veliko.

Primerjava kvalitete storitev med tradicionalnim in omrežjem VoIP je pokazala, da že zelo majhen delček izgubljenih paketov lahko zniža kvaliteto konvergenčnih omrežij pod mejo, ki jo današnji uporabnik pričakuje v tradicionalnih omrežjih [Sinden_02]. Pri vseh kodekih, ki jih je študija obravnavala, je bila degradacija kvalitete storitev zelo hitra, čim je bila presežena meja zakasnitve 150 ms. Tudi pri zakasnitvah manjših od 150 ms in 5% izgubi paketov je kvaliteta govora kodiranega z G.711 (standard za kodiranje govora s 64 kbps) kodekom padla pod nivo kvalitete PSTN omrežij, kljub temu, da je bil uporabljen algoritem za prikrivanje izgub (angl. *packet*

loss concealment). Podoben rezultat je bil pri uporabi kodekov G.729A (standard za kodiranje govora z 8 kbps) in G.723.1 (standard za kodiranje govora s 5,3 kbps), kjer je že pri izgubi paketov med enim in dvema odstotkoma kvaliteta padla pod pričakujočo mejo. Študija je pokazala tudi to, da čim večja je kompresija, tem bolj je kvaliteta storitev občutljiva na izgubo paketov.

5.1.4. Izločanje odmeva

Za prenos govora je nekaj odmeva zaželenega, prevelika količina ali preveč zakasnjen govor pa deluje moteče. Uporabnik bo začel razločevati vrnjeni signal od originalnega, če bo zakasnitev večja od 20 do 30 ms. Vse odmeve, zakasnjene nad 30 ms, je treba izločiti, hkrati pa ohraniti ves koristni signal z oddaljenega konca.

5.1.5. Določanje kakovosti govora

Kakovost govora je subjektivna vrednost. Da bi omogočili merjenje, so določili teste, s katerimi zajamemo to vrednost. Srednja vrednost pridobljenih mnenjskih točk (MOS – *Mean Opinion Score*) uporablja za ocenjevanje ljudi, ki se izrazijo o kakovosti govora z vrednostmi od ena do pet, pri čemer ena pomeni slabo, pet pa odlično. Običajni govor preko telefona ima MOS = 4.

S kodeki za govor, ki so v uporabi, dobimo vrednosti od tri do več kot štiri.

Kodek	*Pasovna širina*	*MOS*
G.711	64 kbps	4.15
G.729a	8 kbps	3.78
G.723.1	5.3 kbps	3.57

Tabela 15: Vrednost MOS pri uporabi različnih kodekov

Poleg MOS-a se uporablja tudi meritev kvalitete govora na podlagi človeškega zaznavanja (PSQM – *Perceptual Speech Quality Measure*), ki omogoča samodejno merjenje kakovosti govora. Primerja prenesen in shranjen vzorec govora in upošteva fiziologijo človekovega sluha in miselne procese ljudi. Rezultati so na skali od 0 (najboljši) do 6,5 (najslabši).

Za testiranje VoIP sta primernejši novi metodi, kot sta ocenjevanja kvalitete govora na podlagi človeškega zaznavanja (PESQ – *Perceptual Evaluation of Speech*

Quality) in analiza ter meritev sistema na podlagi človeškega zaznavanja (PAMS – *Perceptual Analysis/Measurement System*), katerih rezultati so bolj podobni testom MOS.

5.1.6. Načini zagotavljanja QoS

Kot smo ravnokar povedali je kvaliteta storitev osredotočena predvsem na hiter in zanesljiv prenos IP paketov s čim manjšim tresenjem, izgubo in zakasnitvijo paketov. Za standardna omrežja IP je značilno, da se vsak paket obravnava enako, ne glede na vsebino, ki jo nosi. To pomeni, da omrežni elementi (npr. usmerjevalnik) prejete pakete poskušajo kar najhitreje prenesti iz vhodne čakalne vrste na ustrezen izhod, in sicer na podlagi vrstnega reda prihodov (FIFO – *First In First Out*). Ta način se imenuje najboljši možni način (angl. *best effort*) v danih okoliščinah. To pa seveda za današnja omrežja ni sprejemljivo, saj se na podlagi te metode ne more ločevati niti različnih vrst prometa.

Z željo, da zagotovimo hiter in zanesljiv prenos časovno kritičnih paketov, moramo imeti na voljo dovolj pasovne širine. To pa lahko zagotovimo s predpripravo in razvrščanjem paketov v različne časovno kritične skupine. S predpripravo se namreč lahko zagotovi dovolj pasovne širine, tako da ne pride do preobremenjenosti niti v najbolj prometnih urah.

Uporabimo lahko:

1. ***IntServ***

   Z IntServ (angl. *Integrated Services*) pristopom vsak terminal in vsi omrežni elementi, ki se bodo uporabili, rezervirajo določene vire (pasovno širino in procesorski čas) za vsak klic posebej. Primer takega pristopa je protokol za rezervacijo virov (RSVP – *Resource Reservation Protocol*). Ti viri so potem 100% zagotovljeni za ustreznega uporabnika in jih drugi uporabniki ne morejo koristiti. IntServ pristop je uporaben samo v primeru, če vsi usmerjevalniki na poti med dvema uporabnikoma podpirajo ustrezen protokol. Poleg tega je zelo kompleksen, potrebuje osveževanje rezervacij in ni ravno primeren za velika omrežja. Protokol RSVP se trenutno uporablja samo v manjših omrežjih.

2. DiffServ

Z DiffServ (angl. *Differentiated Services*) pristopom razvrščamo promet v različne prometne razrede glede na njegovo časovno kritičnost. Omrežni elementi prejeti paket uvrstijo v ustrezno čakalno vrsto glede na razred kateremu paket pripada in ga nato na podlagi prioritete tudi ustrezno hitro obdelajo. Dobra lastnost tega pristopa je, da ne potrebuje nobene signalizacije oz. vnaprejšnje rezervacije virov in je primeren za velika omrežja. Tudi izkoriščenost omrežja je na precej višjem nivoju kot pri IntServ pristopu. Primer takega pristopa je uporaba posebnega polja v IP glavi imenovanega tip storitve (TOS – *Type of Service*). Glavna razreda, ki jih DiffServ definira sta:

- ***EF*** (angl. *Expedited Forwarding*) – majhne zakasnitve z majhnim nihanjem;
- ***AF*** (angl. *Assured Forwarding*) – več podrazredov z različnimi zakasnitvami in izgubami.

Pakete lahko označujejo že sami končni terminali. Lahko pa je to realizirano s prehodi oz. robnimi usmerjevalniki, ki imajo nalogo označevanja paketov z ustreznimi prioritetnimi razredi. Vsi omrežni elementi morajo obravnavati vse pakete v skladu z dodeljeno prioriteto, tako da imajo definirane različne vrste in različne mehanizme za vsak prioritetni razred.

DiffServ ne rešuje preobremenjenosti omrežij ali katerih drugih omrežnih problemov, vendar s pravilnim dimenzioniranjem vedno zagotovi QoS zahteve prioritetnega prometa.

3. Protokol MPLS

Za zmanjšanje zakasnitev, ki so posledica obdelave paketov, je bilo definirano večprotokolno preklapljanje na osnovi oznak (MPLS – *Multi Protocol Label Switching*). Načeloma mora vsak usmerjevalnik analizirati celotno IP glavo, da lahko pošlje paket naprej proti ustreznemu izhodu. S pomočjo protokola MPLS so vsi IP paketi opremljeni z dodatno oznako. To oznako paketu doda robni usmerjevalnik ali prehod. Tako mora usmerjevalnik analizirati samo to dodatno oznako in že lahko določi ustrezni izhod, kamor paket tudi pošlje. S tem se hitrost obdelave paketov lahko precej poveča.

Glede na to, da danes že obstajajo visoko zmogljivi usmerjevalniki, ki so zmožni obdelati in usmeriti paket z enako hitrostjo, s katero prihajajo do samega usmerjevalnika, protokol MPLS za konvergenčna omrežja ni več potreben.

Zelo uporabna aplikacija, ki jo ponuja MPLS je nadzor nad prometom (angl. *traffic engineering*), kar pomeni, da se IP paketi z določenimi parametri (npr. prioriteta), lahko usmerijo na podlagi vnesenih administratorjevih pravil. Primer tega bi bil, da se časovno kritični promet usmerja tja, kjer so zakasnitve najmanjše, ostali promet pa tja, kjer so zakasnitve večje. Vendar je za vse to potreben dodaten administrativni vložek za vzpostavitev vseh MPLS povezav.

5.1.7. Razpoložljivost in zanesljivost

Ko govorimo o kvaliteti storitev ne smemo pozabiti na razpoložljivost in zanesljivost, saj sta to predvsem s stališča uporabnika dva izredno pomembna vidika. Razpoložljivost klasičnih omrežij se danes giblje v razredu 99.999%, kar pomeni 5 minut izpada v enem letu. Cilj je doseči takšno razpoložljivost tudi v konvergenčnih omrežjih.

Kar se tiče samih lokalnih omrežij (LAN – *Local Area Network*) ali interneta, je potreben kar precej dolg čas (nekaj sekund ali celo minut) za zamenjavo usmerjevalnikov ali za vzpostavitev storitev. To ne povzroča večjih problemov za podatkovne storitve (npr. prenos datotek s pomočjo protokola za prenos datotek (FTP – *File Transfer Protocol*), HTTP …), kar se pa tiče časovno kritičnih aplikacij, je potreben precej hitrejši odziv, ki se lahko doseže samo z zelo previdnim in natančnim načrtovanjem omrežja.

V klasičnih omrežjih se je visoka razpoložljivost dosegala na podlagi drage strojne opreme, odporne na napake. V konvergenčnih omrežjih pa želimo doseči podoben učinek s pomočjo preusmerjanja sporočil na druge strežnike na podlagi DNS koncepta ter podvajanja strojne opreme (uporaba virtualnih IP naslovov), ki nam zelo olajša nadgrajevanje programske opreme. V primeru nedosegljivosti primarnega strežnika lahko uporabnik na podlagi DNS povpraševanja pridobi naslov nadomestnega strežnika, kateremu nato prvotno zahtevo tudi pošlje.

Že sama uporaba signalizacijskega protokola nam lahko povzroča potencialne probleme. V primeru uporabe protokola UDP, ki je nepovezavno orientiran, se pojavi težava pri ugotavljanju ali je paket prišel do želenega cilja ali ne, saj je postopek relativno dolg. Z uporabo protokola TCP, ki je povezavno orientiran, se temu izognemo, vendar pa so zato zakasnitve precej večje. Zaenkrat je še vedno najboljša rešitev uporaba lastnih mehanizmov proizvajalcev strojne ali programske opreme, ki dosegljivost strežnikov neprestano spremljajo po vzoru preverjanja aktivnosti nižjih slojev v TDM sistemih.

5.2. Zagotavljanje varnosti

Eden izmed največjih problemov na katerega naletimo najprej je zagotavljanje varnosti. Ravno zaradi vse večje povezanosti informacijskih sistemov in s tem vse večje dostopnosti, ki omogoča velikemu številu uporabnikov dostop do informacij brez fizične prisotnosti, se možnost zlorab izredno hitro povečuje. Zato je zagotavljanje varnosti vedno večji in pomembnejši vidik pri načrtovanju novih telekomunikacijskih sistemov.

V novih konvergenčnih telekomunikacijskih sistemih imamo opravka predvsem s prenosom paketov (govorna komunikacija, podatki in video) in sporočil. Namenjeni so lahko končnemu uporabniku ali pa so to sistemska sporočila, ki so namenjena za nadzor in upravljanje samega sistema. Ne glede na namen lahko nepooblaščen dostop to teh informacij povzroči manjšo ali večjo škodo samemu uporabniku ali ponudniku telekomunikacijskega sistema. Naloga zagotavljanja varnosti je tako preprečevanje tovrstnih zlorab, kar z drugimi besedami pomeni zagotoviti celovitost paketov in sporočil ter zanesljivo dostavo le-teh pravemu naslovniku.

5.2.1. Celovitost podatkov in sporočil

Pojem celovitosti podatkov in sporočil je razdeljen na tri dele [Tomažič_03]:

- ***avtentičnost*** (zagotavlja identiteto izvora);
- ***verodostojnost*** (zagotavlja enakost oddanega in sprejetega podatka in sporočila);

- ***zasebnost*** (zagotavlja dostopnost podatka ali sporočila samo naslovniku).

Na prvi pogled je najpomembnejši vidik celovitosti verjetno zagotavljanje zasebnosti, saj noben uporabnik ne želi, da bi nekdo tretji bral njegovo pošto, hipna sporočila, poslušal pogovor … Velikokrat pa se zgodi, da sta prva dva vidika precej pomembnejša. Če na primer nekdo uporablja storitve v drugem imenu (avtentičnost), to nenazadnje pomeni, da jih bo moral plačati uporabnik, za katerega se je nepridiprav izdajal. Lahko pa pri nakupu nekega predmeta preko spleta nekdo spremeni naročilo tako (verodostojnost), da bo plačane stvari prejel on in ne plačnik.

Takih primerov je lahko izredno veliko, zato je nujno potrebno zagotoviti celovitost za vse tri vidike. To je mogoče narediti na več načinov in povsem neodvisno od posameznega vidika.

Vse vidike celovitosti podatkov in informacij je mogoče zagotoviti z ustrezno uporabo šifrirnih postopkov, ki pa sami po sebi ne zagotavljajo celovitosti. Zato jih moramo uporabiti v ustreznih protokolih in na ustreznih OSI nivojih.

Glede na to, da so šifrirni postopki relativno varni, saj zaenkrat ni bilo kakšnih znanih zlorab le-teh, napadalci običajno izkoriščajo šibkosti samega protokola, napak v implementaciji ter slabih ali nepravilnih nastavitev s strani uporabnika ali ponudnika.

5.2.1.1. Avtentikacija sporočil in uporabnikov

Avtentikacija sporočila oz. uporabnika pomeni, da lahko z veliko gotovostjo ugotovimo identiteto pošiljatelja oz. avtorja sporočila. Poleg tega moramo včasih poznati tudi natančen čas sporočila, da uporabnik ne more zanikati, da je sporočilo ustvaril on. Zato se uporabljata še časovni žig in storitev časovnega žigosanja.

Avtentičnost sporočil je zelo pomembna pri sistemskih sporočilih, ki so namenjena za upravljanje in nadzor telekomunikacijskega sistema. Uporabniku je dostop dovoljen le, če se je pred tem identificiral. Poleg tega je avtentikacija sporočil zelo pomembna tudi v sistemih, kjer uporabniki niso več vezani na samo fizično lokacijo. V tem primeru se mora vsak uporabnik pred kakršnokoli uporabo storitev najprej identificirati, saj bi se v nasprotnem primeru lahko njegovih storitev posluževal kdorkoli.

Najpreprostejši način dokazovanja identitete je s pomočjo uporabniškega imena in gesla. Ponavadi je uporabniško ime javno in ga lahko pozna kdorkoli. Geslo pa mora biti tajno in naj bi ga poznal samo uporabnik. Sama identifikacija poteka tako, da se uporabniško ime in geslo prenašata po sistemu. Prav zaradi tega ima ta način identifikacije precej pomanjkljivosti. Najpomembnejše so naslednje:

1. Gesla se največkrat prenašajo v čisti tekstovni obliki (angl. *clear text*), kar pomeni, da lahko vsak, ki to sporočilo prestreže, uporablja lažno identiteto.

2. Če se znotraj sporočila šifrirata samo geslo in uporabniško ime, sam sistem ni nič bolj varen, kajti namesto gesla in uporabniškega imena v čisti tekstovni obliki pač uporabimo šifrirano obliko, ki smo jo prebrali v prestreženem sporočilu.

3. Uporabniki ponavadi izbirajo zelo preprosta gesla, ki jih potencialni napadalec lahko hitro ugotovi. Lahko pa v ta namen uporabi eno izmed množice programskih orodij dostopnih na internetu, katerih namen je prav razbijanje gesel. Temu se da v precejšni meri izogniti z ustrezno varnostno politiko, ki ne dovoljuje preprostih gesel (obvezna uporaba določenih znakov, minimalna dolžina, obvezna uporaba malih in velikih črk).

4. Uporabniki ponavadi morajo dostopati do različnih sistemov in prav zaradi tega potrebujejo celo množico uporabniških imen in gesel, ki si jih težko zapomnijo. Zato jih največkrat zapišejo na mesta, ki so lahko dostopna (npr. zadnja stran tipkovnice).

Drugi način avtentikacije, ki odpravlja večino zgoraj naštetih pomanjkljivosti je uporaba protokola na osnovi izziva in odgovora (angl. *challenge and response*). Tudi v tem primeru ima vsak uporabnik svoje uporabniško ime in geslo, ki pa se ne prenašata več po sistemu. To geslo je tajno in ga poznata samo uporabnik in sistem. Tu sistem izzove uporabnika tako, da mu pošlje neko naključno sporočilo (npr. naključno izbrano število, ki je zaradi večje varnosti največkrat neko izredno veliko število). Uporabnik nato uporabi prejeto sporočilo in ga šifrira (uporabi določen šifrirni algoritem) s svojim tajnim geslom. Lahko pa uporabi sporočilo tako, da mu doda še svoje skrito geslo in nad tem uporabi zgoščevalni algoritem (angl. *hash algorithm*) ter pošlje sistemu dobljeni rezultat. Sistem, ki prav tako pozna tajno geslo, nato izvede

enak postopek in primerja rezultate. Če sta enaka je uporabnik identificiran. Tak način preverjanja identitete (angl. *digest authentication*) uporablja tudi protokol SIP o katerem bomo več povedali malo kasneje.

Poleg že omenjenih načinov se uporabnik lahko identificira tudi na podlagi digitalnega podpisa. Kar pomeni, da uporabnik podpiše sporočilo s svojim digitalnim podpisom, s katerim zagotavlja, da je on res on. Sistem pa preveri digitalni podpis uporabnika s pomočjo njegovega javnega ključa. Tak sistem za svoje delovanje potrebuje posebno entiteto – overitelja digitalnih certifikatov (CA – *Certification Authority*). Njegova naloga je, da overjene javne ključe podpiše s svojim digitalnim podpisom in s tem zagotavlja avtentičnost javnega ključa za določen čas. Predpogoj vsega pa je seveda, da vsi uporabniki tega sistema zaupajo v overitelja. V tem primeru je avtentikacija mogoča brez kakršnekoli predhodne izmenjave sporočil.

Glede na to, da je tajni ključ neko izredno veliko praštevilo, ki si ga uporabnik ne more zapomniti, mora biti ta nekje shranjen. Seveda mora biti shranjen tako, da ga ne more uporabiti nihče drug razen nas. To pa pomeni, da spet pridemo do tajnega gesla, ki ga uporabnik potrebuje za šifriranje in dešifriranje privatnega ključa. Za sisteme, kjer je potrebna povečana varnost, pa ključ lahko shranimo na prenosni medij (npr. USB ključ, pametna kartica, magnetna kartica …), ki je dostopen samo nam.

5.2.1.2. Zagotavljanje verodostojnosti

Verodostojnost sporočil pomeni, da lahko z zelo veliko gotovostjo trdimo, da je sprejeto sporočilo identično oddanemu. Pri zagotavljanju verodostojnosti moramo preprečiti možnosti, da bi pri prenosu sporočil prišlo do nenamerne ali namerne spremembe vsebine.

Nenamerno spreminjanje sporočil lahko preprečimo z redundančnim kodiranjem. To pomeni, da originalnemu sporočilu dodamo nekakšen prstni odtis, ki ga dobimo tako, da uporabimo neko zgoščevalno funkcijo. Seveda pri tem mora veljati, da je verjetnost, da bi imeli dve sporočili enak prstni odtis, izredno majhna. Prejemnik sporočila tudi sam izračuna prstni odtis sporočila in ga primerja s prstnim odtisom, priloženim v sporočilu. Če sta enaka, potem obstaja zelo velika verjetnost, da

sporočilo ni bilo spremenjeno. Če pa se prstna odtisa razlikujeta, se s pomočjo prejete redundančne informacije sporočilo poskusi popraviti. Če je sprememb preveč, potem tudi dodatna informacija ni dovolj in sporočilo se mora zavreči. Primera takega kodiranja sta dodajanje paritetnega bita in dodajanje ciklične redundančne kode (CRC – *Cyclic Redundancy Check*).

Zlonamernega spreminjanja sporočil pa na žalost ne moremo preprečiti na tak način, kajti napadalec lahko poleg spremembe sporočila spremeni tudi prstni odtis celotnega sporočila. Take spremembe uporabnik ne more odkriti. Edina možnost je, da prstni odtis, ki ga priložimo sporočilu šifriramo z nekim tajnim ključem (npr. uporaba našega privatnega ključa). V tem primeru pa napadalec ne more več spremeniti vsebine sporočila, ker ne pozna našega tajnega ključa.

5.2.1.3. Zagotavljanje zasebnosti

Zasebnost lahko najbolj neposredno zagotovimo z uporabo ustreznega šifrirnega postopka. Glede na vrsto ključev ločimo dve vrsti šifrirnih postopkov: simetrični in asimetrični. Za prve je značilno, da za šifriranje in dešifriranje uporabljamo isti ključ. Poleg tega tudi računsko niso zahtevni. Edini problem z uporabnikovega vidika je v tem, da je potrebno pred komunikacijo na nek varen način izmenjati ključ.

Pri asimetričnem postopku pa imamo vedno par ključev. Šifrirni in dešifrirni ključ oz. javni in privatni ključ. S šifrirnim ključem sporočilo šifriramo, z dešifrirnim, ki mora biti njegov par, pa ga dešifriramo. Ker šifriranega sporočila tako ne moremo dešifrirati z istim ključem, je povsem nepotrebno, da bi bil ta tajen. Ravno zaradi tega ga imenujemo tudi javni ključ. S tem pa smo tudi rešili problem izmenjave ključev. Ker pa so asimetrični postopki zasnovani na tako imenovani enosmerni funkciji s stranskim vhodom (angl. *one way trapdoor function*), so računsko precej zahtevnejši od simetričnih.

V praksi zato največkrat uporabljamo kombinacijo obeh. To pomeni, da za daljša sporočila uporabljamo simetrični postopek, za krajša pa asimetrični. Drugače povedano, komunikacijo začnemo z asimetričnim postopkom, znotraj katerega poskrbimo za varno izmenjavo simetričnih ključev. Nato pa preklopimo na simetrični postopek, ki je precej hitrejši in ne obremenjuje sistema v taki meri, kot prej

asimetrični postopek. Zaželeno je, da je za vsako sejo ustvarjen nov simetrični ključ, ali pa celo, da se med samo sejo večkrat zamenja.

Za boljše razumevanje povedanega si oglejmo primer preprostega protokola izmenjave sejnega ključa s pomočjo asimetričnega šifrirnega postopka. Uporabnik **A** želi poslati uporabniku **B** zaupno sporočilo, zato:

- **A** sporoči svojo namen **B**-ju.
- **B** pošlje **A**-ju svoj javni ključ $\boldsymbol{E_B}$.
- **A** ustvari naključen sejni ključ $\boldsymbol{S}$ in z njim simetrično šifrira svoje sporočilo. Z javnim ključem $\boldsymbol{E_B}$ nato še asimetrično šifrira sejni ključ **S** in ga skupaj s šifriranim sporočilom pošlje **B**-ju ($\boldsymbol{E_B(S)}$).
- **B** s svojim tajnim ključem $\boldsymbol{D_B}$ najprej dešifrira sejni ključ S ($\boldsymbol{D_B(E_B(S)) = S}$) in potem s pomočjo simetričnega ključa $\boldsymbol{S}$ še poslano sporočilo.

Zgornji primer ima veliko pomanjkljivost, namreč če ima nek tretji uporabnik možnost prestrezanja (angl. *man in the middle attack*) vseh sporočil med uporabnikoma, potem se lahko vmeša v njuno sejo, ne da bi uporabnik **A** ali uporabnik **B** to sploh opazila. To pomanjkljivost se da odpraviti z uvedbo overitelja digitalnih certifikatov. V tem primeru nam nek tretji uporabnik ne bi mogel podtakniti svojega javnega ključa, ker bi javni ključ zahtevali od overitelja. Tako bi sporočilo lahko dešifriral res samo uporabnik, kateremu smo želeli sporočilo tudi poslati. Če v komunikacijskem sistemu nimamo overitelja, potem se lahko uporabijo protokoli za izmenjavo ključev osnovani na asimetričnih, simetričnih postopkih ali pa na enosmernih funkcijah brez stranskih vrat (Diffie-Hellmanova eksponentna izmenjava ključev).

5.2.2. Ranljivost konvergenčnih telekomunikacijskih sistemov

Glede na to, da se komunikacije selijo iz tradicionalnih omrežij v omrežja IP, je potrebno poleg zagotavljanja že dolgo znanih tradicionalnih varnostnih mehanizmov (omejevanje zunanjega fizičnega dostopa do internega omrežja, varnost govorne pošte, preprečevanje goljufije, omejevanje klicanih številk …) zagotoviti tudi ustrezno zaščito pred napadi, ki so specifični za IP okolje. Zato moramo vpeljati nove varnostne storitve, s katerimi bomo lahko zagotavljali podoben nivo varnosti. Nekaj najpomembnejših vidikov je opisanih v naslednjih poglavjih [Bervar_05].

5.2.2.1. Avtentikacija uporabnikov

Identiteta naprav v klasičnih omrežjih je vezana predvsem na fizično povezavo oz. fizični priključek. V omrežjih IP, kjer ni neposredne fizične povezave med napravami, pa je v celoti vezana na neko lastnost naprave (IP naslov, uporabniško ime, geslo, javni ključ …), s katero se le-ta identificira. To pomeni, da je v omrežjih IP identiteta naprav popolnoma mobilna. Napravo (SIP telefon ali uporabniška aplikacija) lahko premaknemo v drugo sobo ali na drug konec sveta, pa bo uporabnik še vedno na popolnoma enak način uspešno dostopal do svojih storitev.

Ta lastnost omogoča napad na krajo identitete. To npr. lahko pomeni, da nekdo ukrade telefon, ga priključi na drugi lokaciji in uporablja vse storitve v imenu lastnika telefona. Drugi vidik kraje identitete so aktivni in pasivni napadi na protokole in elemente overjanja (IP naslov, globalno enoličen naslov za identifikacijo naprav na drugem nivoju OSI referenčnega modela (MAC naslov – *Media Access Control address*), uporabniško ime, geslo …). Zelo pomembno je, da so ti elementi čim močnejši, da jih potencialni napadalci ne morejo pridobiti na preprost način. Najboljša je uporaba infrastrukture javnih ključev s podporo sistema za upravljanje s certifikati (PKI – *Public Key Infrastructure*).

Za preprečevanje kraje identitete je potrebno poskrbeti za:

- ***fizično varovanje naprav***, ki vsebujejo elemente overjanja;
- ***močno aplikacijsko overjanje*** med samimi elementi sistema (npr. uporaba javnih ključev);
- ***alternativno overjanje*** na omrežnem sloju (npr. uporaba varnostnega internetnega protokola (IPSec – *Internet Protocol Security*)) za protokole s šibkim ali neobstoječim overjanjem na aplikacijskem sloju;
- ***opcijsko dodatno overjanje*** posameznih uporabnikov ali celo posameznih klicev (npr. vnos gesla ali osebne identifikacijske številke (PIN – *Personal Identification Number*)).

5.2.2.2. Prenosna infrastruktura

V klasičnih omrežjih so povezave med posameznimi elementi (centralami) večinoma neposredne in fizične. V omrežjih IP pa fizične povezave nadomesti poljubno kompleksno omrežje, ki ni več sestavljeno samo iz fizičnih povezav, temveč tudi iz raznih stikal, usmerjevalnikov, prehodov, požarnih zidov itd., ki ustvarjajo prenosno infrastrukturo.

Te naprave pogosto nudijo cel nabor storitev in možnost inteligentnega upravljanja, kar predstavlja vabljivo tarčo za napadalce. Če napadalcu uspe pridobiti nadzor nad napravo ali delom prenosne infrastrukture, lahko v večini primerov poljubno prestreza in usmerja omrežni promet. S tem lahko nepooblaščeno prisluškuje, snema in spreminja komunikacijske tokove, pooseblja legitimne uporabnike, krade storitve, ovira in prekinja delovanje sistema. Med napadi omenimo:

1. ***Napade na drugem nivoju*** OSI referenčnega modela: preusmerjanje prometa s pomočjo ponarejanja MAC naslovov ali ponarejanja odgovorov protokola za prevedbo naslovov (ARP – *Address Resolution Protocol*), manipulacije protokola vpetega drevesa (angl. *spanning tree*), zasipavanje tabel preklapljanja v stikalih z velikim številom MAC naslovov itd.

2. ***Napade na tretjem nivoju*** OSI referenčnega modela: preusmerjanje prometa s pomočjo izvornega IP usmerjanja (angl. *source routing*), ponarejanje usmerjevalnih informacij v usmerjevalnih protokolih ali preko preusmeritev sporočil internetnega krmilnega protokola (ICMP – *Internet Control Message Protocol*), poosebljanje DHCP strežnika itd.

Za preprečevanje napadov na prenosno infrastrukturo je potrebno:

- ***uporabiti šifrirne postopke*** za zaščito sej med končnimi točkami (npr. uporaba varnega protokola za prenos v realnem času (SRTP – *Secure RTP*), uporaba SCCP protokola na osnovi sloja varnih vtičnic (SCCPS – *SCCP over SSL*) ali uporaba IPSec-a) in med elementi omrežja (uporaba IPSec-a);
- ***uporabiti ustrezne infrastrukturne naprave***, ki omogočajo varen način upravljanja;

- ***uporabiti ustrezne mehanizme usmerjanja*** (avtentikacija in filtriranje vseh usmerjevalnih informacij, dinamično ustvarjanje filtrov za vse informacije in pakete, ki prihajajo od sumljivih izvorov, prepoved izvornega usmerjanja);
- ***uporabiti napredne varnostne mehanizme*** omrežja IP (pregledovanje ARP paketov, nadzor nad izvornimi IP in MAC naslovi priključenih naprav, pregledovanje DHCP paketov);
- ***razdeliti omrežje in nadzor dostopa*** na posamezne enote (uporaba virtualnih omrežij za različne vrste prometa – npr. signalizacija, nadzor in upravljanje, tarifiranje …)

5.2.2.3. Dostopnost

Zelo pomemben je tudi vidik dostopnosti, kajti s prehodom v omrežje IP se le-ta izredno poveča. Na prvem mestu se poveča fizična dostopnost, ki zahteva napadalčevo prisotnost ob samem omrežnem priključku, kot tudi virtualna, ki omogoča dostop iz ostalih omrežij, ki so z njim posredno ali neposredno povezana.

Prav tako je zanimivo tudi dejstvo, da ima dandanes pravzaprav že skoraj vsaka naprava implementiran protokol IP, kar pomeni, da vse te naprave, priključene v omrežje, lahko komunicirajo druga z drugo. To pa seveda, v nasprotju s klasičnim sistemom, močno povečuje število možnih tarč in načinov vdora.

Prvo obrambno črto ponavadi predstavljajo stikala, s pomočjo katerih lahko klasificiramo ves IP promet. Tako ločujemo podatkovni promet od govornega ter preprečimo dostop napadalcev do govornega omrežja. Žal pa je mogoče trenutno uporabljene mehanizme dovolj enostavno zaobiti, vendar so ti še vedno koristni za preprečevanje naključnih napadov ter odvračanje manj sposobnih napadalcev.

Za omejevanje dostopa lahko uporabimo:

- osnovno avtentikacijo med napravo in stikalom (npr. Ciscov protokol odkrivanja omrežja (CDP – *Cisco Discovery Protocol*));
- avtentikacijo in šifriranje seje med napravo in stikalom;
- virtualna omrežja (npr. signalizacija, nadzor in upravljanje, tarifiranje …);

- striktno filtriranje prometa med in v posameznih virtualnih omrežjih (npr. uporaba seznama za kontrolo dostopa (ACL – *Access Control List*), požarnih zidov, seznamov dostopa v stikalih itd.).

5.2.2.4. Zapora strežbe

Največkrat si vsi različni tipi prometa, ki potujejo po omrežju IP, delijo isto fizično infrastrukturo. Prav zaradi tega je potrebno poskrbeti, da dogodki znotraj enega virtualnega omrežja čim manj vplivajo na delovanje ostalih virtualnih omrežij. Tako naj izbruh virusa v podatkovnem podomrežju ne bi vplival na delovanje govornega omrežja. Lahko pa napadalec uspe pridobiti dostop do enega virtualnega omrežja ter z zasipavanjem s paketi moti ali celo prekine delovanje storitev.

Za preprečevanje napadov, ki imajo za posledico zaporo strežbe lahko uporabimo:

- osnovno zaščito kakovosti storitev z logično izolacijo posameznih tipov omrežij in z ustreznimi mehanizmi kakovosti storitev;
- način zagotavljanja najmanjše in omejevanje največje dovoljene pasovne širine za posamezen tip prometa, posamezno napravo ali aplikacijo znotraj vsakega posameznega virtualnega omrežja.

5.2.2.5. Ranljivost naprav in ostalih elementov sistema

V IP telefoniji so naprave, terminali oz. telefoni precej kompleksnejši kot v klasičnih sistemih, saj nudijo in morajo dostopati do precej bolj zapletenih storitev. Tako lahko taka naprava vsebuje strežniške aplikacije, ki odgovarjajo na zahteve protokola HTTP, preprostega protokola za upravljanje omrežij (SNMP – *Simple Network Management Protocol*), protokola FTP itd. To pa omogoča napadalcem napad na programsko opremo naprave. Če napadalcu uspe prevzeti telefon, ga lahko uporabi za snemanje ali spreminjanje pogovorov ter njegovo poosebljanje.

Prav tako kot naprave, so tudi ostali elementi takega sistema precej kompleksni in izredno ranljivi. Njihova ranljivost je v večini posledica dejstva, da delujejo na platformah za splošno uporabo (npr. Windows, UNIX, Linux …), ki v mnogih primerih

niso optimalne za nalogo, ki naj bi jo opravljale, saj nudijo preveč nepotrebnih storitev, v katerih napadalec pogosto najde napake, s katerimi si pomaga pri napadu.

Za preprečevanje napadov na naprave in ostale elemente sistema lahko:

- izklopimo vse funkcije naprave in elementov sistema, ki jih ne potrebujemo;
- uporabimo močno avtentikacijo in omejujemo dostop do storitev naprave in ostalih elementov;
- natančno nadziramo promet, ki ga naprava sprejme iz zaupanja nevrednih omrežij;
- uporabljamo čim preprostejše in namenske elemente in platforme, seveda če nudijo ustrezne varnostne mehanizme;
- sistem opremimo z dodatnimi varnostnimi mehanizmi (lahko tudi lastnimi);
- uvedemo striktno in poglobljeno omrežno filtriranje, na podlagi katerega lahko ustavimo napade, še preden pridejo do končnih uporabnikov.

5.2.3. Načini za povečevanje varnosti

Preden se dejansko začnemo odločati kateri način ali načine bomo uporabili za povečevanje varnosti v svojem sistemu, si moramo odgovoriti na nekaj zelo pomembnih vprašanj:

- kako je sistem lahko ogrožen in kdo ga lahko ogroža,
- kako in v kolikšni meri je za poslovanje pomembna odprtost sistema do drugih omrežij oz. javnega omrežja,
- koliko so vredni podatki, ki jih želimo zaščititi,
- kolikšno škodo lahko povzročijo napadalci,
- kolikšne stroške bi imeli z uvedbo ustreznih zaščitnih ukrepov.

Na osnovi zelo natančne analize lahko izdelamo varnostno politiko, ki določa:

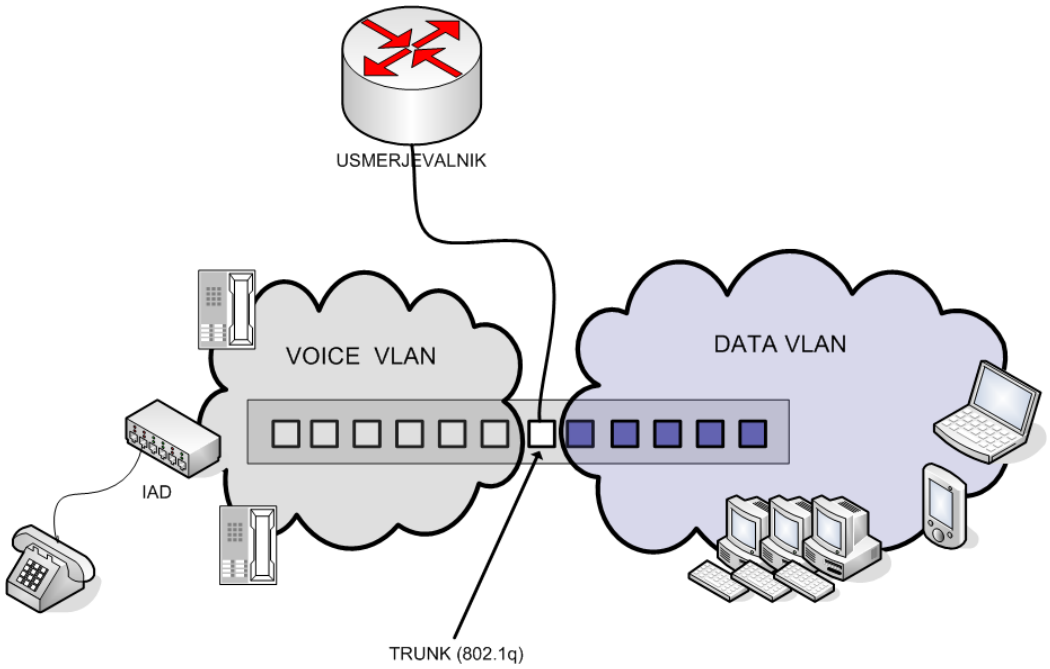
- kateri deli sistema so najbolj vitalni in jih je potrebno tudi najbolje zaščititi,
- kateri uporabniki sistema imajo pravico dostopa do drugih omrežij in kakšne so te pravice,
- kateri uporabniki iz drugih omrežij imajo pravico dostopa in kakšne so te pravice,

- katere zaščitne ukrepe bomo uporabili (ločitev podomrežij, protivirusna zaščita, omrežno prenaslavljanje, enkripcija …) in
- določiti pravila obnašanja uporabnikov sistema.

Seveda moramo paziti, da stroški vzpostavljanja varnosti ne presežejo potencialne škode, ki bi nastala ob vdoru v sistem.

5.2.3.1. Uporaba virtualnih lokalnih omrežij

Z vidika varnosti in zagotavljanja kakovosti storitev bi bila najboljša rešitev striktna ločitev vseh različnih vrst prometa (npr. podatkovni, govorni, signalizacijski itd.). To bi seveda pomenilo več različnih, fizično ločenih omrežij, kar pa po drugi strani odstopa od ključnih vodil uvajanja novodobnih storitev in konvergenčnih omrežij. Najučinkovitejši pristop zato predstavlja logična delitev oz. segmentacija na drugem nivoju OSI referenčnega modela, t.j. vpeljava navideznih lokalnih omrežij (VLAN – *Virtual Local Area Network*).



Slika 19: Logična segmentacija znotraj stikala

Tehnologija VLAN omogoča učinkovit način združevanja in segmentacije omrežij na logičnem nivoju, ne glede na fizično priključitev naprav. V kolikor je zahtevano prehajanje paketov ali sporočil med različnimi segmenti VLAN-a oz. med različnimi

virtualnimi omrežji, je potrebno prečkanje naprave na tretjem nivoju OSI referenčnega modela. To je usmerjevalnik, ki segmentom zagotavlja ustrezno povezljivost, hkrati pa izvaja filtriranje in kontrolo dostopa nad posredovanimi paketi.

Prisotnost velike količine omrežnih aktivnosti tipov razpršenega (angl. *broadcast*) oz. usmerjenega (angl. *multicast*) oddajanja utegne opazno znižati zagotovljeno raven kakovosti storitve. Velikost domen oddajanja neposredno vpliva na povečanje zakasnitev in trepetanja, dvoje ključnih povzročiteljev zmanjšanja kvalitete storitev. Mehanizem VLAN s funkcionalnostjo zmanjševanja domen oddajanja znatno pripomore k optimizaciji omrežja.

5.2.3.2. Varnostni internetni protokol (IPSec)

Enostavnost prisluškovanja podatkom predstavlja glavni razlog za uporabo tehnik šifriranja. Z željo, da bi v ta namen uporabili že razvite, standardizirane in dobro sprejete pristope za ščitenje podatkov v konvergenčnih omrežjih, se poskuša uporabiti mehanizem varnostnega internetnega protokola (IPSec – *IP Security*, RFC 2401 do RFC 2411), ki ščiti omrežni nivo OSI referenčnega modela. Nanaša se na omrežne varnostne storitve, kot so avtentikacija, celovitost, zavračanje ponovljenih podatkov oz. paketov in tajnost, ter za njihovo skrb definira potrebna orodja. Hkrati IPSec definira tudi okvir za šifriranje podatkov, s čimer zagotovi, da prisluškovalci ne razumejo informacij, ki se prenašajo v paketih. IPSec se lahko uporablja za zavarovanje ene ali večih poti med parom uporabnikov, parom usmerjevalnikov ali požarnih pregrad, ali pa med usmerjevalnikom (požarno pregrado) in uporabnikom [SecCon_05].

Za zagotavljanje varnosti pri prenosu podatkov IPSec uporablja dva protokola:

- protokol avtentikacijske glave (AH – *Authentication Header*), definiran v RFC 2402 in
- protokol varovanja koristne vsebine z inkapsulacijo (ovojnico) (ESP – *Encapsulating Security Payload*), definiran v RFC 2406.

Protokol AH zagotavlja nepovezavno (v smislu nepovezavne komunikacije) celovitost, avtentikacijo izvora podatkov in storitev vračanja ponovljenih podatkov, ki pa je izbirna oz. ni obvezna.

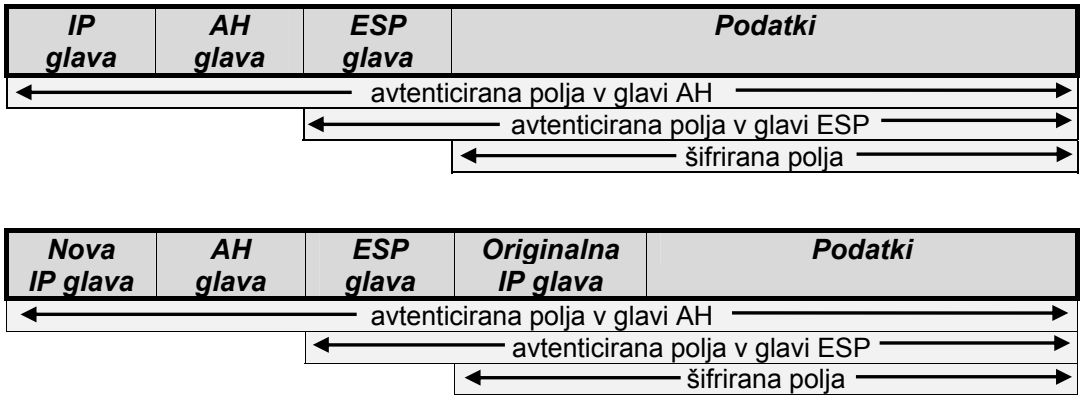
Protokol ESP pa lahko zagotavlja tajnost (s šifriranjem) in omejen pretok zaupnega prometa, hkrati pa tudi nepovezavno celovitost, avtentikacijo izvora podatkov in storitev vračanja ponovljenih podatkov.

Oba protokola, AH in ESP, sta sredstvi za kontrolo dostopa, ki slonita na sistemu izmenjave ključev in opravljanju prometnega pretoka, ki sloni na teh varnostnih protokolih.

Oba protokola podpirata dva načina uporabe IPSec-a in sicer:

- ***transportni način*** (angl. *transport mode*) in
- ***tunelski način*** (angl. *tunnel mode*).

Transportni način šifrira samo podatke višjeležečih nivojev, IP in IPSec glavi pa sta nezaščiteni, zato ju lahko prebere vsak, ki je paket prestregel. To pomeni, da lahko napadalec zbira informacije npr. kdo komunicira s kom in koliko časa. Tunelski način pa odpravlja ravno to pomakljivost, saj šifrira tudi originalen IP naslov in ga zamenja z drugim. Ponavadi je to IP naslov naslednjega vozlišča. Razliko si lahko ogledamo na spodnji sliki [Slika 20].



Slika 20: Transportni in tunelski način protokola IPSec

Uporaba IPSec-a je najprimernejša za povezovanje širšega kroga entitet oz. aplikacij, zato ga največkrat srečamo v izvedbah privatnih virtualnih omrežij (VPN – *Virtual Private Networks*).

Kljub vsemu uporaba mehanizma IPSec prinaša tudi nekaj pomanjkljivosti in nezdružljivosti, saj se IPSec zaradi časa, ki je potreben za šifriranje/dešifriranje podatkov, težko podreja zahtevam za prenos podatkov v realnem času. Pri komunikaciji vnaša zakasnitve, trepetanje in izgube paketov. Eden izmed možnih pristopov za rešitev tega problema je uporaba mehanizmov za kompresijo glav paketov.

1. Zakasnitve šifriranja in dešifriranja

Različni mehanizmi za šifriranje/dešifriranje vnašajo različne stopnje zakasnitve v omrežje. Analize v literaturi so pokazale, da se najhitreje izvaja standard za šifriranje podatkov (DES – *Data Encryption Standard*), medtem ko se šifriranje s trojnim DES-om (3DES – *Triple DES*) in varnim zgoščevalnim algoritmom verzije ena (SHA-1 – *Secure Hash Algorithm*) izvaja znatno počasneje. Pri tem velja opozoriti, da uporaba algoritma DES ni več priporočljiva, ker ga je mogoče enostavno razbiti.

2. Problem razvrščanja in kvalitete storitve šifrirne naprave

Naprava, ki izvaja šifriranje (šifrirnik) navadno predstavlja ozko grlo pri komunikaciji. Za razliko od usmerjevalnikov in požarnih zidov, ki izkoriščajo mehanizme za zagotavljanje QoS na podlagi prioritet paketov, naprave za izvajanje šifriranja teh mehanizmov za razvrščanje paketov navadno ne uporabljajo.

Odsotnost uporabe mehanizmov za zagotavljanje QoS ob uporabi FIFO razvrščanja v čakalne vrste pri šifrirniku paketov lahko povzroči neustrezne zakasnitve in neustrezno varianco zakasnitev, denimo v primeru, ko morajo majhni paketi čakati na izvedbo šifriranja velikih paketov z manjšo prioriteto.

3. Povečanje dolžine paketov

IPSec povečuje velikost paketov, kar predstavlja vzrok za dodatne težave pri zagotavljanju QoS. Razlika v velikosti med nezaščitenimi in zaščitenimi podatki se pojavi na račun dodanih glav: AH oz. ESP glave – v primeru transportnega načina delovanja IPSec-a oz. še celotne IP glave – v primeru tunelskega načina delovanja. Izkaže se, da zaradi povečanja paketov pride do približno 63%

zmanjšanja efektivne kapacitete povezav. Zmanjšanje kapacitete je še dodaten razlog za zakasnitve in trepetanje paketov, ki prečkajo ozka grla v omrežju.

4. Nezdružljivost IPSec-a in naprav NAT

Preštevilčenje popolnoma izniči možnost uporabe IPSec AH mehanizma za ščitenje integritete podatkov, ker se IP naslova pred in za napravo NAT med seboj razlikujeta. Zaradi tega prejemnik ne more preveriti, ali so podatki, ki jih je prejel, resnično takšni, kot jih je pošiljatelj poslal (verifikacija). Iz istega razloga odpove tudi izvajanje avtentikacije pri mehanizmu ESP. Ker avtentikacija in zagotavljanje integritete predstavljata osnovna mehanizma za zagotavljanje varne komunikacije, nezdružljivost predstavlja velik problem. Obstajajo rešitve, ki omogočajo odpravo tega problema: Realm-Specific IP, IPv6 Tunnel Broker, IP Next Layer in UDP inkapsulacija. Področno specifični IP (RSIP – *Realm Specific IP*) predstavlja nadomestilo za NAT in ustvari tunel med uporabnikom in RSIP prehodom. Podpira tako AH kot ESP, njegova implementacija pa je težavna. Najbolj pogosto uporabljena rešitev je UDP inkapsulacija paketov IPSec. To rešitev je sprejel tudi IETF in omogoča, da ves ESP promet prečka napravo NAT: v tunelskem načinu se izvornemu paketu IPSec doda nova glava UDP.

5.2.3.3. Varnost transportnega sloja (TLS)

Varnost transportnega sloja (TLS – *Transport Layer Security*) v nasprotju z IPSec-om skrbi za zaščito transportne ravnine OSI referenčnega modela. Prav tako kot protokol IPSec, protokol TLS zagotavlja varno komunikacijo preko ne varnih povezav in omrežij s pomočjo kriptografije. Tako preprečuje prisluškovanje, ponarejanje sporočil, zagotavlja celovitost, avtentikacijo ter zavračanje ponovljenih sporočil.

Osnova za razvoj protokola TLS je bil sloj varnih vtičnic (SSL – *Secure Socket Layer*) verzije 3. TLS je IETF-ov standard in je bil najprej definiran v RFC 2246, kot TLS protokol verzije 1.0.

TLS je sestavljen iz dveh nivojev in sicer iz tako imenovanega "TLS Record" protokola in "TLS Handshake" protokola. "TLS Record" protokol je nižji nivo protokola TLS in leži nad transportnim nivojem, ki je običajno TCP. "TLS Record" protokol zagotavlja varno povezavo in ima dve osnovni lastnosti:

- V primeru zasebne povezave je uporabljen simetrični šifrirni postopek, pri čemer so ključi ustvarjeni izključno za vsako povezavo. Osnova za ustvarjanje ključev sloni na skrivnem podatku, o katerem se strani dogovorita po nekem drugem protokolu, kot je npr. protokol "TLS Handshake".
- V primeru zanesljive povezave prenos sporočil vključuje preverjanje celovitosti sporočil, pri tem se uporabi kodo za avtentikacijo sporočila, ki je še dodatno kodirana (HMAC – *Keyed-Hashing for Message Authentication Code*). Za dodatno kodiranje se uporablja zgoščevalna funkcija, kot je npr. SHA.

Namen protokola "TLS Record" je zajemanje protokolov z višjih nivojev. Eden takih protokolov je "TLS Handshake", ki omogoča avtentikacijo strežnika in uporabnika. Hkrati se tudi dogovorita o šifrirnem algoritmu in uporabljenih ključih, preden aplikacijski protokol začne oddajati oz. sprejemati podatke.

5.2.3.4. Varni protokol za prenos v realnem času (SRTP)

Za izmenjavo medijskih tokov (avdio in video paketi) v realnem času se običajno uporablja protokol RTP. Ker je protokol praktično brez zaščite, je prisluškovanje in preiskovanje zaseženih paketov zelo preprosto. Prav tako manipulacije in ponovno pošiljanje RTP paketov povzročajo motnje pri prenosu in s tem zmanjšujejo kvaliteto storitev. Spreminjanje podatkovnih enot spremljajočega protokola RTCP pa omogoča nepooblaščeno spreminjanje dogovorjene kakovosti storitev in prekinjanje RTP podatkovnega toka [SecCon_05].

Za rešitev navedenih problemov je bil razvit varni protokol za prenos v realnem času (SRTP – *Secure Real Time Protocol*), ki omogoča zaupnost ter avtentikacijo in preprečuje ponovno pošiljanje sporočil v omrežje. S temi mehanizmi ščiti oba protokola (RTP in RTCP). Protokol SRTP je IETF-ov standard (RFC 3711, Marec 2004).

SRTP povzroča relativno majhno povečanje velikosti paketov in je neodvisen od uporabljenega standarda za upravljanje s ključi. Za enkripcijo uporablja napredni standard za šifriranje (AES – *Advanced Encryption Standard*), za izvajanje avtentikacije pa HMAC-SHA1 transformacijo.

Za podporo SRTP-ju je bil razvit protokol za izmenjavo šifrirnih ključev pri internetnih multimedijskih komunikacijah (MIKEY – *Multimedia Internet Keying*). Njegova naloga je upravljanje in nadzor uporabljenih ključev ter njihova distribucija za multimedijske komunikacije v heterogenih sistemih. Podpira posredovanje kriptogtafskih ključev in varnostnih parametrov za enega ali več varnostnih protokolov. Poleg tega ima še naslednje uporabne lastnosti:

- Protokol MIKEY se lahko implementira kot popolnoma neodvisni knjižnični element in se tako lahko zelo enostavno integrira v multimedijske komunikacijske protokole (SIP, H.323 itd.).
- Izmenjava potrebnih inforamcij poteka znotraj dvostranskega rokovanja (angl. *2-way handshake*), kar je verjetno najboljši način za multimedijske scenarije v realnem času.
- Podpira štiri različne distribucije ključev:
  - predhodna izmenjava ključev,
  - uporaba enkripcije na podlagi javnega ključa,
  - izmenjava ključev s pomočjo Diffie-Hellmanovega algoritma ter uporabe enkripcije na podlagi javnega ključa in
  - izmenjava ključev s pomočjo Diffie-Hellmanovega algoritma, uporabe predhodno izmenjanih ključev ter uporabe zgoščevalnih funkcij (DHHMAC).
- Možna menjava ključev znotraj seje.
- Podpora sejam z večimi udeleženci (angl. *multicast support*).

5.2.4. Varnost in protokol SIP

V samem začetku je bil SIP namenjen in definiran za varna okolja in ni imel vgrajenih posebnih varnostnih mehanizmov. S širitvijo uporabe se je kmalu pojavila tudi potreba po zagotavljanju varnosti, kar je bil eden izmed vzrokov za posodobitev starejšega standarda [RFC2543]. Novi standard [RFC3261] tako vsebuje določene rešitve za zaščito pred vohunjenjem in krajami zaupnih podatkov (angl. *espionage, eavesdropping and monitoring*), zaščito pred nedovoljenim dostopom do omrežja (npr. spreminjanje podatkov o vzpostavljenih sejah in posledičnih stroškov), zaščito pred DoS napadom ter zaščito pred sprejemom nepravilno oblikovanih sporočil, ki bi lahko povzročila poplavo sporočil v posameznih elementih konvergenčnega omrežja.

5.2.4.1. Avtentikacija signalnih sporočil

Za avtentikacijo signalnih sporočil se uporablja tako imenovana HTTP avtentikacija na podlagi izvlečka (angl. *HTTP digest authentication*) [RFC2617], ki deluje na preprostem algoritmu izziva in odgovora o katerem smo že govorili. Tako strežnik SIP ob sprejemu zahteve, ki ne vsebuje glave Authorization, izzove končnega uporabnika s sporočilom 401 (Unauthorized), ki mora obvezno vsebovati glavo WWW-Authenticate. Le-ta naj bi vsebovala naslednje parametre:

- ***realm*** (neko zaporedje znakov, ki končni točki povedo katero uporabniško ime in geslo naj uporabi),
- ***domeno*** (z vejicami ločeno zaporedje zahtevanih URI-jev),
- ***nonce*** (veliko naključno število, ki naj bi bilo enolično ustvarjeno za vsak posamezen izziv),
- ***opaque*** (neko zaporedje znakov, ki jih določi strežnik SIP in jih mora končna točka uporabiti v vseh nadaljnjih zahtevah, ki uporabljajo iste URI-je),
- ***stale*** (zastavica, ki pove, da je bila prejšnja zahteva zavrnjena, ker je bil uporabljen parameter nonce star),
- ***algorithm*** (določa uporabljen algoritem za izvleček, in če ni prisoten, se uporabi MD5; možne variante so: MD5, MD5-sess …)
- ***qop*** (ponazarja kvaliteto varovanja; možne variante so: auth (angl. *authentication*), auth-int (angl. *authentication with integrity protection*) …)

Seveda sta od vseh parametrov obvezna samo realm in nonce, drugi so opcijski. Na podlagi prejetih parametrov končna točka naredi izvleček in odgovori na izziv s ponovitvijo prejšnje zahteve, ki ji mora vključiti glavo Authorization. Ta naj bi vsebovala naslednje parametre, od katerih so prvi trije obvezni, ostali pa opcijski:

- ***username*** (uporabniško ime končne točke),
- ***realm***,
- ***nonce***,
- ***digest-URI*** (URI uporabljen pri izvlečku),
- ***response*** (izvleček, ki ga naredi končna točka),
- ***algorithm*** (uporabljeni algoritem),

- ***cnonce*** (neko zaporedje znakov, ki jih določi končna točka na podlagi prejetega parametra opaque, za zagotavljanje medsebojne avtentikacije in varovanja integritete sporočila),
- ***opaque***,
- ***qop***,
- ***nonce-count*** (števec, ki predstavlja zaporedno številko zahteve, ki jo je poslal pri uporabi istega nonce-a),
- ***auth-parm*** (uporaba za podaljške, definirane v prihodnosti).

Za izvleček končna točka uporabi algoritem, ki je bil določen v izzivu. Osnova za izvleček so uporabniško ime, geslo in parameter nonce. Poleg tega pa se uporabijo še opcijski parametri prejeti v izzivu ter še dodatni, ki jih za izračun uporabi končna točka (cnonce, nonce-count).

5.2.4.2. Uporaba varne večnamenske razširitve za elektronsko pošto (S/MIME)

Sporočila SIP lahko prenašajo tudi večnamenske razširitve za elektronsko pošto (MIME – *Multipurpose Internet Mail Extensions*). MIME že sam po sebi zagotavlja mehanizme za zaščito integritete in enkripcijo vsebine. Varna večnamenska razširitev za elektronsko pošto (S/MIME – *Secure/Multipurpose Internet Mail Extensions*), ki jo uporablja SIP, pa omogoča še dodatne mehanizme za povečanje varnosti, kot so izmenjava ključev, avtentikacija, zaščita integritete ter zaupnost signalnih sporočil SIP. S/MIME je mišljen kot zamenjava za uporabo protokola precejšne zasebnosti (PGP – *Pretty Good Privacy*). Za zaščito glav sporočila SIP se lahko uporabi tuneliranje sporočil SIP v MIME telesih, kar pa povečuje dolžino paketov. Zato naj bi se uporabljal protokol TCP, na podlagi katerega se lahko izognemo problemu fragmentacije paketov UDP [SecCon_05].

S/MIME zahteva uporabo certifikatov in privatnih ključev, kjer naj bi certifikate izdajala zaupanja vredna tretja oseba imenovana CA.

5.2.4.3. Zaupnost medijskih tokov

SIP sam po sebi ne obravnava šifriranja medijskih tokov, zato se lahko uporablja šifriranje RTP paketov, definirano v RFC 1889 ali pa se uporabi protokol SRTP. Za nadzor in upravljanje ključev se lahko uporabi protokol SDP [RFC2327], ki lahko prenese potrebne ključe za vzpostavitev šifrirane seje. Vendar moramo upoštevati dejstvo, da samo z uporabo SDP-ja ne moremo varno prenesti šifrirnih ključev. To je možno samo v primeru, da se že sama SIP zahteva šifrira, po možnosti od enega do drugega konca (angl. *end to end*).

Lahko pa se v ta namen uporabi tudi protokol MIKEY, ki je bil razvit za podporo protokola SRTP. Njegova osnovna naloga pa je prav varna izmenjava kriptografskih ključev.

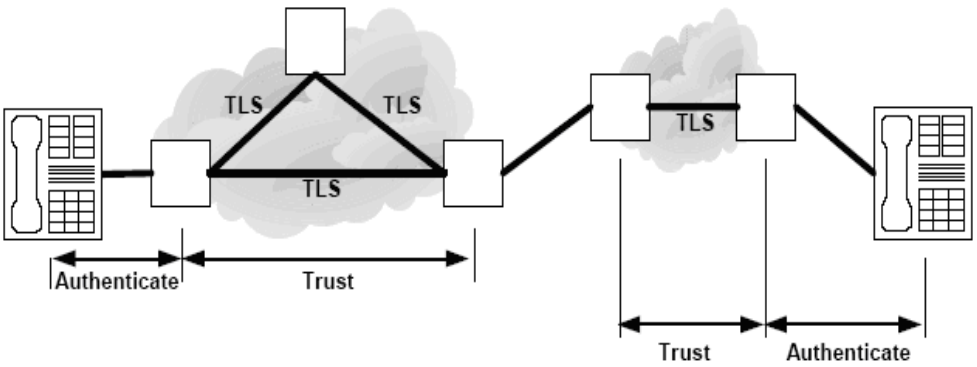
5.2.4.4. Uporaba protokola TLS

Uveljavitev zasebnosti med končnima entitetama ni prioritizirana zgolj za zaščito izmenjanih interaktivnih vsebin (govor, datoteke, sporočila, video …), enako pomembna je storitev zaščite signalizacijskih sporočil. Identiteta kličočega in klicanega, vsebovana v signalizacijskem sporočilu, mora ostati zakrita pred prisluškovalci, kar narekuje vpeljavo kriptografskih mehanizmov med entitetami kontrolne ravnine. V praksi se je za potrebe zaščite poti med odjemalcem ter korenskemu klicnemu strežniku oz. poti med sosednimi klicnimi strežniki uveljavil protokol TLS.

Osnovni SIP standard [RFC3261] za SIP proksi, preusmeritvene, registracijske ter B2BUA strežnike, nekako določa obvezno uporabo TLS-a. Za same uporabniške agente pa je samo priporočljiv. S pomočjo TLS-ja je mogoče popolnoma zagotoviti celovitost sporočil SIP, uporaben pa je tudi za odkrivanje ponovitev le-teh. Integrirano ima tudi upravljanje in nadzor ključev ter njihovo varno distribucijo.

Protokol ima dva možna modela uporabe:

- ***točka – točka*** (angl. *end to end*) in
- ***od vozlišča do vozlišča*** (angl. *hop by hop*) [Slika 21].



Slika 21: Primer modela TLS od vozlišča do vozlišča

Kot je razvidno že iz samega imena, koncept točka – točka nudi celovitost izmenjanih vsebin od pošiljatelja do prejemnika, medtem ko druga metoda pokriva zgolj zaščito med posameznimi vozlišči v omrežju. Vozlišča v konvergenčnih omrežjih predstavljajo klicni strežniki (vse možne variante SIP proksi strežnikov, nadzornikov medijskih prehodov (MGC – *Media Gateway Control Protocol*) in H.323 vratarjev). Prednost slednjega modela je predvsem v razbremenitvi končnih terminalov z vidika zahtevanih zmogljivosti, vendar ta model narekuje visoko stopnjo zaupanja v omrežno infrastrukturo samega operaterja, saj je največkrat v njegovi lasti tudi celotna infrastruktura javnih ključev (PKI).

V kolikor je zahtevana zgolj avtentikacija klicnih strežnikov, zadostuje namestitev podpisanih digitalnih potrdil na strežnikih. Dodatno overjanje uporabniških agentov pa narekuje zmogljive in ustrezno podprte uporabniške terminale.

Poleg tega je potrebno omeniti še dejstvo, da je pri uporabi protokola TLS nujno potreben zanesljiv prenos, kar pomeni uporabo protokola TCP. Protokol UDP se za prenos sporočil SIP v povezavi z TLS-jem tako ne more več uporabljati. Vendar se pri uporabi TLS-ja ne spremeni samo uporabljeni protokol transportnega nivoja, ampak tudi način naslavljanja komunikacijskih elementov. Tako se namesto SIP URI-ja uporabi SIPS URI, ki se sedaj začne s "sips: ".

5.2.4.5. Uporaba protokola IPSec

Prav tako se za zagotavljanje varnosti lahko uporabi protokol IPSec, ki ščiti signalizacijo na omrežnem nivoju. Tak način zaščite je najprimernejši za varovanje SIP naročnikov znotraj SIP VPN scenarija (UA – SIP proksi strežnik) ali med

različnimi administrativnimi SIP domenami. Deluje pa, za razliko od protokola TLS, ne glede na uporabljeni transportni nivo (UDP, TCP ali SCTP). Uporablja se za zagotovitev celovitosti sporočil in tako kot TLS podpira model točka – točka in model od vozlišča do vozlišča.

Poudariti moramo, da osnovno SIP priporočilo ne določa niti samega ogrodja, kako naj bi se IPSec uporabljal. Prav tako ne določa nobene zahteve, kako naj bi potekala upravljanje in nadzor ključev, katere IPSec glave in kateri način naj bi se uporabili. Sprejemljiv protokol za upravljanje in nadzor ključev je hibridni internetni protokol za izmenjavo ključev (IKE – *Internet Key Exchange*), ki je osnovan na internetnem varnostnem protokolu za povezovanje in upravljanje s šifrirnimi ključi (ISAKMP – *Internet Security Association and Key Management Protocol*), varnem protokolu za izmenjavo šifrirnih ključev v internetu (SKEME – *Secure Key Exchange Mechanism for the Internet*) in Oakleyjevem protokolu za določanje šifrirnih ključev (OKDP – *Oakley Key Determination Protocol*, RFC 2412). Zagotavlja namreč avtomatsko izmenjavo kriptografskih ključev in njihov nadzor ter upravljanje. Protokol IKE se tako uporabi najprej za dogovor o potrebnih varnostnih elementih znotraj samega nadzora in upravljanja ključev (prva faza), kot tudi za druge storitve, kot je npr. IPSec (druga faza). Protokol IKE se uporablja zlasti pri vzpostavitvi VPN-a.

5.2.4.6. Novi osnutki

Trenutno se znotraj IETF-a pojavljajo različni osnutki v smislu povečevanja osnovnih varnostnih rešitev protokola SIP. Nanašajo se na zagotavljanje celovitosti sporočil in medijskih tokov. Najpomembnejši osnutki so [SecCon_05]:

- ***SIP Authenticated Identity Body*** (AIB, draft-ietf-sip-authid-body-02) – določa splošen SIP avtentikacijski žeton, njegovo strukturo in format, ki se kot S/MIME telo doda vsaki SIP zahtevi in odzivu. To telo, imenovano AIB, pravzaprav vsebuje digitalni podpis celotnega ali samo dela sporočila SIP.
- ***SIP Authentication Identity Management*** (draft-ietf-sip-identity-01) – prav tako določa nek SIP avtentikacijski žeton, njegovo strukturo in format, ki naj bi se dodajal SIP zahtevam, zaradi izmenjave kriptografsko varnih in avtenticiranih identitet končnih točk. Vzrok za to je dejstvo, da trenutni mehanizmi za izražanje

identitete administrativnim domenam velikokrat ne dovoljujejo ali ne omogočajo preverjanja identitete pošiljatelja zahteve.

- ***S/MIME AES zahteva za SIP*** – določa namesto 3DES algoritma, kot ga določa osnovno priporočilo [RFC3261], izboljšan AES algoritem. Njegova prednost je v hitrosti, saj matematično ni tako zahteven kot 3DES in zato ne zahteva toliko dinamičnega spomina.
- ***Dogovor o uporabi varnostnega mehanizma*** – protokol SIP trenutno podpira pet različnih varnostnih mehanizmov (TLS, HTTP digest avtentikacija, IPSec z IKE, IPSec brez IKE in S/MIME). Na žalost osnovno priporočilo [RFC3261] ne določa nobenega mehanizma, ki bi opisoval, kako naj se dve končni točki dogovorita, kateri izmed vseh varnostnih mehanizmov bi jima najbolje ustrezal. Nato pa dogovorjeni mehanizem tudi uporabita. Res je, da bi se lahko uporabil mehanizem za povpraševanje po zmožnostih (OPTIONS), vendar je preveč ranljiv za tako vrsto uporabe, saj bi lahko nekdo tretji (man-in-the-middle napad) prepričal obe končni točki, da obe strani podpirata samo najšibkejše mehanizme. Zaradi te velike pomanjkljivosti je IETF izdal priporočilo RFC 3329, ki določa tri dodatne glave, na podlagi katerih se uporabniški agent in strežnik SIP dogovorita, kateri varnostni mehanizem bosta uporabljala.

5.3. Prehod preko naprav NAT

Do nedavnega se na področju vpeljave konvergenčnih omrežij nadzoru dostopa ni posvečalo posebne pozornosti. Razlog za to tiči v dejstvu, da so se za vpeljavo odločala predvsem podjetja z že vpeljano varnostno in požarno politiko, ki neavtoriziranim entitetam omejuje dostop do virov varovanega omrežja oz. dovoljuje dostop legitimnih uporabnikov do izbranih storitev omrežja internet. Tako se je večji delež govornega prometa zaključeval v lokalnih omrežnih segmentih, pri katerih za zaupnost in zanesljivost prenosa v veliki meri poskrbi že sama fizična topologija omrežja. Varnostne naprave na robu lokalnih omrežjih v večini implementacij izvajajo prenaslavljanje omrežnih naslovov (NAT – *Network Address Translation*). Mehanizem na nivoju logičnega naslavljanja omogoča dodatno ločitev varovanega omrežnega segmenta od zunanjega. Izkaže se, da vpeljava govornih komunikacij narekuje nezanemarljiv poseg v varnostno omrežno infrastrukturo, saj obstoječi

varnostni mehanizmi niso bili načrtovani za prenos govora preko protokola IP [NATtra_05].

Problematika naslavljanja naprav za prehodi NAT je poleg protokola SIP karakteristična tudi vsem drugim obstoječim signalizacijskim postopkom VoIP-a (MGCP, H.323, Skinny).

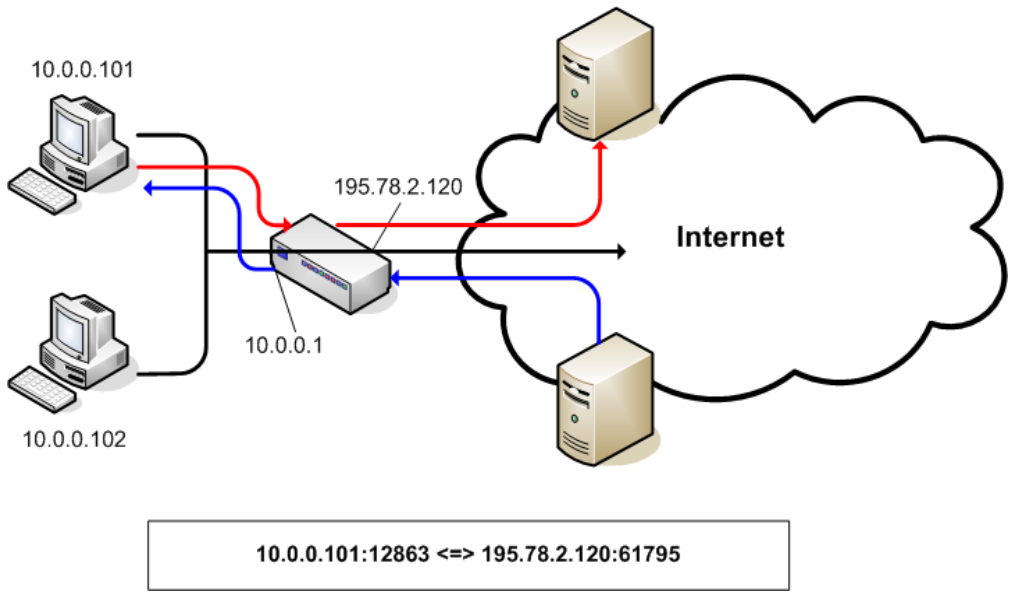
5.3.1. Vrste mehanizmov NAT

Mehanizem NAT je bil vpeljan z namenom razrešitve razpoložljivega naslovnega prostora v protokolu IPv4. Primer: podjetje ima zakupljenih nekaj javnih IP naslovov, število računalnikov, ki želijo komunicirati z javnim omrežjem pa je precej večje. Lahko pa nek posameznik, ki ima xDSL povezavo in en javni IP naslov, želi z internetom povezati več računalnikov. V takih primerih je NAT rešil problem z mapiranjem privatnih parov IP/vrata (naslovni prostor IP – RFC 1918) v javne in s tem omogočil povezljivost z vsemi drugimi napravami, priključenimi v javno omrežje.

Naprave NAT se med seboj razlikujejo glede na tehnike mapiranj privatnih naslovnih parov IP/vrata (varovana cona) z javnimi (internetna cona). V osnovi je razdelitev sledeča:

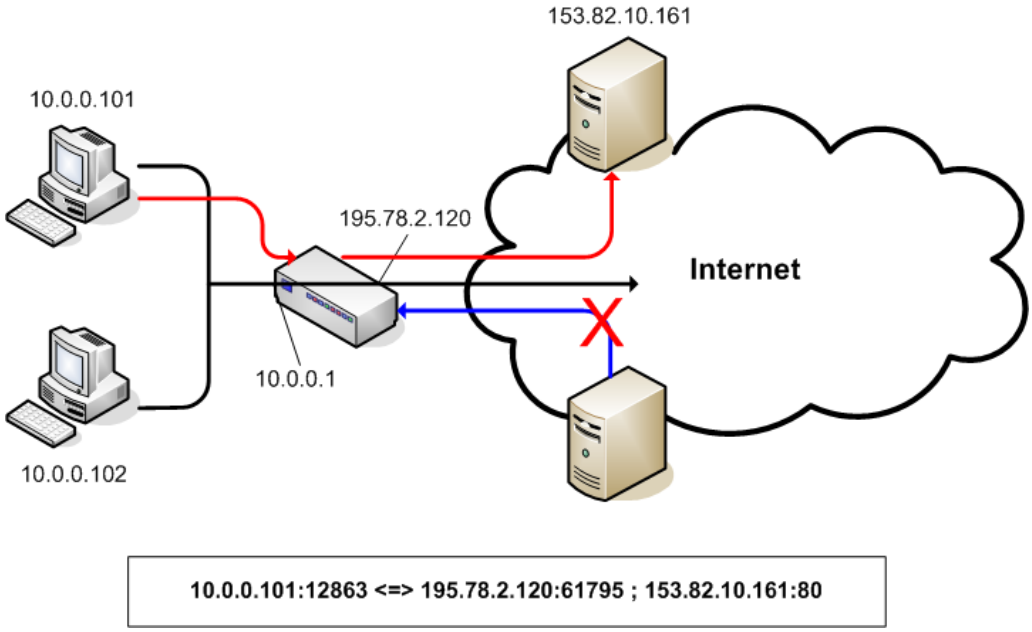
- ***Osnovni NAT*** – preslikovalna tabela NAT vsebuje vnos, ki povezuje privatni IP naslov naprave z javnim IP naslovom naprave NAT. Številka vrat ostane po prehodu naprave NAT nespremenjena.

- ***NAT v obliki stožca*** (angl. *full cone*) – mehanizem priredi privatnemu paru IP/vrata ustrezni par na javni strani naprave NAT. Iz javnega omrežja se na ustrezen terminal za napravo NAT prenesejo vsi prejeti paketi, ki ustrezajo vnosu v preslikovalni tabeli.



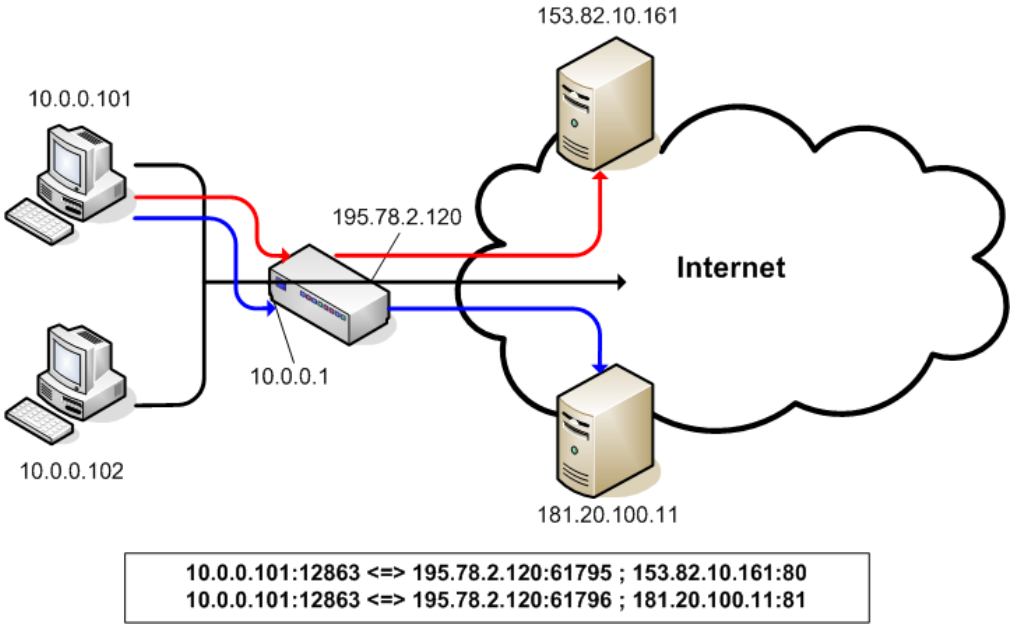
Slika 22: NAT v obliki stožca

- ***NAT v obliki stožca z omejevanjem vrat*** (angl. *port restricted cone*) – funkcionalnost mehanizma je identična zgornjemu opisu z dodatnim varnostnim ukrepom. Na notranjo stran naprave NAT se posredujejo zgolj paketi, ki ustrezajo predhodno vzpostavljenim zvezam. Izvorni naslov glave prejetega paketa se mora na ta način ujemati s ciljnim naslovom glave paketa, ki je vpisan v preslikovalni tabeli.



Slika 23: NAT v obliki stožca z omejevanjem vrat

- ***simetrični NAT*** – predhodne izvedbe mehanizma NAT vsakemu privatnemu paru IP/vrata dodelijo isti javni par. Simetrični NAT pa, v nasprotju s prej opisanimi mehanizmi, vsakemu posameznemu cilju priredi enolični javni par IP/vrata. Privatnim parom IP/vrata lahko na tak način pripada več javnih parov IP/vrata za vse vzpostavljene zveze. V tem primeru lahko znotraj privatnega omrežja več naprav uporablja isti javni par IP/vrata.



Slika 24: Simetrični NAT

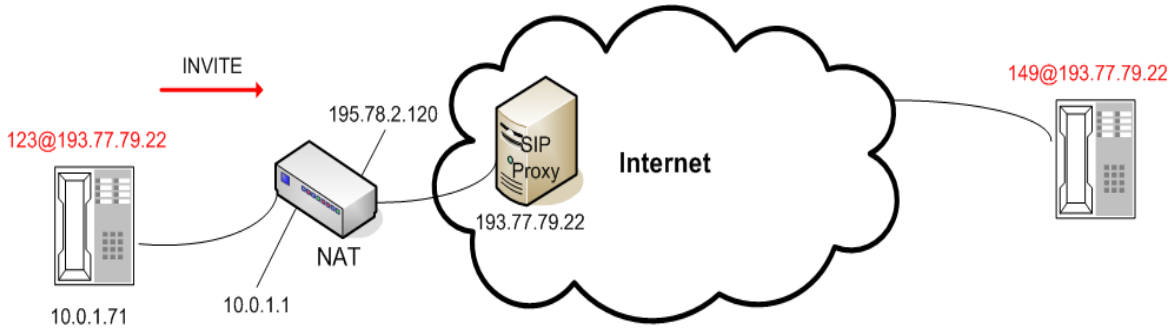
5.3.2. Vplivi NAT-a na protokol SIP

Sama narava protokola SIP zahteva komunikacijo med končnimi točkami na aplikacijskem nivoju. Upoštevati moramo, da je za uspešno vzpostavitev seje predhodno nujno potrebna signalizacija. Z njeno pomočjo se med končnima točkama prenesejo potrebne informacije za vzpostavitev seje. To v končni fazi pomeni, da moramo poskrbeti, da se bosta preko naprave NAT lahko prenašala tako signalizacija kot tudi različni mediji.

Signalizacijsko sporočilo v glavi nosi informacijo o naslovu (IP/vrata), na katerem je entiteta dosegljiva. V kolikor se končna točka nahaja za varnostno napravo NAT, pot do nje z naslovom IP vsebovanim v sporočilu SIP zunanjim entitetam ni poznana. Problematiko prečkanja vmesnih naprav prikazujeta [Slika 25] in [Slika 26], kjer je uporabniški agent SIP lociran za napravo NAT.

```
Session Initiation Protocol
    Request-Line: INVITE sip:149@193.77.79.22 user=phone SIP/2.0
        Method: INVITE
        Resent Packet: False
    Message Header
        Via: SIP/2.0/UDP 10.0.1.71:7244
        Max-Forwards: 70
        From: "123@193.77.79.22" <sip:123@193.77.79.22>;tag=1e2911f98b6e45cb9caf1dd9fe779b55;epid=5722bbe1f7
            SIP Display info: "123@193.77.79.22"
            SIP from address: sip:123@193.77.79.22
            SIP tag: 1e2911f98b6e45cb9caf1dd9fe779b55
        To: <sip:149@193.77.79.22;user=phone>
            SIP to address: sip:149@193.77.79.22
        Call-ID: 6896150e41bf4a35b605f1111e9c74b2
        CSeq: 1 INVITE
        Contact: <sip:10.0.1.71:7244>
        User-Agent: RTC/1.3
        Content-Type: application/sdp
        Content-Length: 440
```

Slika 25: Primer sporočila INVITE za napravo NAT



Slika 26: Primer uporabniškega agenta SIP za napravo NAT

Naslovljena entiteta se na zahtevo INVITE odzove z odgovorom na naslov, ki ustreza javnemu naslovu naprave NAT. Takšen odziv je možen, dokler naprava NAT vzdržuje vnos v NAT preslikovalni tabeli. Trajanje posameznega vnosa zavisi od uporabljenega transportnega protokola za prenos signalizacijskih sporočil.

1. Če se za povezavo uporablja TCP, ki je povezavno orientiran transportni protokol, se zapis vzdržuje vse do konca TCP seje.

2. Če se za povezavo uporablja UDP, ki je nepovezavno orientiran transportni protokol, je potrebno frekventno osveževanje aktivne seje (tipični čas trajanja vnosa UDP v NAT preslikovalni tabeli je krajši od ene minute).

Zaradi omenjene problematike ter zahtevane zanesljivosti prenašanih signalizacijskih sporočil, specifikacije razširitev protokola SIP narekujejo uporabo transportnega protokola TCP.

Še kompleksnejšo situacijo predstavlja postavitev, kjer se za napravo NAT nahaja klicana entiteta. Pobudno sporočilo (INVITE) je v tem primeru poslano SIP proksi strežniku, kjer je ciljni uporabniški agent registriran. Strežnik SIP v tem primeru služi posredovanju signalizacijskih sporočil napravam, maskiranih za prehodom NAT, kajti pri registraciji si poleg osnovnih informacij (glava Contact) zabeleži tudi privatni par IP/vrata (npr. Via: SIP/2.0/UDP 10.0.1.71:5060;received=195.78.2.120;rport=12345). Tudi tu je zahtevano vzdrževanje vnosa, ki preslika naslovni par ponorne naprave ter strežnika SIP.

Prehod RTP prometa preko NAT-a predstavlja daleč največji problem, saj v tem primeru nimamo več strežnika SIP, ki bi nam pomagal pri usmerjanju teh paketov. Poleg tega pa uporabniški agenti tako ali tako za vsak klic spremenijo številko vrat.

5.3.3. Možne rešitve pri prehodu NAT-a

V primeru, da se uporabniški agent nahaja za enim izmed prej opisanih prvih treh tipov NAT-a, je rešitev relativno preprosta. Uporabniški agent mora odkriti, kakšna je dejanska preslikava njegovega naslova in potem v nadaljevanju ta naslov uporabljati v opisu SDP. Agent lahko informacijo o dejanski preslikavi zahteva od NAT-a ali od neke druge naprave, ki se nahaja izven NAT-a.

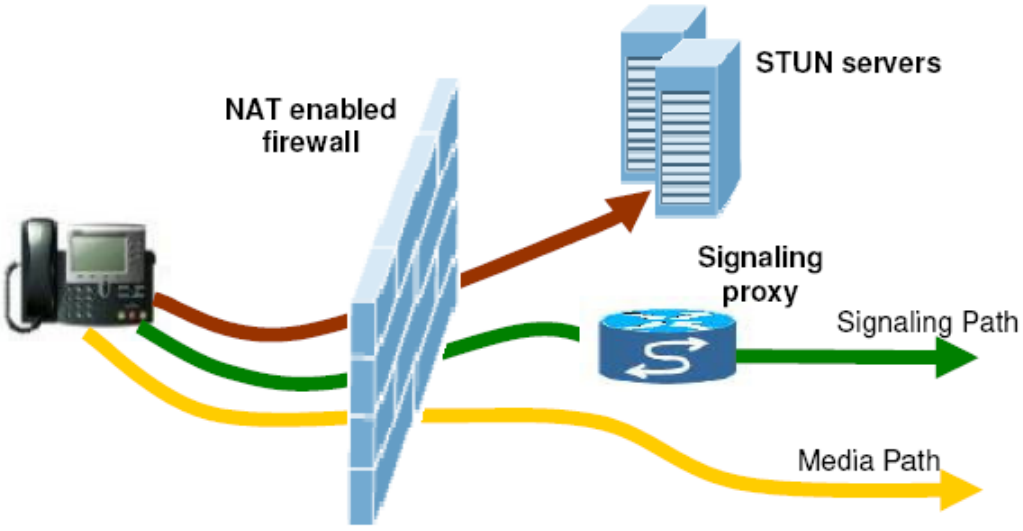
Delovna skupina MIDCOM (članica IETF-a) [IETF] predlaga rešitev navedenih težav z naslednjimi možnimi koncepti:

1. ***Univerzalna arhitektura "vstavi in poženi"*** (UPnP – *Universal Plug and Play*) – gre za rešitev, predlagano s strani korporacije Microsoft. SIP entiteta naslovi poizvedbo po uporabljenemu paru IP/vrata na napravo NAT, ki mora podpirati obravnavano funkcionalnost. Slabosti navedene rešitve so naslednje:
   - mehanizem ne deluje v primeru postavitve naprav NAT v kaskadi,
   - potrebna je nadgradnja obstoječe požarne pregrade (nov firmware),

- specifikacija rešitve ne obravnava varnostne problematike, povezane z implementacijo.

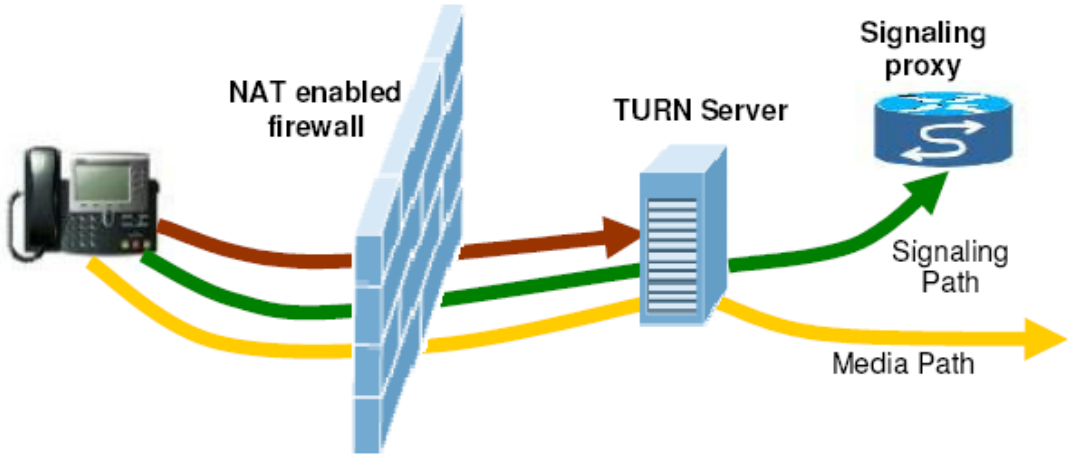
2. ***Zunanja poizvedba*** – gre za rešitev, ko naprava ali naprave NAT nimajo implementirane zgornje funkcionalnosti, zato SIP entiteta določi svoj javni par IP/vrata na podlagi zunanje poizvedbe. Tako pošlje zahtevo neki napravi (npr. sondi) v javnem omrežju. Ta nanj odgovori z informacijo o javnem paru IP/vrata uporabniškega agenta, ki ga sonda prebere iz prejete zahteve. SIP entiteta bo ne glede na število naprav NAT vedno prejela odgovor. Slabosti navedene rešitve so naslednje:
   - mehanizem ne deluje v kombinaciji s simetričnim prehodom NAT – naslovni par IP/vrata se pri simetrični izvedbi mehanizma NAT razlikuje glede na cilj,
   - uporabniški agent mora pošiljati in sprejemati RTP promet preko istih vrat,
   - uporabniški agent mora SIP zahtevo poslati takoj za povpraševanjem, kajti v nasprotnem primeru se lahko medtem njegov javni naslovni par spremeni.

3. ***Simetrični prehod UDP paketov preko naprave NAT*** (STUN – *Symmetric Traversal of UDP Through Network Address Translation*, RFC 3489) – uporaba protokola STUN SIP entiteti omogoči poizvedbo o vrsti naprave NAT, za katero se ta nahaja. Arhitektura STUN vključuje odjemalca STUN, ki se implementira v protokolnem skladu uporabniškega agenta ter strežnik STUN, ki je priključen v javnem internetnem omrežju. Odjemalec s poizvedbo na STUN strežniku pridobi potrebno informacijo o javnem naslovnem paru IP/vrata. Informacija se potem uporabi v glavah sporočil SIP za zamenjavo privatnih naslovnih parov (RFC 1918) z javnimi. Slabosti navedene rešitve so naslednje:
   - mehanizem ne deluje v kombinaciji s simetričnim prehodom NAT,
   - obvezna je nadgradnja programske opreme na strani odjemalca,
   - centralna točka odpovedi, ki jo predstavlja strežnik STUN.



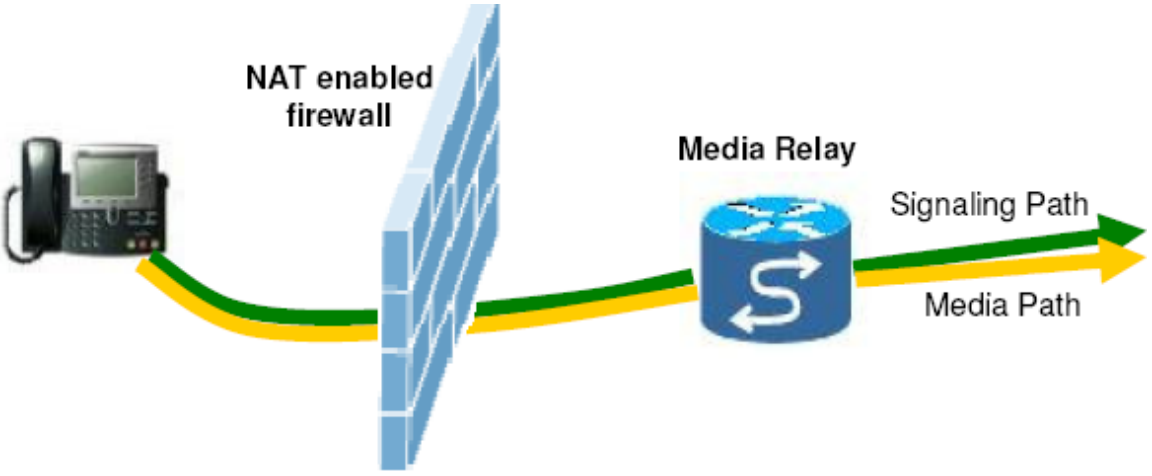
Slika 27: Prikaz mehanizma STUN [NATtra_05]

4. ***Povezavno orientiran medij*** – v primeru simetričnega NAT-a mora uporabniški agent za NAT-om najprej poslati RTP paket drugi strani, potem pa počakati na njen odgovor. Vsaka RTP komunikacija se mora vzpostaviti korak za korakom. To pomeni, da mora uporabnik na drugi strani počakati na prvi RTP paket s strani, ki je za napravo NAT. Šele nato lahko RTP paket pošlje na pravi naslov. Ker pa uporabniški agent B ne ve, kdaj je informacija v opisu SDP pravilna in kdaj ne, mora opis SDP vsebovati atribut ***a=direction:active***. Ta namreč sporoča, da bo stran A RTP sejo vzpostavila aktivno, na podlagi poslanega RTP paketa.
5. ***Simetriči RTP*** – koncept je zelo podoben prejšnemu. Razlikuje se samo v tem, da uporabniški agent vedno ignorira informacijo v opisu SDP in čaka na prvi RTP paket, na katerega tudi odgovori. To je rešitev de-facto, ki jo uporablja Cisco. Velik problem pa nastane, če sta oba uporabniška agenta za NAT-om.
6. ***Prehod s pomočjo vmesnih naprav NAT*** (TURN – *Traversal Using Relay NATs*, draft-rosenberg-midcom-turn-02.txt) – odpravlja pomanjkljivosti protokola STUN, saj omogoča prehajanje simetrične različice mehanizma NAT. Koncept temelji na vpeljavi strežnika TURN, katerega se umesti na poti signalizacijskega in medijskega pretoka.



Slika 28: Prikaz mehanizma TURN [NATtra_05]

7. ***Medijski preklopnik*** – združuje prednosti simetričnega RTP-ja in TURN strežnika. Preklopnik ima to zmožnost, da lahko obema koncema pošlje RTP paket in tako vzpostavi RTP komunikacijo. Če sta oba uporabniška agenta za NAT-om, potem je njegova naloga tudi pravilna preslikava glav RTP paketov. V tem primeru deluje kot B2BUA strežnik.

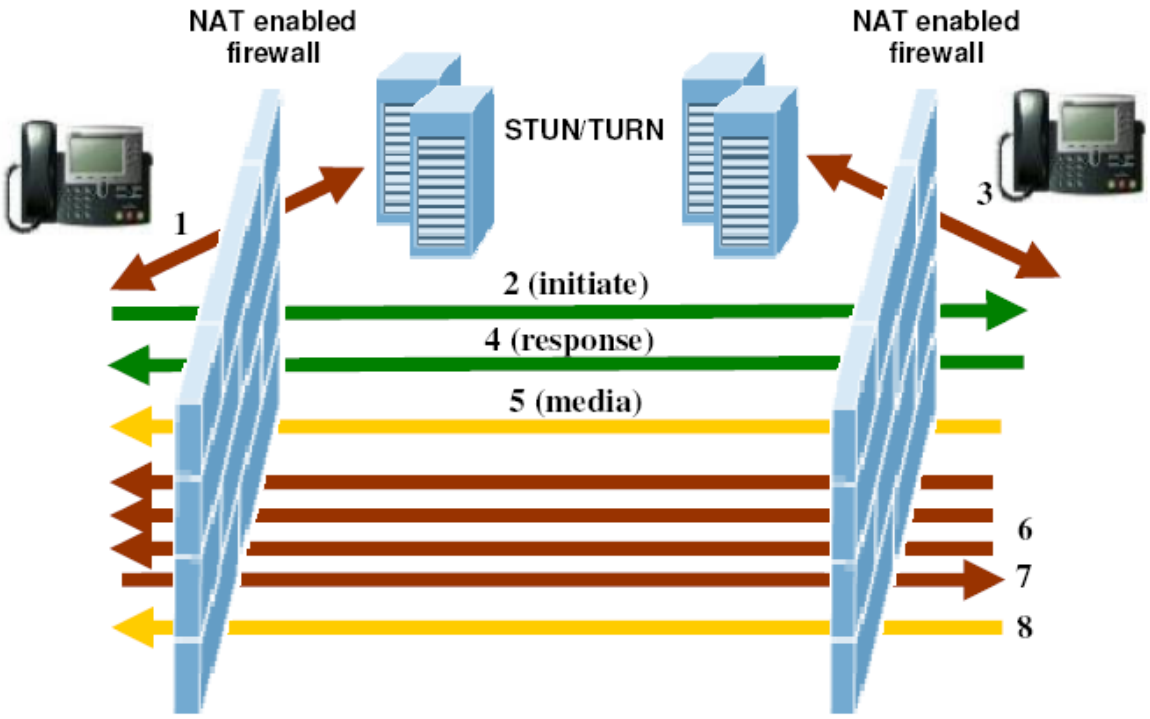


Slika 29: Medijski preklopnik [NATtra_05]

8. ***Področno specifični IP*** (RSIP) – koncept poskuša primankovanje IP naslovov namesto z NAT-om rešiti s t.i. RSIP prehodi, ki opravljajo podobno nalogo kot naprave NAT. Razlikuje se v tem, da namesto dodeljevanja privatnih naslovov najema naslove iz javnega prostora in jih dodeljuje posameznim aplikacijam, t.i. RSIP odjemalcem. Slabost koncepta je v tem, da mora RSIP prehod ves čas vzdrževati nabor naslovov, ki jih po potrebi dodeljuje RSIP agentom.

9. ***Prehod na aplikacijskem nivoju*** (ALG) – koncept dovoljuje spreminjanje glav signalizacijskih sporočil. Mehanizem ALG odpravlja vrzeli delovanja NAT-a v povezavi s sistemi VoIP. Tehnika prenaslavljanja se namreč dotika zgolj spreminjanja glav omrežnega ter transportnega sloja OSI referenčnega modela, medtem ko glave višjih slojev ostajajo nespremenjene. Signalizacijska sporočila SIP informacijo o omrežnem in transportnem naslovu prenašajo tudi v glavah sporočil SIP in v opisih pripadajočih sej (SDP), ki za naprave NAT predstavljajo vsebino aplikacijskega sloja. Prednost koncepta ALG pa je ravno v tem, da omogoča spreminjanje naslovnih polj tudi na aplikacijskem nivoju, na nivoju signalizacije SIP. Tipično je mehanizem implementiran na samem prehodu NAT, kar narekuje nadgradnjo oz. zamenjavo obstoječih naprav.

10. ***Vzpostavitev medsebojne povezave*** (ICE – *Interactive Connectivity Establishment*) – koncept dovoljuje končnim uporabnikom, da se na podlagi lastne poizvedbe sami odločijo za najboljši možni prehod naprave NAT. Sama poizvedba vključuje večino zgoraj opisanih konceptov (STUN, TURN, RSIP …). Stran A najprej poskusi pridobiti informacijo o svojem javnem paru IP/vrata [Slika 30] (1). Nato pošlje zahtevo za vzpostavitev seje strani B (2), ki lahko vključuje več javnih naslovov z različnimi prioritetami. Pri tem je potrebno poudariti, da sam mehanizem ne vključuje samega prehajanja SIP signalizacijskih sporočil. Stran B prav tako najprej začne s poizvedbo (3) o svojem javnem paru IP/vrata, nato pa odgovori na prejeto zahtevo (4). Glede na to, da že pozna pravi naslov, je komunikacija med obema stranema direktna. Nato lahko obe strani vzpostavita direkten RTP kanal (5), na podlagi naslova z najvišjo prioriteto. Poleg tega pa obe strani še dodatno pošljeta STUN zahtevo na isti naslov kot RTP pakete (6). Na podlagi prejetega naslova z najvišjo prioriteto (7) ustrezno spremenita naslov RTP paketov.



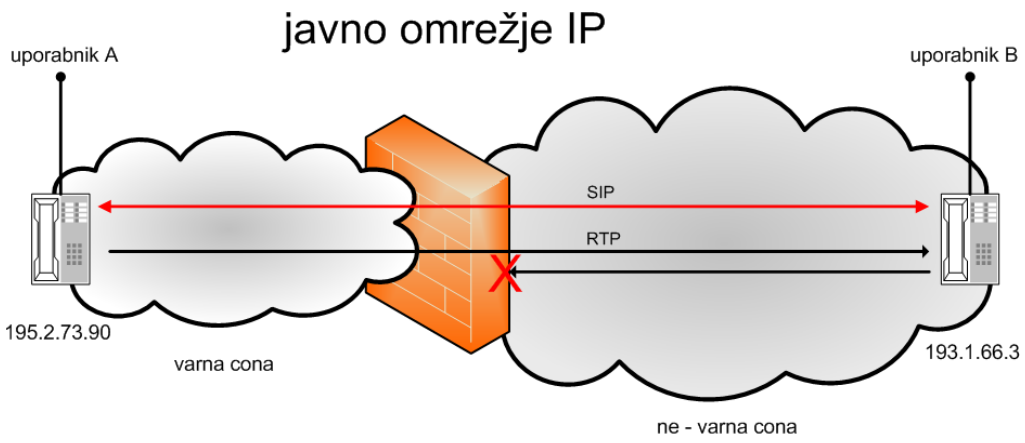
Slika 30: Prikaz mehanizma ICE [NATtra_05]

5.4. Uporaba požarne pregrade

Požarne pregrade so dandanes pravzaprav osnova zagotavljanja varnosti lokalnih (LAN – *Local Area Network*) in prostranih omrežij (WAN – *Wide Area Network*), demilitariziranih con (DMZ – *Demilitarized Zone*) in tudi posameznih računalnikov. Predstavljajo prvo linijo zaščite pred potencialnimi napadalci. Delujejo na principu omejevanja prometa glede na varnostno politiko, vzorce znanih napadov itd. Tako je ves promet, ki se ne ujema s pravili, zavržen. Primer takega pravila bi bil "Zavrži ves promet FTP (vrata 21)". Poudariti pa moramo, da požarna pregrada predstavlja centralno lokacijo za implementacijo varnostne politike, ki pa v primeru konvergenčnih omrežij predstavlja veliko verjetnost izpada storitev.

Za prenos RTP paketov skrbi UDP nivo, kar predstavlja dodatno težavo, saj je rezervacija UDP naslovov, ki jih končni entiteti rezervirata za komunikacijo, povsem naključna. Ker tipična požarna politika na robu varovanega omrežja odpira le omejen nabor vstopnih vrat ali parov IP/vrata, takšno naslavljanje predstavlja težavo ob implementaciji konvergenčnih omrežij. Kratkoročna rešitev je odpiranje celotnega niza vrat na požarni pregradi, tako da ta prepušča kakršnikoli medijski pretok RTP.

Druga možnost je uporaba požarne pregrade, ki ne pregleduje paketov povsem neodvisno drug od drugega, temveč si zna zapomniti stanje posamezne seje, saj lahko preveri vse aplikacijske podatke vsebovane v posameznem paketu.



Slika 31: Uporaba požarne pregrade

Transparentno naslavljanje entitet za napravo NAT narekuje poseg v naslovna polja signalizacijskih sporočil. Naloga presega osnovni nabor funkcionalnosti obstoječih mehanizmov kontrole dostopa, zato je potrebna nadgradnja obstoječih varnostnih mehanizmov. Primeri dobre prakse vodilnih ponudnikov storitev nove generacije navajajo vpeljavo namenskih aplikacijskih prehodov (ALG-jev).

Poleg tega pa je mogoča tudi uporaba virtualni privatnih omrežij in IPSec tuneliranja. V tem primeru se lahko ves promet tunelira direktno skozi požarno pregrado, kar pa pomeni, da je onemogočeno pregledovanje paketov, s čimer je funkcionalnost požarne pregrade izničena.

6. Primer celostne rešitve

Ponudnikov celostnih rešitev in elementov za konvergenčna omrežja, ki so osnovana na protokolu SIP, je kar nekaj: 3COM, Alcatel, Cisco, Ericsson, Lucent, Nortel, Sonus, Siemens, Huaway … Sam najbolje poznam rešitve, ki jih ponuja Siemens, zato se bom tudi osredotočil na njegovo skupino rešitev, ki je zajeta z enotnim imenom – SURPASS. Skupina rešitev SURPASS je sestavljena iz večih rešitev, ki so namenjene srednjim in večjim operaterjem telekomunikacijskih omrežij. Poudarek skupine rešitev SURPASS temelji na zlivanju že obstoječih omrežij, integraciji konvergenčnih omrežjih in komunikacij za podjetja in telekomunikacijske operaterje.

Glede na to, da sem sam sodeloval v integracijski skupini pilotskega projekta, ki je bil namenjen nizozemskemu telekomunikacijskemu ponudniku KPN, je verjetno najbolje, da se osredotočim na ta projekt. Projekt se je začel pred slabim letom. Začetek je bil zelo klavrn, saj ni bilo ne jasnih zahtev s strani kupca, niti sistem ni deloval tako kot bi moral, vendar so se s časom, predvsem pa zaradi naših naporov odkriti čim več napak v protokolu, kot tudi v programski opremi vseh sestavnih delov sistema, zadeve obrnile na bolje. Sam projekt je bil zaradi lažje integracije razdeljen na več korakov, ki so se skoraj vsakodnevno spreminjali in prilagajali trenutnim željam kupca, kar je tudi razlog zakaj pravzaprav projekt še vedno ni končan.

6.1. Arhitektura omrežja

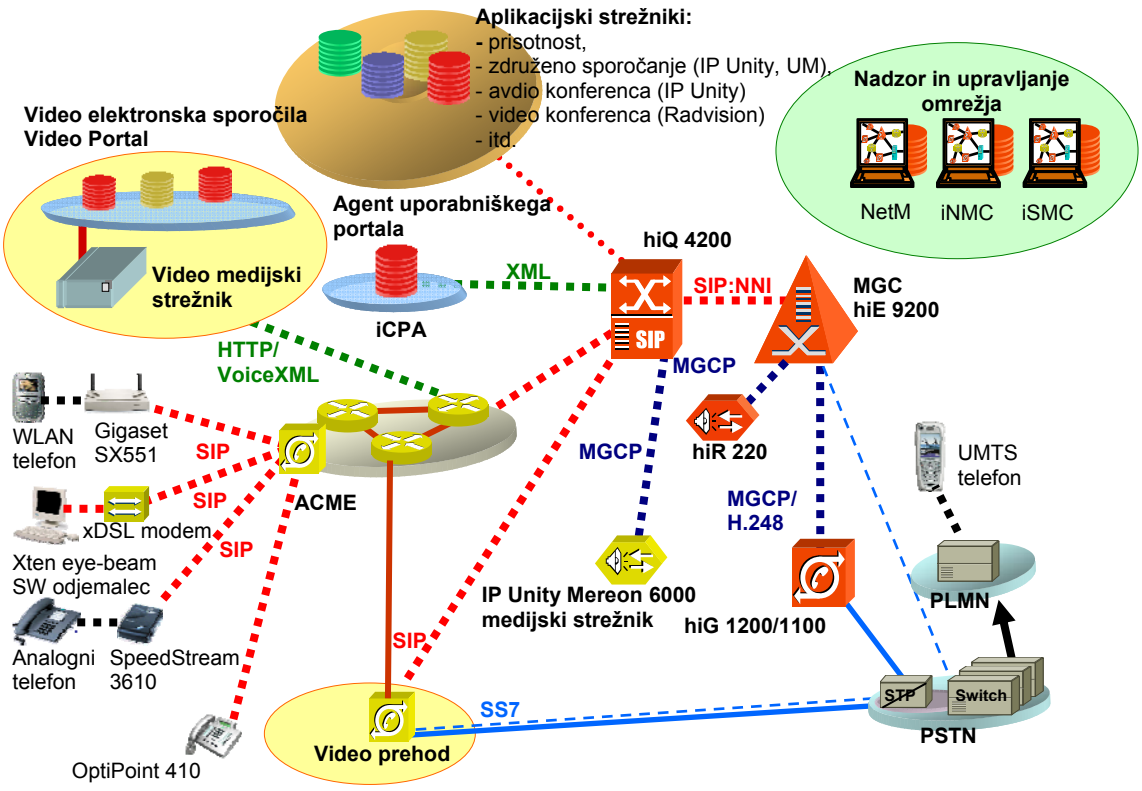
Za KPN sta bili zanimivi predvsem dve rešitvi: prva, ki je namenjena povezavi zasebnih uporabnikov preko VoIP-a (CV – *Consumer VoIP*) in druga, ki temelji na povezavi podjetij (BC – *Business Connect*). Rešitvi se dejansko razlikujeta v naboru storitev, ki jih kot celota ponujata in s tem ciljni skupini uporabnikov, katerim je rešitev namenjena. Dejansko je pri obeh rešitvah osnova enaka s to razliko, da BC rešitev dodatno potrebuje le še nekaj strojne in programske opreme za namene nadzora in upravljanja tudi s strani samega uporabnika. Prvo rešitev je KPN dejansko že implementiral na terenu, za drugo pa še vedno tečejo pogajanja in usklajevanja.

6.1.1. Rešitev CV

Rešitev CV je imenovana tudi VoIP@home in je namenjena tradicionalnim telekomunikacijskim operaterjem, ki lahko na podlagi te rešitve klasičnim uporabnikom ponudijo bolj priročne in osebnostno naravnane storitve in to z enako zanesljivostjo kot tradicionalne storitve. Ciljna skupina so predvsem uporabniki širokopasovnega dostopa. Penetracija širokopasovnega dostopa je namreč dosegla kritično maso, tako da imajo sedaj operaterji idealno priložnost, da na to, ravnokar vzpostavljeno dostopovno omrežje, vpeljejo svoje storitve po agresivno nizkih cenah. Vendar pa nizka cena vseeno ni dovolj. Zato so potrebne nove storitve in ravno tu se kaže pravi potencial v zmožnosti bogatenja komunikacijskega doživetja posameznega uporabnika.

Glavne storitve, ki jih CV podpira so [CV 2.1]:

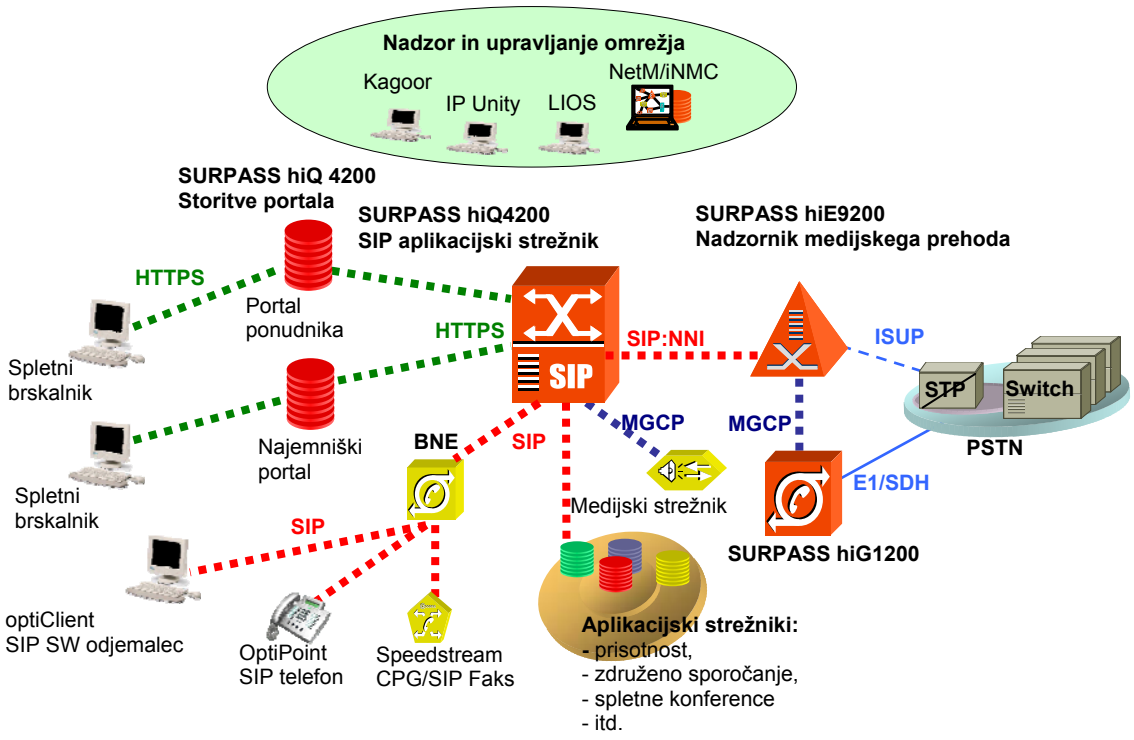
- vse vrste preusmeritev,
- prikaz identitete kličočega (CLIP – *Calling Line Identification Presentation*),
- skrivanje svoje identitete (CLIR – *Calling Line Identification Restriction*),
- prikaz identitete klicanega (COLP – *Connected Line Identity Presentation*),
- skrivanje identitete klicanega (COLR – *Connected Line Identity Restriction*),
- ponovitev zadnjega klica,
- ponovitev zadnjega prejetega klica,
- zavračanje anonimnih klicev,
- ne moti,
- klic na čakanju,
- odkrivanje zlonamernih klicev,
- indikacija čakajočih sporočil,
- omogočeno spreminjanje svojih nastavitev in popoln nadzor nad klici preko spletnega portala iCPA,
- video telefonija (tudi povezava z UMTS telefoni),
- avdio in video konferenca
- video elektronska sporočila,
- video portal …



Slika 32: Arhitektura rešitve CV [CV_2.1]

6.1.2. Rešitev BC

Rešitev BC je imenovana tudi SURPASS Hosted Office. V nasprotju s rešitvijo CV je usmerjena na večje enote, kot so podjetja in korporacije, ki danes uporabljajo privatne telefonske centrale (PBX – *Private Branch Exchange*) ali pa storitve TDM CENTREX skupin. BC je namreč rešitev, ki je sestavljena iz večih produktov, in v osnovi ponuja končno in izboljšano SIP CENTREX rešitev. Ponuja nabor multimedijskih storitev, vključno s poglavitnimi PBX in IP-CENTREX storitvami. Sem spadajo tudi različni spletni portali za uporabnike in administratorje, preko katerih lahko dostopajo do svojih nastavitev in storitev ter različnih orodij za nadzor in upravljanje.



Slika 33: Arhitektura rešitve BC [BC_5.1]

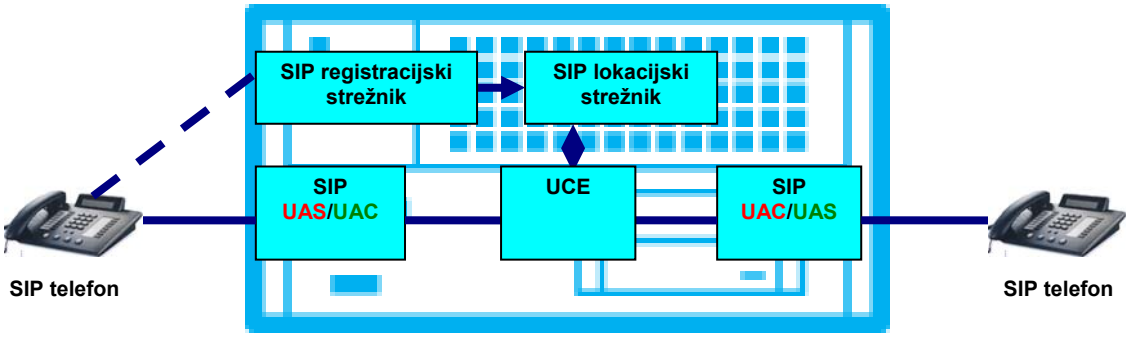
Glavne storitve, ki jih BC poleg že omenjenih CV storitev podpira so [BC_5.1]:

- dostopna koda za vsako poslovno enoto,
- avtorizacijska koda za zunanje klice,
- različne storitve, ki se nanašajo na pomoč pri klicanju (angl. *attendant support*),
- predaja klica,
- vnos imena poslovnega oddelka ali skupine,
- neposredno izbiranje navznoter (DID – *Direct Inward Dialing*),
- neposredno izbiranje navzven (DOD – *Direct Outward Dialing*),
- skrajšano izbiranje,
- prevzem klica znotraj skupine (GCPU – *Group Call Pickup*),
- omejevanje odhodnih/dohodnih klicev,
- hitro izbiranje z eno ali dvema številkama,
- istočasno zvonjenje (angl. *simultaneous ringing*),
- podpora nočnih storitev,
- daljinska preusmeritev klicev,
- različno zvonjenje (notranji/zunanji klic),

- podpora CSTA vmesnika za SIP končne točke,
- podpora video storitev in hipnih sporočil,
- omogočeno spreminjanje svojih nastavitev in popoln nadzor nad klici preko spletnega portala COM Manager …

6.2. Elementi omrežja

Srce celotne rešitve je SIP aplikacijski strežnik, imenovan hiQ4200 [Slika 34]. Poleg tega, da je B2BUA strežnik, vsebuje tudi podatkovno bazo vseh uporabnikov SIP, skrbi za povezavo s TDM svetom, vsemi pomožnimi aplikacijskimi strežniki ter drugimi strežniki SIP.



Slika 34: Arhitektura hiq4200

Celoten nabor vseh možnih omrežnih elementov je zbran v spodnji tabeli [Tabela 16].

Omrežni element	Verzija	Opis funkcionalnosti
SURPASS hiQ4200	R10.1	SIP aplikacijski strežnik
SURPASS hiE9200	V3.2	nadzornik medijskega prehoda (MGC) – za povezavo s TDM svetom
SURPASS hiR220	V2	strežnik za standardna obvestila TDM naročnikov
SURPASS hiG1200	V5	medijski prehod manjših kapacitet
SURPASS hiG1100	V2	medijski prehod večjih kapacitet
iNMC	R10.1	strežnik za nadzor in upravljanje elementov: hiG1200 in hiQ4200
iSMC	R10.1	strežnik za nadzor storitev naročnikov in omrežja
iCPA	R10.1	spletna storitev, ki uporabniku ponuja nadzorno funkcionalnost in administracijo samega sebe
iNetM	V6.2	strežnik za nadzor in upravljanje SURPASS omrežnih elementov
IP Unity Mereon 6000	V3.1	strežnik za standardna obvestila SIP naročnikov

IP Unity UM	V3.1	strežnik za glasovna, elektronska in faks sporočila
IP Unity Conference	V3.1	strežnik za razvoj avdio konferenc
ACME Session Director	V2.2	mejni krmilnik seje (SBC – *Session Border Controller*)
Kagoor Voice Flow VF 1000	-	mejni krmilnik seje
Radvision MCU ViaIP 400	V4.0	strežnik za večtočkovno glasovno in video konferenco
Dilithium Video GW DTG 2000	V2.1	strežnik za prekodiranje avdio in video standardov in protokolov
Dylogic Media Server PSE.MS	V3.1	strežnik za razvoj interaktivnih video storitev
Dylogic Video Mail PSE.VAM	V3.0	video tajnica
Dylogic Video Portal PSE.VP	V3.0	interaktivni video odzivnik
ERX 1400	R5	robni usmerjevalnik
Black Diamond L2/L3 Switch	R7	L2/L3 stikalo
OptiPoint 410 Advanced	V4.1	SIP telefon
OptiClient 130	V3.0	SIP SW odjemalec
SpeedStream 3610	-	SIP CPG
Gigaset SX551	-	SIP IAD
Gigaset SX651	-	SIP IAD
Xten eye-beam	V1.1	SIP SW odjemalec

Tabela 16: Spisek omrežnih elementov rešitve CV in rešitve BC

Kodeki, ki jih podpirajo vsi omrežni elementi so sledeči:

- G.711 a – zakon
- G.711 μ – zakon
- G.729
- G.729A
- G.726
- G.723
- T.30 (G.711)
- T.38
- H.263

6.3. Varnostni koncept

Omrežja VoIP so izpostavljena različnim varnostnim grožnjam, zato je potrebno predhodno sprejeti ustrezen varnostni koncept [BC_5.1]. Spodnja tabela prikazuje glavne nevarnosti in njihove rešitve [Tabela 17].

Varnostna grožnja	Varnostni mehanizem
Kraja storitev: nekdo ukrade identiteto določenemu uporabniku na podlagi maskiranja in spreminjanja paketov in podatkov, ki jih paket nosi.	Identifikacija uporabnika na podlagi topologije omrežja ali na podlagi varnostnih mehanizmov na aplikacijskem nivoju (npr. digest avtentikacija).
Neavtoriziran dostop do informacij ali sistema.	Identifikacija uporabnika na podlagi topologije omrežja ali na podlagi varnostnih mehanizmov na aplikacijskem nivoju (npr. digest avtentikacija).
Zapora storitev: preprečevanje dostopa do omrežja ali omrežnih storitev s pomočjo bombardiranja omrežnih elementov z nelegalnimi paketi.	Primerna struktura omrežja (ločevanje omrežij) in uporaba varnostnih pristopov na omrežnih elementih (npr. utrjevanje (angl. *platform hardening*)) in uporaba požarnih zidov na samih omrežnih elementih).
Kraja paketov: neavtorizirano prestrezanje govornih paketov.	Primerna topologija omrežja, predvsem na dostopovnem delu.

Tabela 17: Grožnje in glavni varnostni mehanizmi

Za preprečevanje kraje paketov bi se lahko uporabljala enkripcija, ki pa še ni implementirana, ker do nedavnega to področje še ni bilo dovolj dobro standardizirano. Priporočilo RFC 3711 za SRTP je namreč dostopen že od aprila 2004, vendar je takrat manjkal protokol za nadzor, upravljanje in distribucijo ključev (MIKEY). Implementacija enkripcije je planirana nekje do sredine leta 2006.

6.3.1. Aplikacijska varnost

Za varnost SIP odjemalcev je zaenkrat poskrbljeno z digest avtentikacijo med končnimi uporabniki in SIP aplikacijskim strežnikom, ki deluje na osnovi skritega gesla in velikega naključnega števila. Avtentikacija je potrebna za vsako posamezno zahtevo SIP odjemalca.

Določeni omrežni elementi ne podpirajo digest avtentikacije (hiE9200), zato je mogoče vse te elemente dodati na listo zaupanja vrednih končnih točk, ki ne potrebujejo avtentikacije. To je smiselno samo v primeru, če se vsi ti elementi nahajajo znotraj iste kontrolne domene. V nasprotnem primeru se lahko uporabi IPSec.

V primeru spletnega dostopa do uporabniških aplikacijskih portalov se uporablja protokol SSL ter ustrezni certifikati.

Elementi upravljanja in nadzora (NetM, iNMC, iSMC …) podpirajo sofisticirano varovanje na aplikacijskem nivoju. Protokoli, ki se uporabljajo so SNMPv2, FTP, SSH

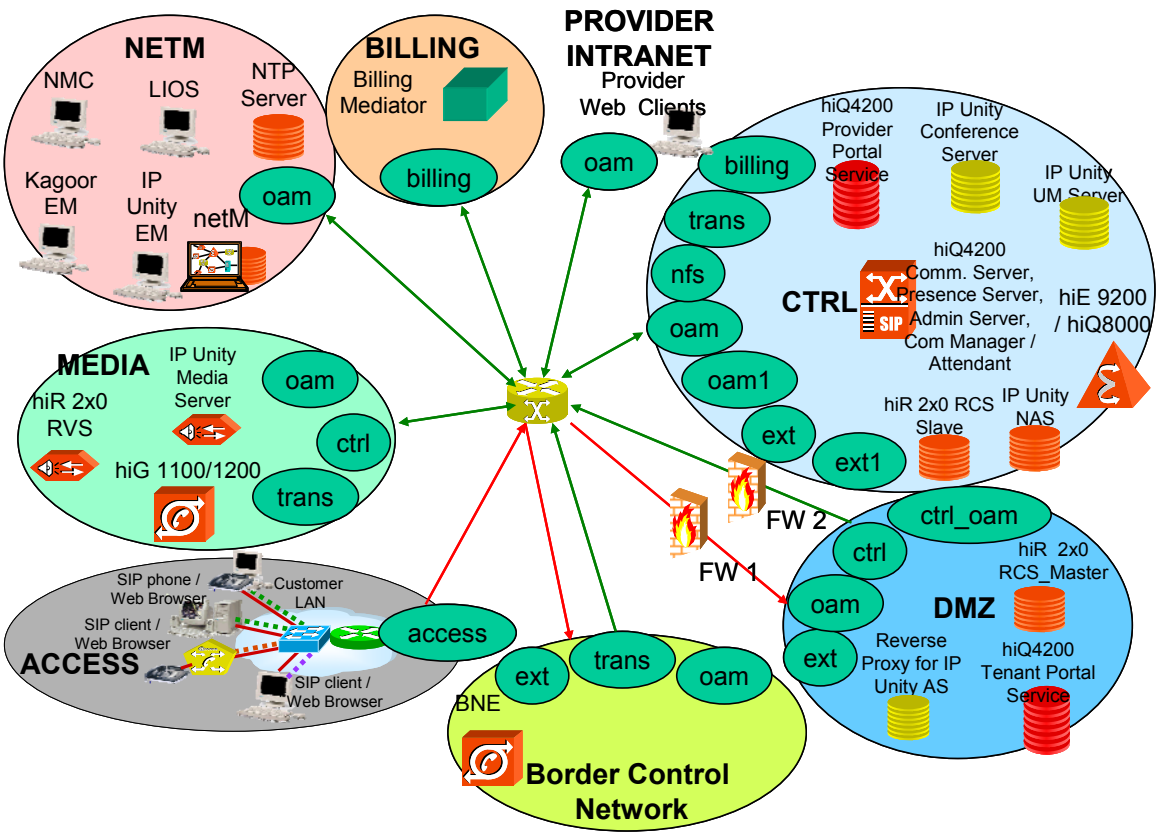
in HTTPS. Poleg tega pa je v prihodnosti planiran IPSec za iNMC in SNMPv3 za NetM.

6.3.2. Omrežna varnost

Predpostavlja se, da je rešitev SURPASS implementirana na hrbtenično omrežje, ki že zagotavlja ustrezno kvaliteto storitev, zanesljivost in ustrezno varnost. Potem je potrebno poskrbeti samo še za ustrezno logično delitev in segmentacijo omrežja na več varnostnih domen:

- domena nadzora in upravljanja (NETM),
- kontrolna domena (CTRL),
- demilitarizirana domena (DMZ),
- domena mejne kontrole (BCN),
- domena dostopa (ACCESS),
- medijska domena (MEDIA),
- domena tarifiranja (BILLING),
- domena intranet ponudnika (PROVIDER INTRANET) …

Poleg tega se nato še vsaka varnostna domena deli na več podomrežij (oam, ext, nfs, ctrl …). Spodnja slika prikazuje primer segmentacije omrežja [Slika 35]. Glavni del je seveda usmerjevalnik na sredini slike, ki določa, kdo lahko s kom komunicira. Pravila so določena na podlagi ACL seznama, ki se jih da ustvariti s pomočjo programskih orodij namenjenih izključno temu. Predhodno je potrebno definirati samo pravila [Tabela 18].



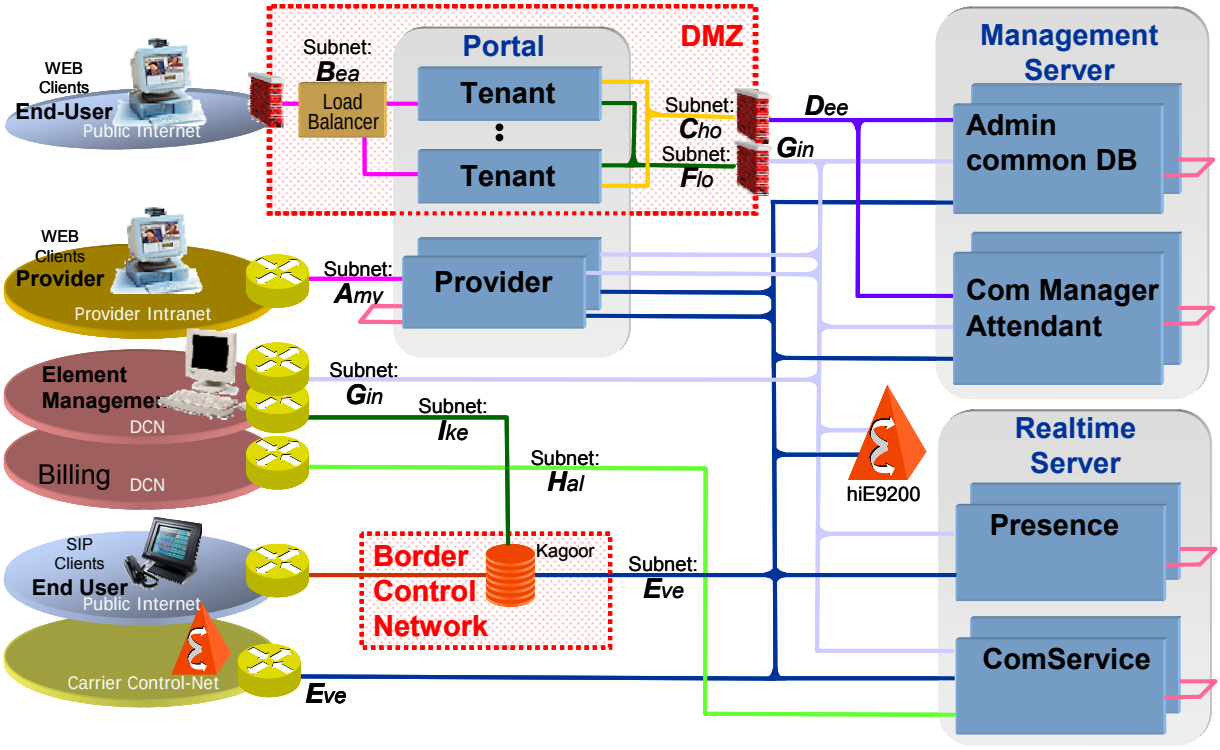
Slika 35: Segmentacija omrežja [BC_5.1]

Podomrežje	Opis	Strežnik za nadzor	Najemniški portal	Portal ponudnika	hiQ4200	IP Unity medijski str.	IP Unity aplikacijski str.	Kagoor VF3000
CTRL_ext	kontrolni/signalizacijski promet med komponentami CTRL varnostne domene	X		X	X		X	
CTRL_ext1	spletni promet od/do najemniškega portala v DMZ varnostni domeni	X						
CTRL_nfs	promet od/do CTRL varnostne domene (NAS strežnik)					X	X	
CTRL_oam	nadzorni in upravljavski promet od/do NETM varnostne domene	X		X	X		X	
CTRL_oam1	konfiguracijski promet (HTTPS) od/do varnostne domene intranet ponudnika			X				
CTRL_billing	promet tarifiranja proti BILLING varnostni domeni				X			
DMZ_ext	spletni promet od/do zunanjega omrežja (zunanji uporabniki)		X					
DMZ_ctrl	spletni promet od/do CTRL varnostne domene		X					
DMZ_oam	nadzorni in upravljavski promet od/do NETM		X					

	varnostne domene							
BCN_ext	kontrolni/signalizacijski promet od/do zunanjih uporabnikov in hiQ4200							X
BCN_oam	nadzorni in upravljavski promet proti NETM varnostni domeni							X
BCN_trans	medijski promet (RTP/RTCP) od/do MEDIA varnostne domene							X
MEDIA_ctrl	kontrolni/signalizacijski promet od/do CTRL varnostne domene					X		
MEDIA_trans	medijski promet (RTP/RTCP) proti MEDIA varnostni domeni					X		
MEDIA_oam	nadzorni in upravljavski promet od/do NETM varnostne domene					X		

Tabela 18: Pravila za komunikacijo med varnostnimi domenami [BC_5.1]

Če sedaj ta komunikacijska pravila upoštevamo pri risanju omrežne strukture, dobimo spodnjo sliko [Slika 36].



Slika 36: Logična omrežna struktura [BC_5.1]

SIP signalizacijski promet zunanjih uporabnikov je tako usmerjen skozi omrežje mejne kontrole (BCN – *Border Control Network*) proti SIP aplikacijskem strežniku (hiQ4200), ki se nahaja v kontrolnem omrežju. Elementi omrežja BCN se uporabljajo izključno za povečevanje varnosti omrežij, po katerih se prenašajo mediji. Element BCN bo odprl vrata RTP samo na zahtevo SIP aplikacijskega strežnika. Prav tako

elementi BCN znajo prenaslavljati omrežne naslove oz. popraviti signalizacijska sporočila SIP, če je bil na poti NAT že uporabljen. Elementa BCN, ki se trenutno uporabljata sta Kagoor ali ACME. Prav tako morajo ti elementi znati ločevati med več različnimi podjetji, ki so nanj povezana in v primeru napake na strani enega podjetja to ne sme vplivati na drugo podjetje. Poleg tega naj bi znali tudi omejevati število sporočil SIP od posameznega podjetja.

Ves ostali promet mora iti preko cone DMZ, ki ima za vsako podomrežje svojo požarno pregrado, ki pa skrbi za prvo obrambno linijo proti tipičnimi omrežnimi, transportnimi in aplikacijskimi napadi. Načeloma DMZ cona vsebuje zaključevanje HTTPS sej, proksi strežnik, izenačevalnik prometa, vzpostavitev varnih sej (HTTPS, IPSec) proti internemu omrežju, vendar se to lahko razlikuje od vsakega posameznega omrežja (stranke) posebej.

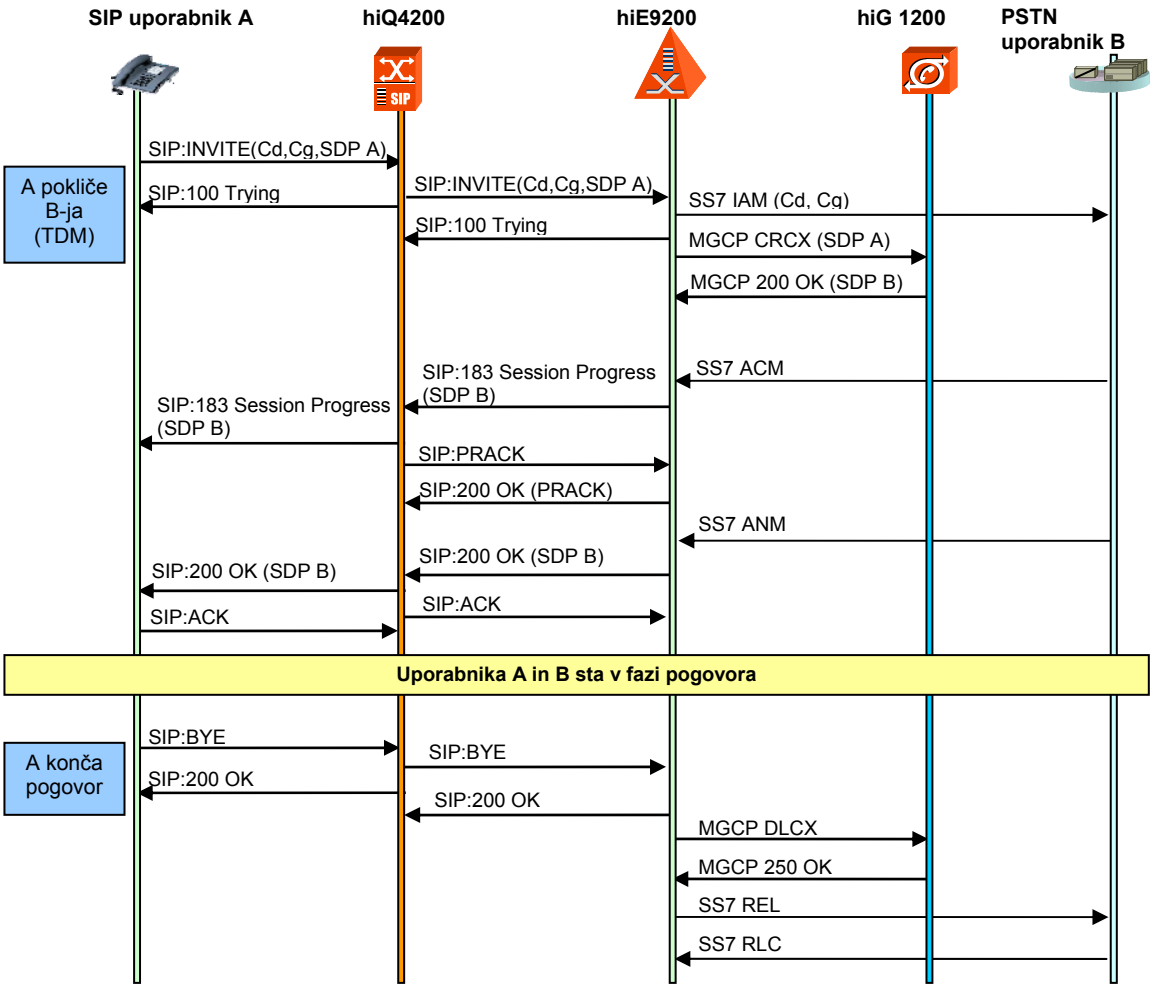
6.3.3. Varnost omrežnih elementov

Napadi se lahko sprožijo tako iz zunanjega kot tudi iz notranjega omrežja, zato moramo poskrbeti za varnostno utrjevanje vseh omrežnih elementov. Najpomembnejša sta seveda Kagoor ali ACME ter najemniški portal, saj igrata najpomembnejšo vlogo pri varovanju nosilnega omrežja. Prav zaradi tega je potrebno vpeljati še dodatne varnostne mehanizme, kot so: kontrola dostopa do posameznega elementa, beleženje dostopov, zaščita datotek, zaščita pred preobremenitvijo, uporaba oz. implementacija robustnih protokolnih skladov itd.

6.4. Poteki klicev

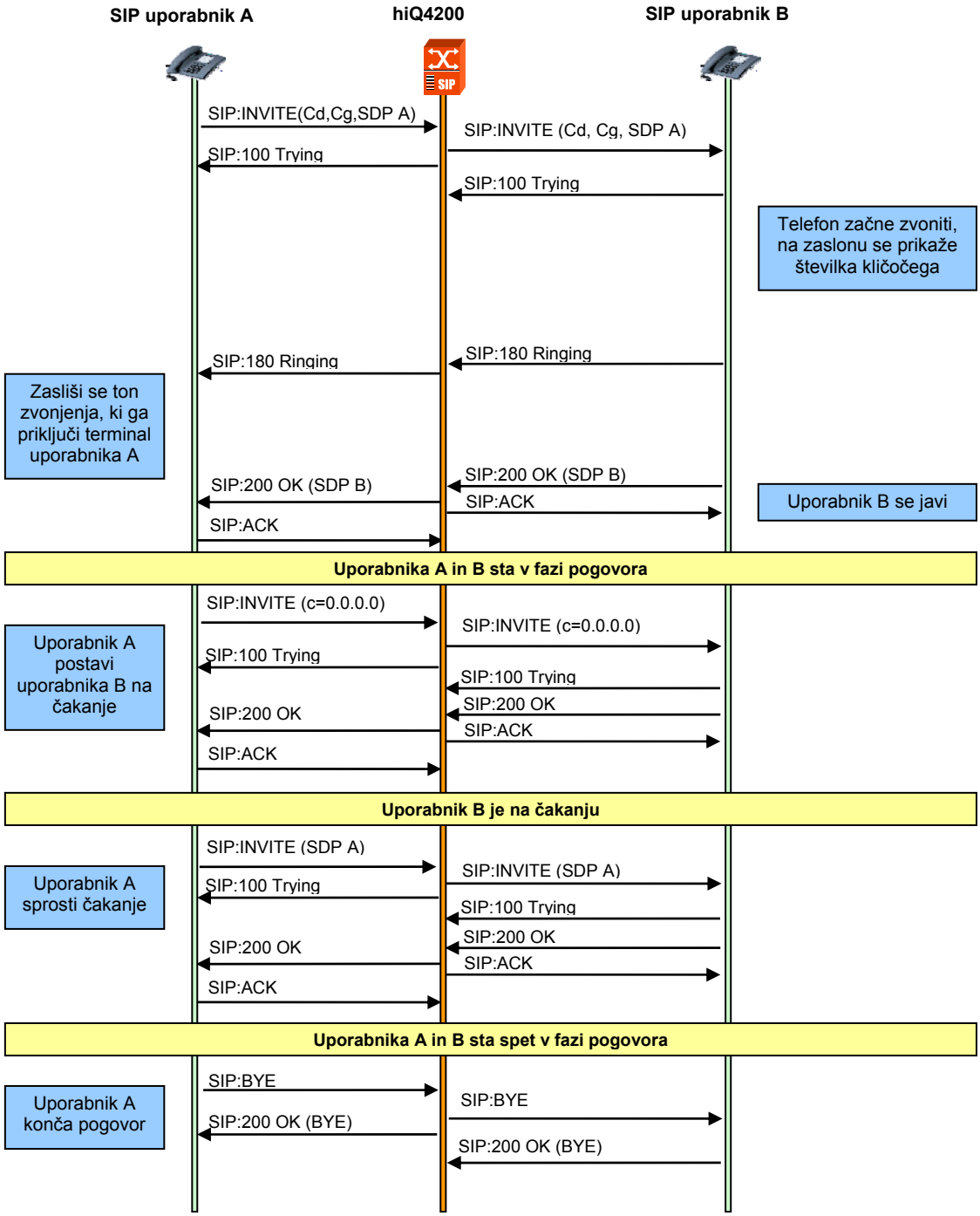
Sedaj pa si poglejmo še nekaj diagramov poteka klicev za storitve, ki jih je zahteval KPN.

6.4.1. Osnovni klic SIP – TDM



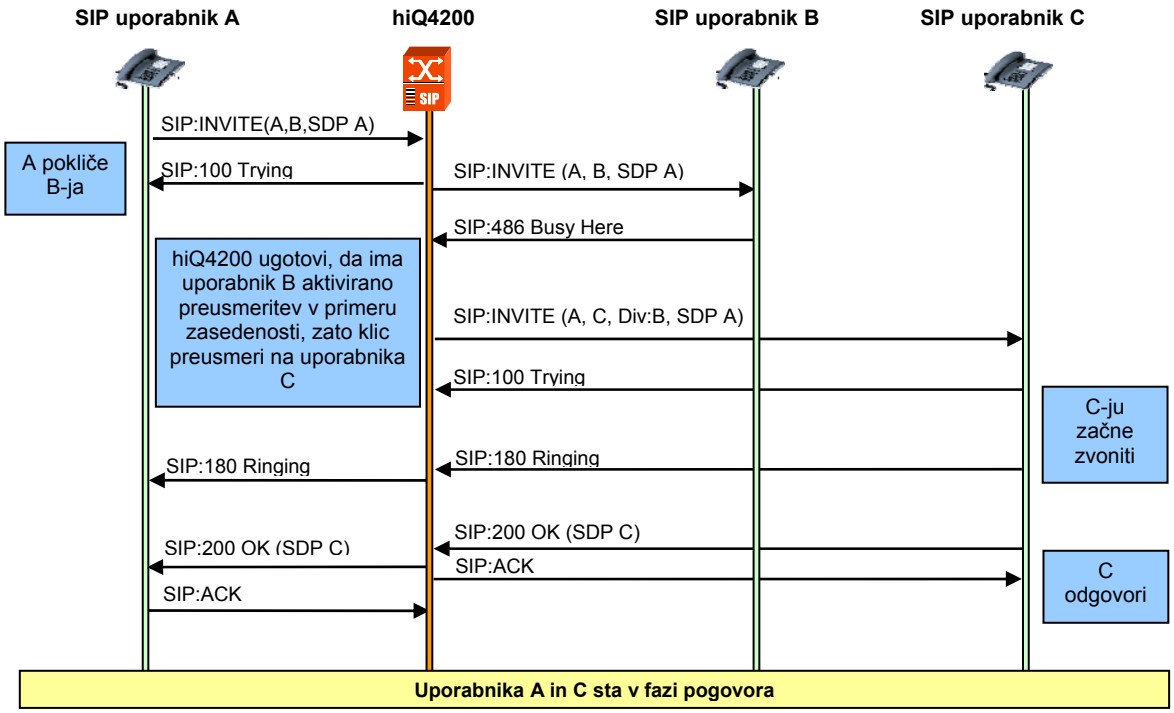
Slika 37: Osnovni klic SIP – TDM

6.4.2. Klic na čakanju



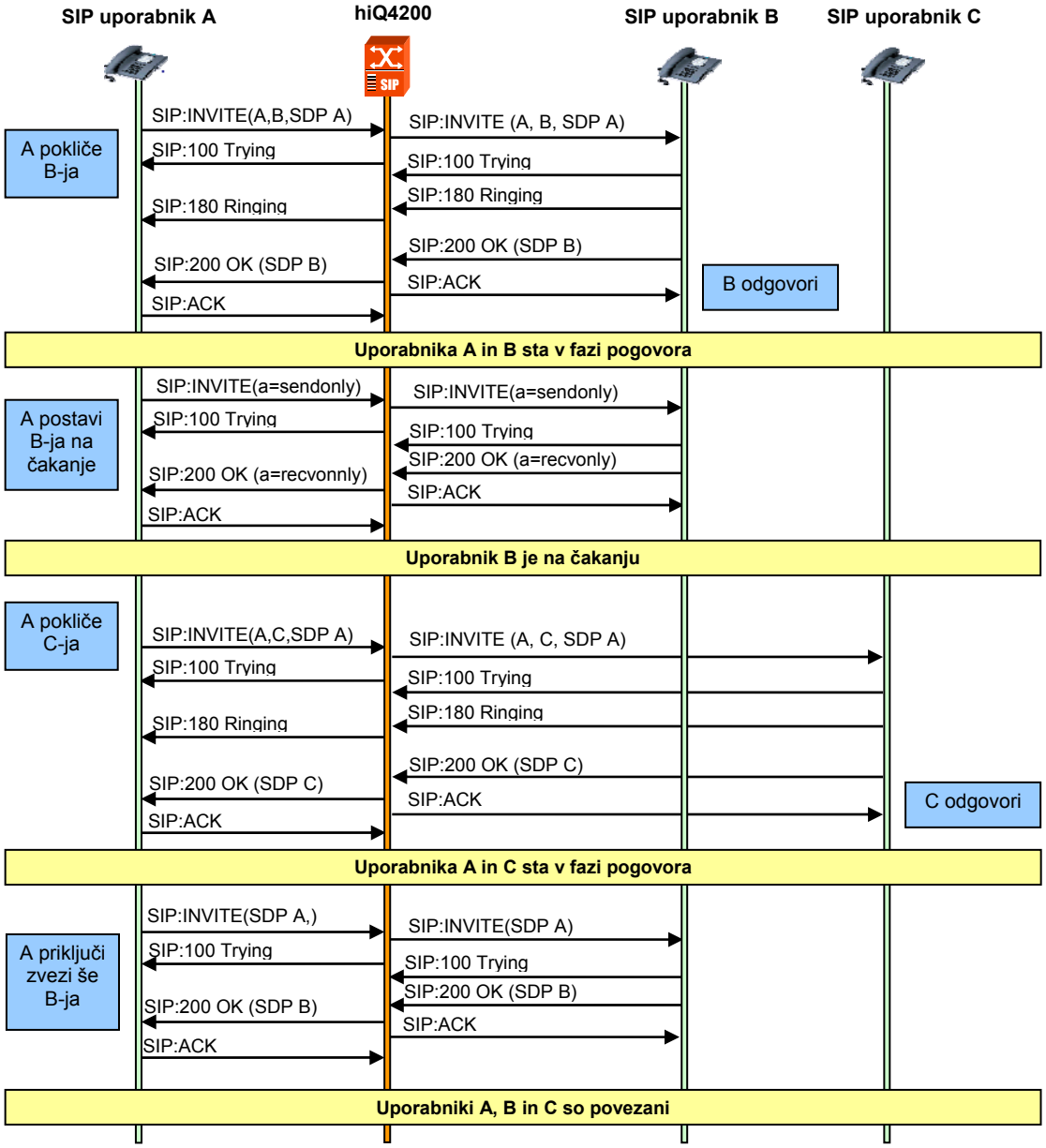
Slika 38: Klic na čakanju

6.4.3. Preusmeritev klica v primeru zasedenosti



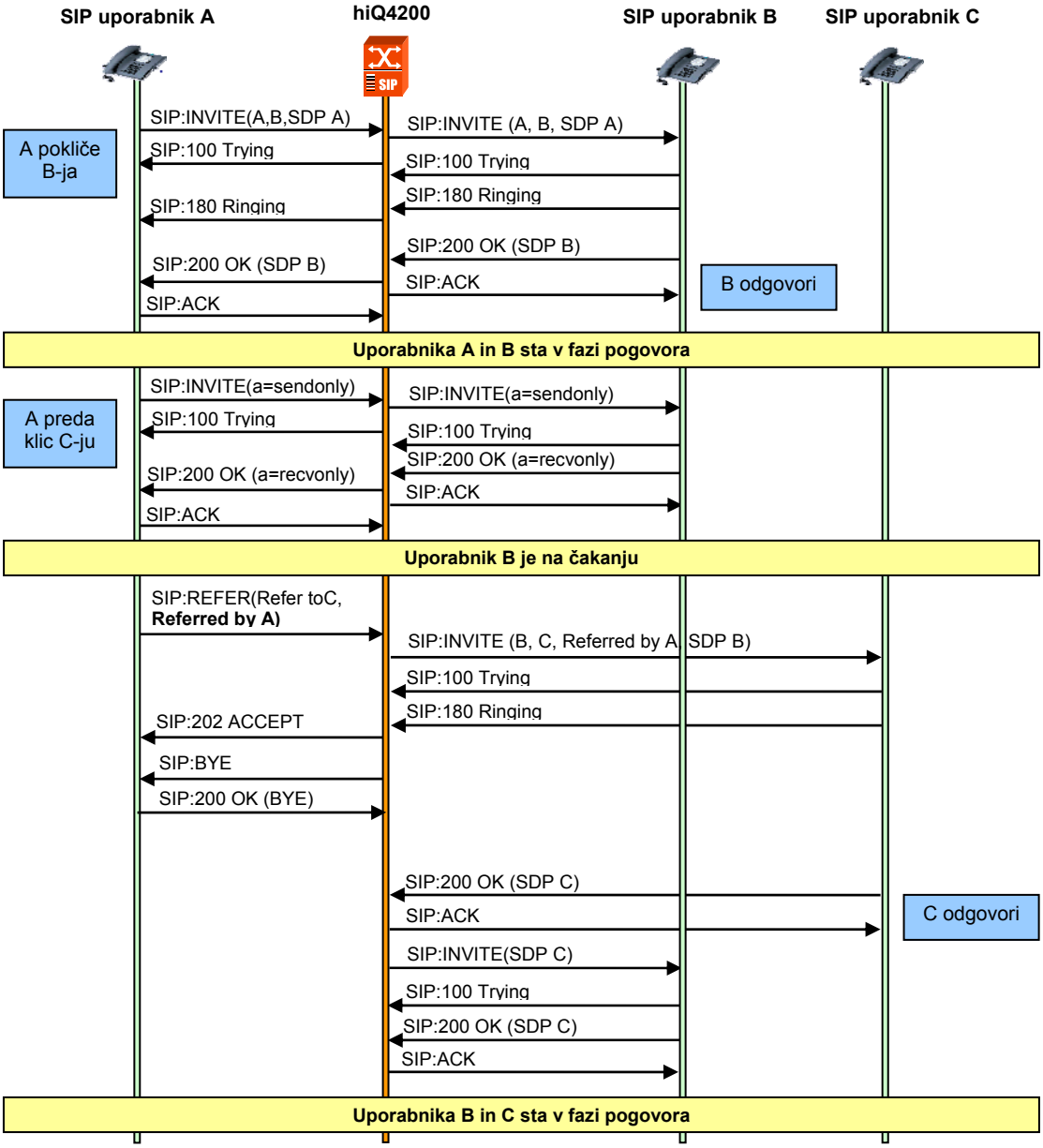
Slika 39: Preusmeritev klica v primeru zasedenosti

6.4.4. Konferenca treh udeležencev



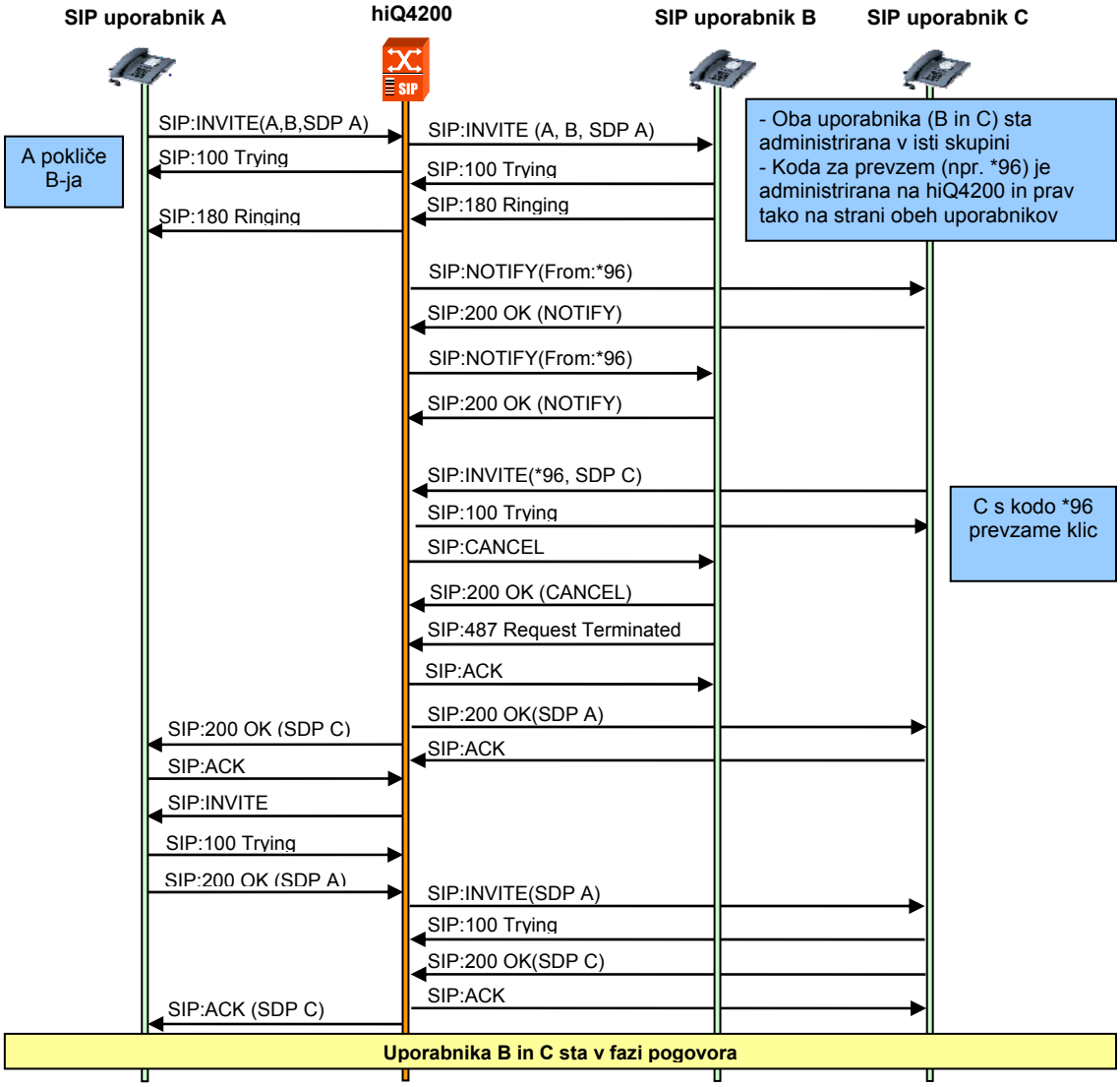
Slika 40: Konferenca treh udeležencev

6.4.5. Predaja klica brez posvetovanja



Slika 41: Predaja klica brez posvetovanja

6.4.6. Prevzem klica znotraj skupine



Slika 42: Prevzem klica znotraj skupine

7. SKLEP

Protokol SIP predstavlja povsem novo poglavje znotraj konvergenčnih sistemov. Eden izmed ključnih vzrokov za njegov začetek je bila njegova preprostost. Njegovi prvi uporabniki so bili predvsem novi ponudniki storitev, ki so se hoteli uveljaviti s ponujanjem storitev osnovanih na IP tehnologiji.

Dandanes pravzaprav ni več proizvajalca, ne samo s področja telekomunikacij (Nortel, Siemens, Nokia, Cisco …), temveč tudi s področja informatike (IBM, Microsoft), ki v svoje rešitve ne bi vključil protokola SIP. Njegova bistvena prednost je v odprti zasnovi, ki posledično omogoča izredno enostavno, predvsem pa hitro integracijo z različnimi naprednimi internetnimi aplikacijami in povsem novimi storitvami, ki bodo pritegnile tako ponudnike in upravljavce telekomunikacijskih sistemov, kot tudi končne uporabnike. Protokol SIP tako postaja izredno močno orodje za zagotovitev uspešnejšega modela poslovanja ter učinkovitejše izrabe virov, dokumentov in delovnih procesov v podjetjih. Poleg tega že tudi sama arhitektura sistema, v nasprotju s tradicionalnim TDM sistemom, zagotavlja hitro izvedbo inovativnih rešitev in vpeljavo novih storitev.

Zavedati se moramo, da je kompatibilnost s starejšimi oz. obstoječimi TDM sistemi in drugimi protokoli za prenos govora preko omrežja IP v glavnem že zagotovljena. Prav tako je podporo protokolu SIP uvedla tudi organizacija imenovana partnerski projekt tretje generacije (3GPP – *Third Generation Partnership Project*), ki ga uporablja kot osnovni protokol v IP multimedijskem podsistemu (IMS – *IP Multimedia Subsystem*). Poskrbeti pa bo potrebno še za interoperabilnost med opremo različnih proizvajalcev ter skladnost z IETF priporočili, saj je le tako mogoče zagotoviti večproizvajalsko okolje, večjo fleksibilnost ter cenovno učinkovitost.

Poleg tega pa bo potrebno poskrbeti za vse raznovrstne probleme, ki so se in se še bodo pojavili. Za večino danes znanih problemov rešitve že obstajajo, vendar verjetno še niso dokončne, kajti vse skupaj je še precej na začetku svoje navidezno začrtane poti. Velika večina proizvajalcev se prav ta trenutek trudi izboljšati in uskladiti rešitve s pripravo novih predlogov in priporočil.

Protokol SIP se je že pokazal kot učinkovit protokol pri uvajanju novih aplikacij in storitev, zato ga mnogi označujejo kot protokol prihodnosti, ki bo postal nekaj tako samoumevnega kot mobilna telefonija. Kljub temu proizvajalcem opreme in ponudnikom storitev sama uporaba protokola ne bo nujno zagotovila uspeha. Nenazadnje so uporabniki tisti, ki potrdijo ali ovržejo uspeh določenega produkta. Pri tem jih ne zanima uporabljena tehnologija, temveč uporaba in funkcionalnost storitev ter rešitev, ki jo tehnologija ponuja.

Dober primer tega je ravno naš projekt za telekomunikacijskega operaterja KPN, saj je v slabem letu, iz začetnih nekaj 10 naročnikov, pridobil več kot 40.000 naročnikov. To seveda ne bi bilo možno, če ne bi celotna skupina vložila toliko energije, časa, volje, znanja, pripravljenosti in želje, da projekt, in s tem novi sistemi resnično zaživijo tudi v praksi in ne samo na papirju. Ta uspeh nam je tako vlil še dodatno energijo in zadovoljstvo za doseganje novih ciljev, kot so izboljševanje sistema in njegova nadgradnja.

8. SEZNAM UPORABLJENIH VIROV

[RFC2327] M. Handley, V. J., *SDP: Session Description Protocol*, RFC 2327, april 1998, popravljen junij 2004

[RFC2396] T. Berners-Lee, R. F., U. C. I., L. M., *Uniform Resource Identifiers (URI): Generic Syntax*, RFC 2396, august 1998

[RFC2543] M. Handley, H. S., E. S., J. R., *SIP: Session Initiation Protocol*, RFC 2543, marec 1999

[RFC2617] J. Franks, P. H., J. H., S. L., P. L., A. L., L. S., *HTTP Authentication: Basic and Digest Access Authentication*, RFC 2617, junij 1999

[RFC3261] J. Rosenberg, H. S., G. C., A. J., J. P., R. S., M. H., E. S., *SIP: Session Initiation Protocol*, RFC 3261, junij 2002

[RFC3264] J. Rosenberg, H. S., *An Offer/Answer Model with the Session Description Protocol (SDP)*, RFC 3264, junij 2002

[RFC3265] A. B. Roach, Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265, junij 2002

[RFC4028] S. Donovan, J. R., *Session Timers in the Session Initiation Protocol (SIP)*, RFC 4028, april 2005

[IETF] The Internet Engineering Task Force – IETF. http://www.ietf.org/

[ITU_00] International Telecommunication Union – ITU, http://www.itu.int/home/

[ITU_G114] ITU-T Recommendation G.114 (1998), *Delay*

[Cumming_03] Jonathan Cumming, *SIP Market Overview*, september 2003, http://www.sipforum.com

[Sinden_02] R. Sinden, *Comparison of Voice over IP with circuit switching techniques*, Department of electronics and Computer Science, Southampton University, UK, januar 2002

[SecCon_05] D. Richard Kuhn, T. J. W., S. F., *Security considerations for Voice over IP Systems*, Recommendations of the National Institute of Standards and Technology, januar 2005

[NATtra_05] B. Sterman, D. S., *NAT traversal in SIP*, september 2005, http://www.sipforum.com

[App_Crypt] A. Menezes, P. Van O., S. V., *Handbook of Applied Cryptography*, CRC Press, 1996

[Bervar_05] Jan Bervar, *Lastnosti varnih omrežij telefonije IP v podjetjih* Sedemnajsta delavnica o telekomunikacijah, Elektrotehniška zveza Slovenije, VITEL zbornik referatov, maj 2005

[Hiti_05] Marko Hiti, *SIP danes in jutri*, Sedemnajsta delavnica o telekomunikacijah, Elektrotehniška zveza Slovenije, VITEL zbornik referatov, maj 2005

[Tomažič_03] Sašo Tomažič, *Varnost v telekomunikacijah in kako jo zagotoviti*, Štirinajsta delavnica o telekomunikacijah, Elektrotehniška zveza Slovenije, VITEL zbornik referatov, maj 2003

[Baptiste_05] Carl Baptiste, *SIP Status and Prospects*, VoiceCon conference, februar 2005

[Simnet_05] Ed Simnet, *SIP Status and Prospects*, VoiceCon conference, februar 2005

[Thallhammer_04] J. Thallhammer, *Security in VoIP-telephony systems*, januar 2004

[LMSpec] Carolyn Kirin, LM Specification, *FRN0727 – BC 1.0 Impacts to hiQ4200*, P30310-Q0295-Q080-01-7659, SIEMENS Network Convergence, maj 2004

[BC_1.1] Martin Erler, S. S., SURPASS Solution Package Description, SURPASS Hosted Office, *Business Connection V 1.0 and 1.1*, P30309-A8000-A001-01-7618, Siemens ICN, Information and Communication Networks, marec 2005

[BC_5.1] Sigrid Schneiders, W. G., J. S., S. R., H. H., SURPASS Solution Package Description, SURPASS Hosted Office, *Business Connection V 5.1*, Siemens Com, Communications, marec 2005

[CV_2.1] Lutz Krempel, SURPASS Solution Package Description, VoIP@Home, *Consumer VoIP 2.1*, Siemens ICN, Information and Communication Networks, december 2005

[CV_2.0] Lutz Krempel, SURPASS Solution Package Description, Voice@Home, *Consumer VoIP 1.0*/*2.0*, Siemens ICN, Information and Communication Networks, april 2005

[Avaya_04] White paper, *Evolving to Converged Communication with Session Initiation Protocol (SIP)*, Avaya, februar 2004, http://www.sipforum.com

[Intel_06] M. Kolbehdari, D. L., G. S., S. T., *Session Initiation Protocol (SIP) Evolution in Converged Commmunication*, Intel Technology Journal, Converged Communication, februar 2006, ISSN 1535-864X

[Lazar_06] I. Lazar, *VoiceCon Spring 2006: SIP And Today's IP-Telephone Market*, Burton Group, marec 2006

9. IZJAVA

Izjavljam, da sem magistrsko delo samostojno izdelal pod vodstvom mentorja prof. dr. Janeza Beštra. Izkazano pomoč drugih sodelavcev sem v celoti navedel v zahvali.

Damjan Jelovčan

10. SEZNAM UPORABLJENIH KRATIC IN SIMBOLOV

3DES	*Triple DES*	Trojni DES
3GPP	*Third Generation Partnership Project*	Partnerski projekt tretje generacije
ACL	*Access Control List*	Seznam za kontrolo dostopa
AES	*Advanced Encryption Standard*	Napredni standard za šifriranje
AH	*Authentication Header*	Avtentikacijska glava
ALG	*Application Level Gateway*	Prehod na aplikacijskem nivoju
ARP	*Address Resolution Protocol*	Protokol za prevedbo naslovov
B2BUA	*Back to Back User Agent*	Vrsta SIP aplikacijskega strežnika
BC	*Business Connect*	Rešitev, ki temelji na povezavi podjetij
BCN	*Border Control Network*	Omrežje mejne kontrole
CA	*Certification Authority*	Overitelj oz. izdajatelj digitalnih potrdil
CDP	*Cisco Discovery Protocol*	Ciscov protokol odkrivanja omrežja
CENTREX	*CENtral EXchange*	Tehnika javne telefonske komutacije, ki podpira navidezna zasebna omrežja
CLIP	*Calling Line Identification Presentation*	Prikaz identitete kličočega
CLIR	*Calling Line Identification Restriction*	Skrivanje svoje identitete
COLP	*Connected Line Identity Presentation*	Prikaz identitete klicanega
COLR	*Connected Line Identity Restriction*	Skrivanje identitete klicanega
CPG	*Customer Premises Gateway*	Prehod na strani uporabnika
CRC	*Cyclic Redundancy Check*	Ciklično preverjanje redundance
CV	*Consumer VoIP*	Rešitev, ki temelji na povezavi zasebnih uporabnikov preko VoIP
DES	*Data Encryption Standard*	Standard za šifriranje podatkov
DHCP	*Dynamic Host Configuration Protocol*	Protokol za dinamično konfiguriranje gostiteljskih računalnikov
DID	*Direct Inward Dialing*	Neposredno izbiranje navznoter
DMZ	*Demilitarized Zone*	Demilitarizirano področje
DNS	*Domain Name System*	Sistem domenskih imen
DOD	*Direct Outward Dialing*	Neposredno izbiranje navzven
DoS	*Denial of Service*	Zapora strežbe
ESP	*Encapsulating Security Payload*	Varovanje koristne vsebine z enkapsulacijo
FEC	*Forward Error Correction*	Vnaprejšnje popravljanje napak
FIFO	*First In First Out*	Prvi noter, prvi ven
FTP	*File Transfer Protocol*	Protokol za prenos datotek
GCPU	*Group Call Pick Up*	Prevzem klica znotraj skupine
GSM	*Global System for Mobile Communications*	Globalni sistem za mobilne komunikacije
HMAC	*Keyed – Hashing for Message Authentication*	Kodiran MAC

HTTP	*HyperText Transfer Protocol*	Protokol za prenos hiperteksta
HTTPS	*HTTP over SSL, encrypted version of HTTP*	http preko protokola SSL, šifrirana verzija http-ja
IAD	*Integrated Access Device*	Naprava z integriranim dostopom
ICE	*Interactive Connectivity Establishment*	Vzpostavitev medsebojne povezave
ICMP	*Internet Control Message Protocol*	Protokol internetnega krmilnega sporočila
IETF	*Internet Engineering Task Force*	Delovna skupina za internetsko inženirstvo
IKE	*Internet Key Exchange*	Internetni protokol za izmenjavo šifrirnih ključev
IM	*Instant Messages*	Hipna sporočila
IMS	*IP Multimedia Subsystem*	IP multimedijski podsistem
IN	*Intelligent Network*	Inteligentno omrežje
IP	*Internet Protocol*	Internetni protokol
IPSec	*Internet Protocol Security*	Varnostni internetni protokol
Ipv4	*IP version 4*	IP verzija 4
Ipv6	*IP version 6*	IP verzija 6
ISAKMP	*Internet Security Association and Key Management Protocol*	Internetni varnostni protokol za povezovanje in upravljanje s šifrirnimi ključi
ISDN	*Integrated Services Digital network*	Digitalno omrežje z integriranimi storitvami
ISUP	*ISDN User Part*	ISDN uporabniški del
IT	*Information Technology*	Informacijska tehnologija
ITU	*International Telecommunication Union*	Mednarodno telekomunikacijsko združenje
ITU-T	*International Telecommunication Union-Telecommunication*	Mednarodno telekomunikacijsko združenje, oddelek za telekomunikacije
LAN	*Local Area Network*	Lokalno omrežje
LDAP	*Lightweight Directory Access Protocol*	Protokol, ki določa dostop do imenika in je specificiran po IETF priporočilu RFC 1777
MAC	*Media Access Control*	Globalno enoličen naslov za identifikacijo naprav na drugem nivoju OSI modela
MBONE	*Multicast Backbone*	Hrbtenično omrežje z oddajanjem večim prejemnikom
MG	*Media Gateway*	Medijski prehod
MGC	*Media Gateway Controller*	Nadzornik medijskih prehodov
MGCP	*Media Gateway Control Protocol*	Protokol za nadzor medijskih prehodov
MIKEY	*Multimedia Internet Keying*	Protokol za izmenjavo šifrirnih ključev pri internetnih multimedijskih komunikacijah
MIME	*Multipurpose Internet Mail Extensions*	Večnamenska razširitev za elektronsko pošto
MOS	*Mean Opinion Score*	Srednja vrednost pridobljenih mnenjskih točk
MPLS	*Multi Protocol Label Switching*	Večprotokolno preklapljanje na osnovi oznak
MSRP	*Message Session Relay Protocol*	Protokol za prenos sporočil znotraj vzpostavljene seje
NAT	*Network Address Translation*	Prevajanje omrežnih naslovov
NGN	*Next Generation Networks*	Omrežja prihodnje generacije
OKDP	*Oakley Key Determination Protocol*	Oakleyjev protokol za določanje šifrirnih

		ključev
OSI	*Open Systems Interconnection*	Medsebojno povezovanje odprtih sistemov
PAMS	*Perceptual Analysis/Measurement System*	Analiza in meritev sistema na podlagi človeškega zaznavanja
PBX	*Private Branch Exchange*	Privatna telefonska centrala
PC	*Personal Computer*	Osebni računalnik
PCM	*Pulse Code Modulation*	Pulzno kodna modulacija
PESQ	*Perceptual Evaluation of Speech Quality*	Ocenjevanje kvalitete govora na podlagi človeškega zaznavanja
PGP	*Pretty Good Privacy*	Protokol precejšne zasebnosti; ime izdelka na osnovi asimetričnih šifrirnih postopkov (hibridna kriptografija)
PIN	*Personal Identification Number*	Osebna identifikacijska številka
PKI	*Public Key Infrastructure*	Infrastruktura javnih ključev
PSQM	*Perceptual Speech Quality Measure*	Meritev kvalitete govora na podlagi človeškega zaznavanja
PSTN	*Public Switched Telephone Network*	Javno komutirano telefonsko omrežje
QoS	*Quality of Service*	Kakovost storitve
RFC	*Request For Comment*	Stanje priporočila, ki ga izdaja IETF
RSIP	*Realm Specific IP*	Področno specifični IP
RSVP	*Resource Reservation Protocol*	Protokol za rezervacijo virov
RTC	*Real Time Collaboration*	Sodelovanje v realnem času (multimedijsko sodelovanje)
RTCP	*Real Time Transport Control Protocol*	Protokol za nadzor prenosa v realnem času
RTP	*Real Time Transport Protocol*	Protokol za prenos v realnem času
S/MIME	*Secure/Multipurpose Internet Mail Extensions*	Varna/večnamenska razširitev za elektronsko pošto
SBC	*Session Border Controller*	Mejni krmilnik seje
SCCP	*Signaling Connection Control Part*	Krmilni del signalizacijske zveze
SCCPS	*SCCP over SSL*	SCCP preko protokola SSL, varni krmilni del signalizacijske zveze
SCTP	*Stream Control Transmission Protocol*	Prenosni protokol z nadzorovanim pretokom
SDP	*Session Description Protocol*	Protokol za opis seje
SHA	*Secure Hash Algorithm*	Varni zgoščevalni algoritem
SIMPLE	*SIP Instant Messaging and Presence Leveraging Extensions*	Razširitev protokola SIP za neposredno sporočanje in vpliv navzočnosti
SIP	*Session Initiation Protocol*	Protokol za vzpostavljanje sej
SKEME	*Secure Key Exchange Mechanism for the Internet*	Varni protokol za izmenjavo šifrirnih ključev v internetu
SLA	*Service Level Agreement*	Dogovor o kvaliteti storitev
SMTP	*Simple Mail Transfer Protocol*	Preprost protokol za prenos elektronske pošte
SNMP	*Simple Network Management Protocol*	Preprost protokol za upravljanje omrežij
SRTP	*Secure Real Time Protocol*	Varni protokol za prenos v realnem času, uporabljen za prenos govora
SSH	*Secure Shell*	Varnostna lupina
SSL	*Secure Socket Layer*	Sloj varnih vtičnic

STUN	*Symmetric Traversal of UDP Through Network Address Translation*	Simetrični prehod UDP paketov preko naprave NAT
SW	*Software*	Programska oprema
TCP	*Transmission Control Protocol*	Protokol za krmiljenje prenosa
TDM	*Time Division Multiplex*	Časovni multipleks
TLS	*Transport Layer Security*	Varnost transportnega sloja
TOS	*Type of Service*	Tip storitve
TURN	*Traversal Using Relay NATs*	Prehod s pomočjo vmesnih naprav NAT
UA	*User Agent*	Uporabniški agent
UAC	*User Agent Client*	Odjemalec uporabniškega agenta
UAS	*User Agent Server*	Strežnik uporabniškega agenta
UDP	*User Datagram Protocol*	Uporabniški datagramski protokol
UMTS	*Universal Mobile Telecommunications System*	Univerzalni mobilni telekomunikacijski sistem
UPnP	*Universal Plug and Play*	Univerzalna arhitektura "vstavi in poženi"
URI	*Unified Resource Identifier*	Enolični identifikator virov
UTF-8	*8-bit Unicode Transformation Format*	Enotni osem bitni kodni transformacijski format
VLAN	*Virtual Local Area Network*	Navidezno lokalno omrežje
VoIP	*Voice over IP*	Govor preko internetnega protokola
VPN	*Virtual Private Networks*	Navidezna zasebna omrežja
WAN	*Wide Area Network*	Prostrano omrežje
WWW	*World Wide Web*	Svetovni splet