VoIP

VoIP (Voice over IP) je tehnologija, ki uporablja Internetni protokol (IP) za prenos govora v obliki paketov preko IP omrežja. Iz takšnega stališča je VoIP storitev možno izvesti preko poljubnega podatkovnega omrežja, ki uporablja IP, kot so Internet, Intranet in lokalna omrežja LAN. Osnovni pristop, ki ga uporablja VoIP storitev, je digitalizacija govornih signalov, njihovo komprimiranje in inkapsulacija v IP pakete, ki se lahko prenašajo preko IP omrežja. Ob tem so potrebni dodatni signalni protokoli, ki se uporabljajo za vzpostavljanje povezav, prekinjanje povezav in nosijo dodatne informacije, potrebne za lokaliziranje uporabnikov in pogajanje o sposobnostih. Osnovna motivacija Internetne telefonije je predvsem povezana z nižjimi stroški, vendar so s tem povezane tudi potrebe po multimedijskih komunikacijah in potrebe po integraciji govornih in podatkovnih omrežij.
Za uspešno razvijanje VOIP storitev je potrebno razrešiti nekatera ključna vprašanja, pri tem nekatera izmed njih izhajajo iz dejstva, da je IP omrežje zasnovano za prenos podatkov.

- Kvaliteta govora – IP omrežje je v sami osnovi oblikovano za prenos podatkov in tako ne ponuja garancije za prenose v realnem času, temveč nudi le storitve v obliki najboljšega truda. Da bi govorne komunikacije preko IP omrežja postale sprejemljive za samega uporabnika, je potrebno zmanjšati zakasnitve in variacije zakasnitev pod neko določeno vrednost praga. Za zagotavljanje kvalitete govora se lahko uporablja pristop izničevanja odmevov (Echo Cancellation), dodajanje višjih prioritet paketom, ki prenašajo govor, in uporaba napredne odprave napak (Forward Error Correction) ter krmiljenje zamašitev.
- Interoperabilnost – V okoljih javnih omrežij se od izdelkov različnih proizvajalcev zahteva nemoteno medsebojno delovanje in ta pogoj je potrebno zadostiti za uspešno širjenje VOIP storitev. Za doseganje interoperabilnosti med opremo različnih proizvajalcev se izdajajo standardi, kjer najbolj splošna standarda za signalizacijo v VoIP predstavljata H323 in SIP.
- Varnost – Problem varnosti v javnem Internetnem omrežju obstaja predvsem iz razloga, da vsakdo lahko zajema pakete v omrežju, ki so bili namenjeni nekomu drugemu. Nekaj dodatne varnostni je možno doseči z uporabo šifriranja podatkov, kjer varnost zagotavlja splošen mehanizem za šifriranje SSL (Secure Socket Layer) in uporabe tunelskih prenosov, kjer se najpogosteje srečujemo s splošnim tunelskim protokolom (Layer 2 Tunneling).

- Integracija z javnim preklopnim telefonskim omrežjem (PSTN) – V času razvoja in razširjanja Internetne telefonije je potrebno delovanje v kombinaciji z obstoječimi javnimi preklopnimi telefonskimi omrežji. Hkrati pa je z vidika uporabnika potrebno zagotavljati skupno sliko, v kateri javno preklopno telefonsko omrežje in IP telefonsko omrežje nastopata kot enovito omrežje.
- Razširljivost – Znotraj domene Internetne telefonije je veliko raziskovalnega dela namenjenega zagotavljanju enakovredni kvaliteti govora, kot je to v primerih klasičnih telefonskih klicev, vendar za mnogo nižjo ceno. Iz tega razloga obstaja velik potencial za izjemen porast VOIP sistemov, kar hkrati od sistemov zahteva zadovoljivo stopnjo fleksibilnosti za večje tržišče in možnost mešanja privatnih in javnih storitev.

Med najpomembnejše parametre za uspešen razvoj in razširjanje VoIP storitev lahko štejemo interoperabilnost opreme, kjer sta za signalizacijo trenutno predstavljana dva standarda in sicer H.323 (ITU-T priporočilo) in SIP (IETF standard). Priporočila ITU (International Telecommunications Union) H.323 standarda ponujajo tehnične zahteve za govorne komunikacije preko lokalnih omrežij (LAN) s predpostavkami, da znotraj teh omrežij ni predstavljanega zagotavljanja kvalitete storitev (QoS).

V osnovi je bil razvit za multimedijske konference znotraj lokalnih omrežij in se kasneje razširil na obseg govornih storitev preko IP omrežij. Prva različica standarda je bila izdana leta 1996, medtem ko je druga različica stopila v veljavo leta 1998. Standard obsega tako komunikacije od točke do točke, kot tudi večtočkovne konference. Izdelki in aplikacije različnih proizvajalcev lahko medsebojno delujejo, če upoštevajo H.323 specifikacije. Ob tem se je s strani IETF (Internet Engineering Task Force) razvil SIP (Session Initiation Protocol) protokol, ki je namenjen vzpostavljanju VoIP povezav. Priporočila standarda predstavljajo kontrolni protokol na aplikacijskem nivoju za ustvarjanje, spreminjanje in končevanje sej z enim ali več udeleženci.

Arhitektura SIP je podobna HTTP (odjemalec-strežnik protokol), saj se zahteve ustvarjajo na strani uporabnika in pošiljajo proti strežniku. Strežnik zahteve obdela in proti uporabnikom pošilja odgovore. Zahteva in odgovor na zahtevo tvorita transakcijo, ki vključuje sistemski sporočili za definiranje zanesljivega kanala, preko katerega se lahko pošiljajo klicna kontrolna sporočila. S takšnega vidika SIP zahteva le minimalne predpostavke glede podrejenega transportnega protokola in že sam ponuja zanesljivost ter je tako neodvisen od zanesljivosti

TCP. Za usklajevanje in identifikacijo opreme znotraj vzpostavljanja seje se uporablja SDP (Session Description Protocol). Na ta način se terminalom soudeležencev omogoča usklajevanje glede skupnega nabora združljivih tipov prenosnih medijev. Med pomembnejše lastnosti SIP štejemo tudi podporo mobilnosti uporabnikov, ki temelji na uporabi zastopniških strežnikov (proxy) in preusmerjanju zahtev na trenutne lokacije uporabnikov.

Zagovorniki SIP trdijo, da so bile H.323 specifikacije oblikovane predvsem z mislimi na signalizacijo ATM in ISDN omrežij in iz tega razloga H.323 ni tako primeren za kontrolo govora preko IP omrežij. H.323 je po svoji naravi precej kompleksen, z mnogimi lastnostmi na višjem nivoju, ki so neučinkovite za VOIP storitve. Pri tem pa mu primanjkuje razširljivosti, ki je potrebna za signalni protokol VOIP storitev. V nasprotju, je bil SIP protokol zasnovan z mislimi na Internet in se tako izogiba problemom kompleksnosti in razširljivosti. SIP izrablja večino že definiranih polj paketnih glav, kodirnih pravil, kodov napak in mehanizmov za dokazovanje pristnosti znotraj HTTP. H.323 uporablja binarno zapisana sporočila, medtem ko se pri SIP uporabljajo tekstovna sporočila, ki so podobna HTTP.

Tabela 1 Primerjava signalizacijskih protokolov SIP in H323

H.323	SIP
Kompleksen protokol	Primerljivo preprostejši
Binarna predstavitev sporočil	Tekstovna predstavitev sporočil
Potrebuje polno združljivost nazaj	Ne zahteva polne združljivosti nazaj
Ni visoke modularnosti	Visoka modularnost
Ni visoko razširljiv	Visoka razširljivost
Kompleksno signaliziranje	Preprosto signaliziranje
Velik tržni delež	Podpora IEFT
Težavna detekcija zanke	Primerljivo enostavna detekcija zanke

SIP lahko deluje v kombinaciji z RSVP (Resource Reservation Protocol), RTP/RTCP (Real-Time Transport Protocol), RTSP (Real-Time Streaming Protocol), SAP (Session Announcement Protocol) in SDP (Session Description Protocol). RTP/RTCP se uporablja za prenos podatkov v realnem času, RVSP za rezervacijo virov, RTSP za kontroliran prenos

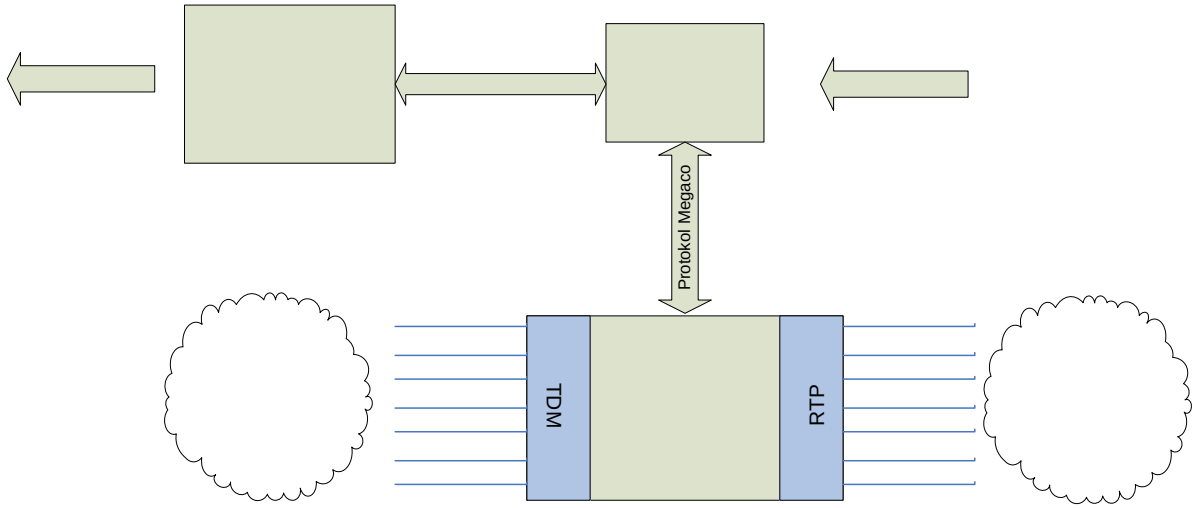
podatkovnih tokov, SAP za oglaševanje multimedijskih sej in SDP za opisovanje multimedijskih sej. Ob tem H.323 prav tako deluje v kombinaciji z RTP in RTCP (Real-Time Control Protocol).

V primerjavi obeh protokolov lahko zaključimo, da je H.323 protokol načeloma trenutno bolj razširjen in zajema večji del tržišča, vendar je SIP protokol v prednosti zaradi razširljivosti in preprostosti ter vključevanja RSVP protokola, ki omogoča rezervacijo virov znotraj omrežja in s tem pripomore k povečanju kvalitete storitev.

V praksi se manjši operaterji med sabo povezujejo preko protokola SIP. Tudi povezava do končnih strank se običajno realizira z uporabo protokola SIP. Protokol H323 pa se bolj uporablja pri medoperaterskih povezavah na tranzitu mednarodnega prometa.

Ker je prevladujoča tehnologija v svetu govornih komunikacij še vedno TDM, je potrebno VoIP omrežja marsikdaj povezovati s tradicionalnimi TDM omrežji. Povezavo izvedemo s pomočjo prehodov (gateway). V večini primerov so prehodi sestavljeni iz dveh delov, in sicer signalnega prehoda in medijskega prehoda. Signalni prehod komunicira z medijskim prehodom preko MGCP (Media Gateway Control Protocol). Največkrat proizvajalci prehodov združijo medijski in signalizacijski prehod v eno napravo, ki jo največkrat napačno poimenujejo kar »Media gateway«, čeprav v osnovi združuje tako signalizacijski, kot tudi medijski prehod. V tem primeru lahko medijski in signalizacijski prehod komunicirata preko nestandardnega protokola, ki ga definira proizvajalec opreme.

Splošna shema prehoda je prikazana na sliki 2.



Slika 1 Shema medijskega in signalizacijskega prehoda

Medomrežno povezovanje

Medomrežno povezovanje je zelo pomembni dejavnik v uspešnosti poslovanja novega operaterja. Preden se prične snovati strategija dogovarjanja in način izvedbe medomrežnega povezovanja z domačimi in tujimi operaterji je potrebno pregledati nekaj zadev, ki pomembno vplivajo na odločitve.

Tehnologija priklopa medomrežnih povezav je pred prihodom alternativnih ponudnikov bila strogo na strani TDM-TDM povezav, z uporabo signalizacije št. 7 (SS7).

S prihodom VoIP tehnologije se je v svetu pričelo pojavljati vse več podjetij, ki na osnovi te tehnologije ponuja cenejše mednarodne povezave. Kljub temu, je način povezovanja dostikrat še vedno TDM-TDM z uporabo VoIP-TDM vmesnikov (gateway).

Naslednji korak v evoluciji so pravi alternativni operaterji na VoIP tehnologiji, ki pa se lahko povezujejo tudi direktno v VoIP-VoIP tehniki, kar pomeni čisto ethernet medomrežno povezavo (in ne več SDH in n x E1). Takšen način prinaša prednosti (lažja implementacija med VoIP centralami, cenejša oprema in lažji nadzor) ter tudi nekaj slabosti, na katere je potrebno biti previden (predvsem na kvaliteto same povezave in zajamčeno bitno hitrost – pasovno širino povezave v smislu zagotavljati minimalnih pogojev QoS).
Kadar med dvema operaterjema ni predvidena dovolj velika količina izmenjanega prometa, da bi bilo direktno medomrežno povezovanje (bodisi VoIP ali TDM) ekonomsko upravičeno, se lahko operater posluži tranzita prometa preko nekega operaterja, s katerim je medomrežno povezan. V tem primeru sklenejo vsi trije operaterji tripartitno pogodbo o tranzitu prometa. Operater, preko katerega se promet tranzitira tovrstno storitev seveda obračuna.
Običajno operater sklene pogodbo o medomrežni povezavi preko protokola SS7 z enim operaterjem (največkrat je to nacionalni operater Telekom Slovenije), z ostalimi pa bodisi tripartitno pogodbo za tranzit ali pa medomrežno povezavo preko VoIP, odvisno od tehničnih zmožnosti in ekonomske upravičenosti medomrežne povezave.

Prenosljivost številk

Splošno o prenosljivosti številk

Prvi odstavek tretjega člena zakona o prenosljivosti številk pravi, da so vsi operaterji dolžni prilagoditi svoja omrežja, tako da slednja omogočajo prenosljivost številk, ter jih razvijati in izboljševati v skladu z naraščanjem števila prenesenih številk.

Če torej želimo načrtovati in izgraditi sistem, ki ustreza vsem zakonom v Republiki Sloveniji, je potrebno prenosljivost številk podpreti.

Za izmenjavo podatkov o prenesenih številkah med lokalnimi bazami prenesenih številk (LBPŠ) se uporablja centralna baza podatkov (CBP).

Centralna baza podatkov vsebuje vse prenesene številke, številke za usmerjanje klicev na prenesene številke in transakcije med operaterji (imena operaterjev dajalcev številk in operaterjev prejemnikov številk, datume prenosov številk, obvestila o statusu procesa prenosa številk).

Za vzpostavitev, razvoj, vzdrževanje in upravljanje centralne baze podatkov je odgovoren upravljavec centralne baze podatkov. Upravljavec centralne baze podatkov je odgovoren za pravočasno ažuriranje podatkov. Trenutno je v Republiki Sloveniji le en ponudnik centralne baze podatkov, in sicer je to podjetje Avtenta, hčerinsko podjetje Telekoma Slovenije. Trenutno se v Republiki Sloveniji med operaterji vsak dan prenese med 500 in 1000 telefonskih številk, pri čemer je največji donator številk nacionalni operater Telekom Slovenije.

Vsakemu operaterju v Republiki Sloveniji je s strani agencije za radio, pošto in telekomunikacije (APEK) dodeljena posebna unikatna štirimestna številka, ki operaterja enoznačno identificira. To številko imenujemo NRN (Network Routing Number). Vsaka dodeljena telefonska številka v Republiki Sloveniji tako vedno pripada nekemu NRN, na podlagi katerega si operaterji potem usmerjajo promet. V posebnih primerih se lahko enemu operaterju dodeli tudi več NRN številk, in sicer takrat ko uporabnik npr. opravlja storitve fiksne in mobilne telefonije. V tabeli 2 so prikazane NRN številke vseh trenutno registriranih slovenskih operaterjev.

Tabela 2 NRN številke slovenskih operaterjev

Company	Code
AKTON d.o.o.	9818
AMIS d.o.o.	9812
DEBITEL d.d.	9803
IN.LIFE, d.d.	9816
IT tel d.o.o.	9808

IZI MOBIL d.d.	9817
Ljubljanski kabel d.d.	9807
MEGA M, d.o.o., Velenje	9804
Mobitel d.d.	9800
Mobitel d.d.	9809
SI.MOBIL d.d.	9801
SINFONIKA d.d.	9813
SOFTNET d.o.o.	9815
STELKOM d.o.o.	9810
T - 2 d.o.o.	9806
T - 2 d.o.o.	9814
TELEING d.o.o.	9819
Telekom Slovenije d.d.	9811
TUŠ TELEKOM d.d.	9805
TUŠMOBIL d.o.o.	9802
UPC TELEMACH d.o.o.	9820

Kot je omenjeno že zgoraj, je potrebno pri usmerjanju prometa poskrbeti za hitrost. Čas vsakršne poizvedbe je kritičnega pomena in mora biti minimiziran, kolikor je to mogoče. Klici se lahko usmerjajo po dveh metodah, in sicer »Query on Release« ali »All Call Query«.

Metoda »Query on Release« je metoda usmerjanja klicev na prenesene številke, pri kateri izvorno omrežje pred vzpostavljanjem vsakega klica pošlje zahtevo za vzpostavitev klica proti komunikacijskemu omrežju operaterja, kateremu je bila številka dodeljena. Če telekomunikacijsko omrežje operaterja, kateremu je bila dodeljena številka, sprejme signalizacijsko zahtevo za vzpostavitev klica na številko, ki je prenesena v neko drugo komunikacijsko omrežje, zavrne zahtevo za vzpostavitev klica na način, ki je določen s Priporočilom ITU-T Q.850. Po sprejemu signalizacijskega sporočila z vzročno vrednostjo # 14 (SS7 Release cause value # 14) izvorno omrežje izvrši povpraševanje v lastni lokalni bazi prenesenih številk in na osnovi številke za usmerjanje, pridobljene iz lastne lokalne baze, vzpostavi klic direktno v omrežje, v katerem se nahaja prenesena številka.

»Metoda All Call Query« je metoda direktnega usmerjanja klicev na prenesene številke, ki temelji na IN-inteligentnem omrežju in kjer izvorno omrežje z namenom ugotovitve, če je klicana številka prenesena, pred vzpostavljanjem vsakega klica izvrši povpraševanje v lastni lokalni bazi prenesenih številk (LBPŠ). V primeru, da je klicana številka prenesena, izvorno omrežje na osnovi številke za usmerjanje, pridobljeni v LBPŠ, vzpostavi klic direktno proti omrežju, kjer se prenesena številka nahaja. V primeru, da številka ni prenesena, izvorno omrežje vzpostavi klic direktno z omrežjem, kjer se nahaja klicana številka.

V začetku uvedbe obvezne prenosljivosti številk se je uporabljala metoda »Query on Release«, pred nedavnim pa je bil sprejet zakon, ki nalaga vsem operaterjem uporabo metode »All Call Query«.

Podjetje Avtenta je razvila dva načina dostopa do LBPŠ, in sicer preko imeniške strukture LDAP ali preko domenskega sistema ENUM. Operater si lahko izbere ali želi v svoji lokalni bazi celotno bazo vseh številk v Republiki Sloveniji (teh zapisov je približno 100 milijonov) ali pa samo tiste ki so bile prenesene. Zaradi velike količine podatkov se pri prvem ponavadi uporablja ENUM, pri drugem pa bodisi LDAP ali pa ENUM.

Postopki pri prenosih številk

Proces prenosa številk lahko smiselno razdelimo v tri podskupine:

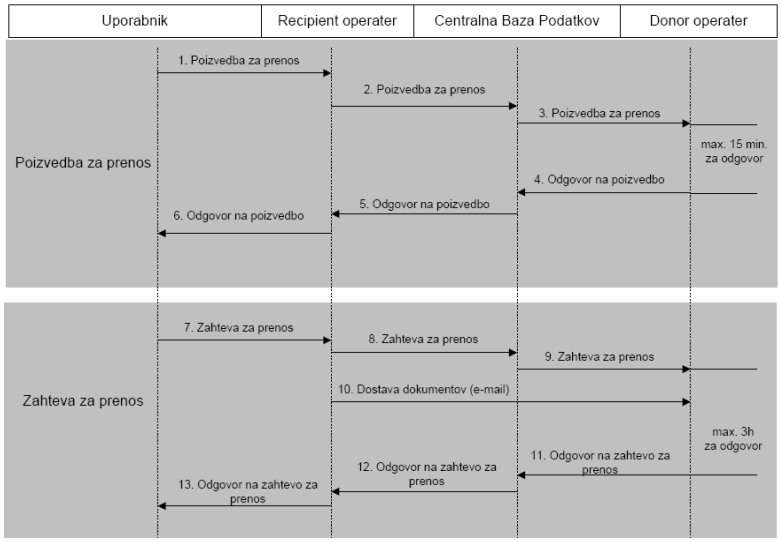
- Administrativni proces
- Tehnični proces
- Vračilo številke

a) Administrativni proces

Znotraj tega procesa prejemnik in donor, preko Avtente kot posrednika, določita končni datum prenosa številke iz donorskega v prejemnikovo omrežje.

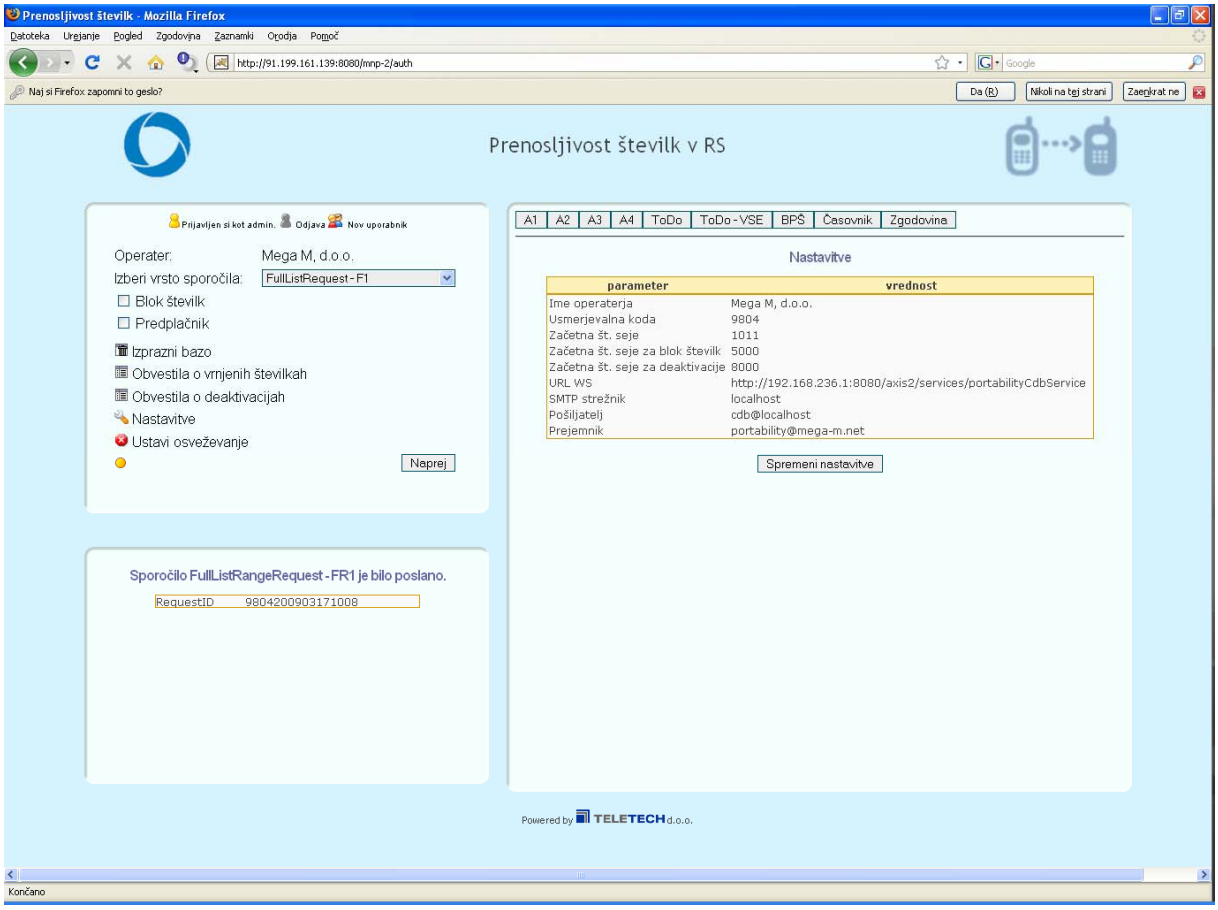
Prenos naročniške številke v administrativnem delu je sestavljen iz dveh delov. Najprej prejemnik na zahtevo stranke sproži poizvedbo za prenos številke iz donorskega v prejemnikovo omrežje. Donor je dolžan odgovor podati v 15 minutah po prejemu zahteve. V kolikor donor poda pozitiven odgovor, lahko prejemnik pošlje dejansko zahtevo za prenos številke. V primeru negativnega odgovora prejemnik odpravi razloge za negativen odgovor in ponovno pošlje zahtevo za prenos z novo številko seje. Poleg zahteve je prejemnik dolžan preko elektronske pošte ali faksa poslati donorju dokumente o stranki, ki želi opraviti prenos številke. Po prejeti zahtevi za prenos ima donor 3 ure časa, da poda datum prenosa številke. Odgovor je preko Avtente posredovan prejemniku in s tem je administrativni proces prenosa številke končan.

Potek je prikazan na sliki 3.



Slika 3 Potek administrativnega dela pri prenosu številk

Omenjeni procesi se prožijo preko vmesnika za prenosljivost številk. Ilustrativni izgled vmesnika je prikazan na sliki 4.



Slika 4 Administracijski vmesnik za prenosljivost številk

b) Tehnični proces

Tehnični proces določa vse potrebne postopke za posodobitev baze prenesenih številk pri vseh operaterjih. Avtenta znotraj tehničnega procesa vodi štiri liste MSISDN/NSN številk.
Sporočila za prihodnost:
- lista številk za prenos za naslednji dan
- lista številk za prenos za določeno časovno obdobje
- TO DO lista številk za naslednji dan
- TO DO lista številk za določeno časovno obdobje
Sporočila za preteklost:
- lista prenesenih številk
- lista prenesenih številk za določeno časovno obdobje

V listi številk za prenos za naslednji dan, so vpisane vse MSISDN/NSN številke, ki so bile znotraj administrativnega procesa določene za prenos za naslednji dan. Ker lahko donor teoretično odgovarja na zahteve za prenos do 18:59:59 ure in lahko pri tem določi datum za prenos na naslednji dan, se tudi lista številk za prenos dopolnjuje do tega trenutka.
Med 0:00 in 6:00 uro zjutraj vsi operaterji izvajajo postopek deaktivacij/aktivacij številk. Ko donor deaktivira številko, ki je bila določena za prenos, o tem obvesti Avtento. Avtenta številko doda v listo prenesenih številk, v listi številk za prenos pa to isto številko označi za preneseno.
Med tem, ko je lista prenesenih številk operaterju na voljo ves čas, pa se lista številk za prenos ob 8:00 zbriše, ter napolni z novimi številkami, za katere je bil določen datum prenosa za naslednji dan. Ta lista se dopolnjuje do 18:59:59.

c) Proces vračila številke

Proces vračila številke opisuje prehod številke nazaj k operaterju izvornega omrežja.
Pri procesu vračila številke zadnji prejemni operater, kjer je bila številka v uporabi, po izklopu številke iz svojega omrežja o tem obvesti Avtento. Avtenta izbriše številko iz baze prenesenih številk in o tem obvesti NRH operaterja (lastnika številčnega prostora v katerega sodi številka) in vse ostale operaterje. NRH operaterju je tako omogočeno, da začne postopek za ponovno uporabo številke. Postopki se izvajajo preko administracijskega vmesnika, ki je ilustrativno prikazan na sliki 4.