UNIVERZA V LJUBLJANI
Fakulteta za elektrotehniko

Primož Brajnik

Primerjava lastnosti protokolnih skladov za prenos signalizacij v klasičnih in internetnih omrežjih

MAGISTRSKO DELO

Mentor: dr. Janez Bešter

Ljubljana, 2006

ZAHVALA

Za pomoč in vodenje pri pisanju magistrske naloge se zahvaljujem mentorju dr. Janezu Beštru, ter predvsem mag. Franciju Katrašniku za številne koristne napotke in pravilno usmerjanje k cilju.

Zahvala gre tudi sodelavcem Tinetu Stegelu, Jaki Javorniku, Romanu Kotniku, ter vsem, ki so mi kakorkoli pomagali pri študiju in pri nastanku te magistrske naloge, tako z idejami, konkretno pomočjo ali pa le z moralno podporo.

Zahvalil bi se tudi staršema, ki sta mi omogočila študij, znala prisluhniti vsem mojim težavam in me tudi vseskozi na različne načine spodbujala.

Delo posvečam Tini!

KAZALO

SEZNAM SLIK

SEZNAM TABEL

POVZETEK

Izredno hitra rast podatkovnega prometa povzroča usmerjenost sodobnih telekomunikacijskih omrežij k paketnim tehnologijam prenosa in usmerjanja. Signalizacijski in krmilni protokoli so postali ključnega pomena za vzpostavitev, nadzor in rušenje zvez ali večpredstavnih sej med uporabniki.

Magistrska naloga obravnava prenos signalizacije SS7 preko omrežja IP. Narejena je primerjava med protokolnim skladom SS7, ki je poznan po svoji zanesljivosti, ter protokolnim skladom SIGTRAN. Poudarek je na postopkih, ki povečujejo zanesljivost signalizacije v omrežjih IP in se približujejo lastnostim klasične signalizacije v svetu TDM.

V uvodu je predstavljen prehod klasične telefonske signalizacije v domeno interneta. V preteklosti so se zahteve po zanesljivosti reševale z ločenim namenskim omrežjem, sedaj pa je razvoj usmerjen v prestavitev prenosa in signalizacije v univerzalno omrežje IP. Poudarek je na zanesljivosti in zagotavljanju storitev, ki jih je bil uporabnik do sedaj vajen.

V drugem poglavju je opisan Signalni sistem številka 7, ki ga delimo na podsistem MTP in njegove uporabniške protokole. Predstavljena je zgodovina in razvoj signalnega omrežja SS7, arhitektura omrežja in razdelitev protokolnega sklada. Naštete so bistvene lastnosti podsistema za prenos sporočil MTP, ter namen posameznih uporabniških slojev.

V tretjem poglavju je predstavljen protokolni sklad SIGTRAN. Prikazan je prehod iz klasičnega telefonskega omrežja v omrežje IP. Opisani so posamezni elementi, ki so potrebni za prehod, ter njihov namen. Protokolni sklad SIGTRAN je skupina potrebnih protokolov za prenos signalizacij preko omrežja IP. Ker omrežni protokol IP, ne zagotavlja zanesljivega prenosa, uporabljamo za zanesljiv, strukturiran in časovno urejen prenos uporabniških sporočil transportni protokol SCTP. Opisani so posamezni prilagodilni sloji in umestitev v protokolni sklad. Naštete so bistvene lastnosti in namen posameznega prilagodilnega sloja.

V četrtem poglavju je podrobno obdelan posamezen sloj v protokolnem skladu SS7 in SIGTRAN. Predstavljena je primerjava med posameznimi

funkcijami in lastnosti istoležnih slojev. Za izhodišče na tretjem nivoju je vzet protokol M3UA, ki je edini od prilagodilnih slojev, ki zajema vse funkcionalnosti sloja MTP3. To pomeni, da omogoča enakovredne možnosti redundančnih postopkov, kot je to omogočeno v protokolnem skladu SS7.

Peto poglavje zajema teste in preizkuse nekaterih redundančnih arhitektur, ter postopke preklopa ob izpadu določenih povezav. V Laboratoriju za telekomunikacije smo za slovensko telekomunikacijsko podjetje implementirali in razvili protokole SCTP, M3UA, M2PA, razvijamo pa še protokol M2UA. Preizkusi so bili izvedeni v laboratorijskem testnem okolju.

V sklepu so povzete bistvene lastnosti protokolnega sklada SIGTRAN in primerjava med protokolnim skladom SS7. Podana je tudi ocena primernosti protokolov SIGTRAN za prenos signalizacije v omrežju IP.

Ključne besede: signalizacija, SS7, MTP, SIGTRAN, omrežje IP, SCTP, M3UA, zanesljivost, redundanca, signalni prehod, aplikacijski strežnik, signalne točke, signalne povezave.

ABSTRACT

Fast growth of data traffic in today's communications has caused networks to rely on packet technologies and routing. Signaling and management protocols have become significant for establishing, monitoring and terminating calls and multimedia sessions among users.

This master thesis is discussing transfer of Signaling System No. 7 over IP. It contains extended comparison between SS7 protocol suite, which is known for its reliability, and SIGTRAN protocol suite. It focuses on mechanisms which improve signalization reliability in IP networks and come close to classical TDM signalization characteristics.

The introduction describes transience of telephone signalization into internet domain. The reliability needs in the past have been solved by introducing physically separated network. Today the researches have focused on transferring the traffic and signalization to universal IP networks and they are based on reliability and service provisioning the users have been accustomed to in the past.

The second chapter describes Signaling System No. 7 which contains two subsystems. The first part is transferring system MTP and the second part consist of user protocols. The chapter continues with the history and development of SS7, its architecture and protocol suite. Main characteristics of MTP subsystem and user protocol purposes are emphasized at the end.

The third chapter introduces SIGTRAN protocol suite. It shows the transfer from classical telephone network to IP network. It describes individual elements that are required for successful transfer and their purpose. While IP protocol does not provide reliable transport on network layer, the transport layer uses SCTP protocol which features reliable, structured and sequenced delivery of user messages. Chapter also contains detailed description of adaptation layers, their characteristics and purpose.

In the fourth chapter individual SIGTRAN layers are analyzed in detail and compared with equivalent SS7 layer. Analysis includes the

comparison between functionalities and characteristics of individual layers. The main focus is M3UA protocol which is the only adaptation layer that covers all mechanisms and attributes of MTP3 layer in SS7. It is shown that M3UA with SCTP has equivalent redundancy options and mechanisms as SS7 system.

Fifth chapter describes scenarios and actual testing of different redundancy architectures and procedures when individual links disconnect. In the Laboratory for telecommunications the protocols SCTP, M3UA and M2PA were developed and thoroughly tested. Chapter includes testing results and their extended analysis.

The conclusion sums up the main characteristics of SIGTRAN protocol suite and comparison with the SS7 suite. It evaluates the suitability of SIGTRAN protocols in transporting signalization in IP networks and it introduces main directions for further work.

Keywords: signalization, SS7, MTP, IP network, SCTP, M3UA, redundancy, reliability, signalling gateway, application server, signalling point, signalling connections.

1. UVOD

Prenos govora je ena najstarejših in tudi najbolj razširjenih telekomunikacijskih storitev. V družbi, v kateri živimo, so komunikacije iz dneva v dan bolj pomembne in dobivajo večjo veljavo. Prav zato so postale telekomunikacije ena najvplivnejših gospodarskih panog. V preteklosti sta se razvila dva splošna tipa omrežij, ki danes igrata glavno vlogo v razvoju telekomunikacij. Prvo je podatkovno omrežje s paketno komutacijo, drugo pa telefonsko z vodovno komutacijo. Danes je internet največji fenomen sodobne družbe.

Po drugi strani pa so ljudje še vedno navajeni na govorne komunikacije. Zato telefonsko omrežje še ne izgublja veljave. Telefonija in vse pripadajoče storitve (glasovna pošta, prikaz številke, ...) ne bi delovale brez telefonske signalizacije. Ta pojem opisuje informacije, ki se prenašajo po telefonskem omrežju in se uporabljajo za vzpostavitev, nadzor in prekinitev telefonskega klica, ter za mnoge dodatne storitve, kot so zaračunavanje, gostovanje mobilnih telefonov, teleglasovanja, itd. Telefonska signalizacija je obstajala in se razvijala skozi vso zgodovino telefonije in je prav tako pomembna kot sam prenos zvoka, saj na njej temelji celotno telefonsko omrežje. Danes se je po vsem svetu najbolj uveljavila Signalizacija številka 7.

Čeprav je današnje telefonsko omrežje zanesljivo in zmogljivo, se nenehno tehnološko izboljšuje. Digitalizacija prenosa vsebin in signalizacije je pocenila prenosno omrežje ter izboljšala njegovo zanesljivost. Omogočene so bile napredne storitve, lažje povezovanje različnih omrežij, poenostavili pa so se tudi pogovori med zelo oddaljenimi kraji. Telefonsko omrežje je tako postalo kvalitetnejše in bolj uporabno, še vedno pa je ostalo ločeno od vzporedno razvijajočih se prenosnih tehnologij, omrežij, protokolov in drugih storitev.

Trenutna smernica razvoja v telekomunikacijah je postala zlivanje tehnologij in omrežij. Telekomunikacije se razvijajo proti cilju dostave katerekoli oblike informacij (zvoka, teksta, videa, podatkov in slik) skozi katerokoli omrežje na poljuben terminal, ki si ga izbere uporabnik. Internetno omrežje tako postaja univerzalni prenosni sistem

za vse telekomunikacijske vsebine in predstavlja most za povezavo različnih tehnologij. Omrežje IP zaradi svoje univerzalnosti sicer še ne dosega zmogljivosti namenskih prenosnih tehnologij, razvitih za določeno storitev, omogoča pa enostavno nadgradnjo protokolnih skladov, ki celotni sistem izboljšajo v smislu zmogljivosti, zanesljivosti in varnosti.

Zaradi omenjenih lastnosti se tudi telefonija širi iz namenskega telefonskega omrežja v omrežje IP. Kljub temu, da bo obstoječe omrežje zaradi svoje ogromne razsežnosti in visoke zanesljivosti še dolgo uporabi, pa se operaterjem ponujajo nove možnosti za povezovanje in izkoriščanje naprednih in raznovrstnih tehnologij.

Univerzalnost in lahka dostopnost do interneta je sprožila razvoj množice računalniških programov, ki preko javnega omrežja IP omogočajo telefonsko storitev. Tovrstne rešitve sicer predstavljajo resno konkurenco navadni telefoniji, vendar imajo tudi veliko pomanjkljivosti. Med njimi najbolj izstopajo odvisnost kvalitete pogovora od zmogljivosti in zasedenosti internetne povezave, manjša zanesljivost zveze, uporabnikova odvisnost od širokopasovnega dostopa in dostopnost do uporabnikov navadne telefonije le preko prehodov. Poleg tega tudi niso del univerzalnega standarda, ki bi omogočal dostop do kateregakoli končnega telefonskega uporabnika na svetu.

Telefonski operaterji se zgornjim težavam izognejo z uporabo svojega ločenega omrežja IP, v katerem lahko nadzorujejo in vzdržujejo potrebno zmogljivost, varnost in zanesljivost. Signalni in medijski prehod prestavita signalizacijo in prenos govora iz omrežja SS7 v omrežje IP in obratno. Operaterji njuno mesto v arhitekturi omrežja določijo glede na vrsto rešitve, ki jo potrebujejo.

Integracija SS7/IP formalno še ni standardizirana s strani mednarodnih ali nacionalnih standardizacijskih organizacij (ITU, ETSI). Večji del protokolnih specifikacij nastaja v IETF v delovni skupini SIGTRAN. Protokolni sklad SIGTRAN sestavlja množica protokolov, prirejenih za različne načine prehoda signalizacije. Celotnemu skladu sta skupna mrežni protokol IP in pa transportni sloj SCTP. Protokol SCTP je bil razvit v delovni skupini SIGTRAN zato, ker TCP in UDP ne izpolnjujeta

strogih zahtev signalizacijskih protokolov in nista najbolj primerna kandidata za protokol transportnega sloja. SCTP kombinira dobre lastnosti TCP in UDP in je načrtovan tako, da zadosti stroge zahteve glede zakasnitev, obenem pa omogoča veliko prilagodljivost, potrebno za zanesljivo delovanje signalizacijskega omrežja. Poudarek SIGTRAN protokolov je predvsem na uporabi redundance in selektivnega potrjevanja prenesenih podatkov. V magistrski nalogi je predstavljena primerjava s protokolnim skladom SS7, ter opis posameznih mehanizmov za zagotavljanje zanesljivosti in redundance. V praktičnem delu so prikazani primeri redundančnih arhitektur in prikaza delovanja realiziranih protokolov.

2. SIGNALNI SISTEM ŠTEVILKA 7

Signalizacija predstavlja način izmenjave krmilnih informacij za vzpostavitev, vodenje in rušenje telekomunikacijske seje med dvema končnima točkama - uporabnikoma omrežnih storitev. Ravno zaradi tega, ker predstavlja osnovo njihovemu delovanju in omogoča storitve, je signalizacija v telekomunikacijskih sistemih ključnega pomena. Signalizacijski protokoli delujejo v krmilni ravnini omrežij. Glede na pozicijo v omrežni strukturi ločimo signalizacijo na vmesniku med uporabnikom in omrežjem ter signalizacijo na vmesnikih v omrežju.

V analognih komunikacijskih omrežjih so za prenos krmilne informacije večinoma uporabljali signalizacijo po pridruženem kanalu (CAS – Channel Associated Signaling). Signalizacija po pridruženem kanalu zagotavlja v analognih omrežjih robustno delovanje, vendar pa te signalizacija ne ustreza zahtevam digitalnih procesorsko krmiljenih komunikacijskih omrežij. Ta omrežja ponujajo v primerjavi z analognimi komunikacijskimi omrežji precej večje področje delovanja že zaradi številnih novih telekomunikacijskih in dodatnih storitev. Ustrezno večja je tudi količina in raznolikost podatkov, ki jih je treba prenesti. Informacije ni več mogoče ekonomično prenašati z običajnimi signalizacijami po pridruženem kanalu. Zato je v digitalnih procesorsko krmiljenih omrežjih potreben nov, zmogljiv signalni sistem.

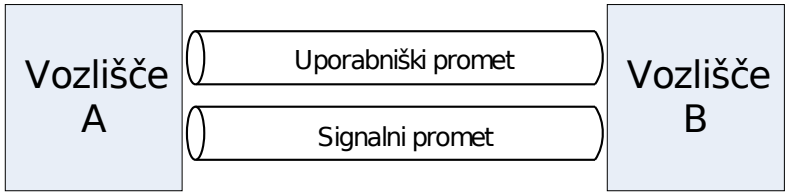
2.1. ZGODOVINA SS7

Z uvajanjem elektronskih procesorjev je v preklopnih (switching) sistemih nastopila možnost signalizacije po skupnem kanalu. To je signalna metoda izven prenosnega medija (out-of-band), kjer se skupni podatkovni kanal uporablja za prenos signalne informacije, ki se nanaša na večje število linij. V sredini šestdesetih let prejšnjega stoletja je CCITT (Consultative Committee for International Telegraphy and Telephony) uvedel standarde za signalizacijo po skupnem kanalu (imenovano CCS6). Usmerjanje je bilo na osnovi permanentnih navideznih zvez. CCS6 ni imel večslojne strukture. Načrtovan je bil za 2,4 kbit/s prenos, zato so bila sporočila kratka in enake dolžine. Leta 1980 so bili dodani datagrami in sporočila v obliki vprašanj, ter

povezava s centraliziranimi podatkovnimi bazami. Uvedli so servis 800 (freephone) in calling card service.

V sredini osemdesetih let prejšnjega stoletja je CCITT naredil korak naprej in postavil standarde za današnjo signalizacijo številka 7 (SS7). Priporočila so pisana v skladu s OSI nivojsko arhitekturo, uporabljen pa je bil bitno orientiran protokol HDLC (HigH Level Data Link Control). Sodobna vodovno komutirana omrežja dandanes uporabljajo signalizacijska omrežja številka 7 (SS7). Protokoli SS7 so namenjeni izmenjavi krmilnih sporočil med elementi omrežja. Krmilne funkcije v omrežnih elementih uporabljajo vsebino signalnih sporočil za usmerjanje, rezervacijo virov, prevedbo naslovov, vzpostavitev in upravljanje klica, ter zaračunavanje.

Slika 1: Signalizacija po pridruženem kanalu



Slika 2: Signalizacija po skupnem kanalu

2.2.ARHITEKTURA SIGNALNEGA OMREŽJA

Signalno omrežje sestavljajo signalne točke in podatkovne signalne povezave (ang. signalnig data links) med temi točkami. Signalna sporočila se prenašajo prek signalnih povezav v sporočilih različne dolžine, ki jih imenujemo signalni stavki (ang. signal unit). Imamo tri vrste signalnih stavkov, ki se ločijo po indikatorju dolžine. To so polnilni stavek FISU (Fill In Signal Unit), ki se prenaša kadar ni drugih stavkov, statusni stavek LSSU (Link Status Signal Unit) za prenos kontrolnih informacij in sporočila, ki se prenašajo v MSU (Message Signal Unit) signalnih stavkih. Signalna sporočila se med vozlišči prenašajo v

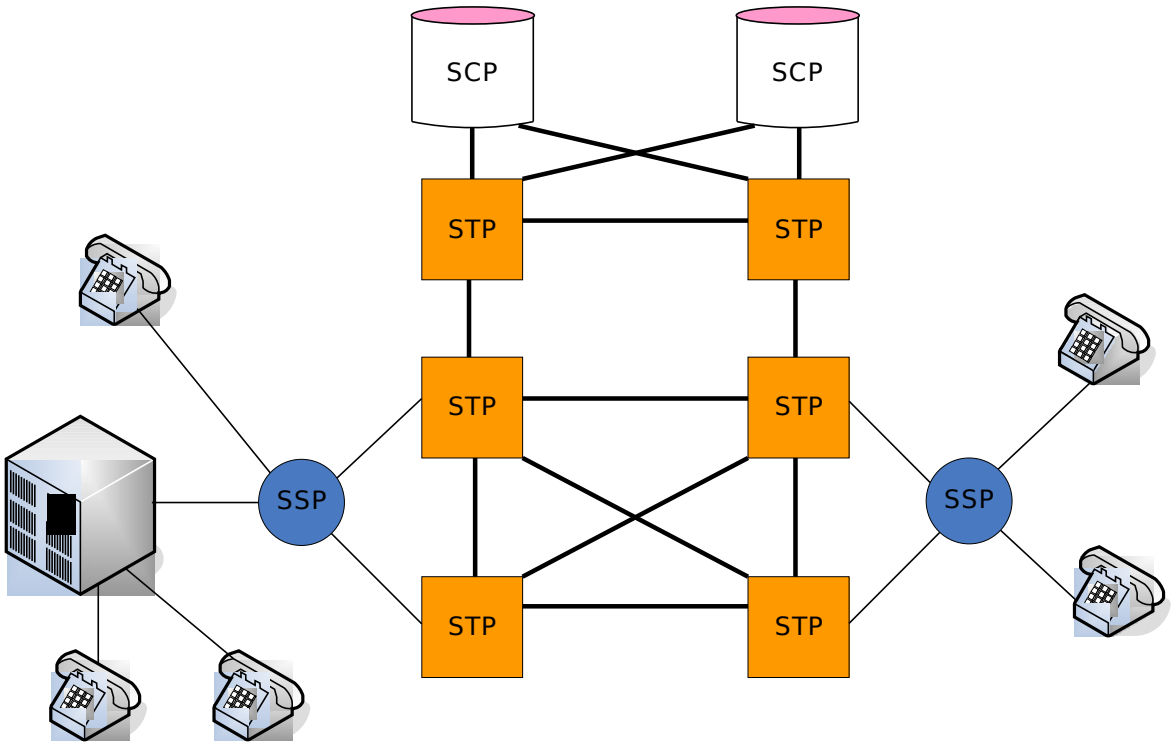
paketih s postopkom t. i. paketne komutacije, kar zagotavlja boljšo izrabo signalnih povezav. Ločimo tri vrste signalnih točk: storitvene komutacijske točke (SSP – Service Switching Point), signalne prenosne točke (STP – Signalling Transfer Point), ter storitvene krmilne točke (SCP – Signalling Control Point).

2.2.1.SIGNALNE TOČKE

Signalne točke zagotavljajo dostop do signalizacijska omrežja SS7, dostop do podatkovnih baz, ter usmerjajo sporočila do ostalih točk znotraj omrežja. Svetovno signalno omrežje je razdeljeno na dve ravni, ki sta funkcijsko neodvisni:

- mednarodna raven z enim mednarodnim omrežjem,
- nacionalna raven z mnogimi nacionalnimi omrežji.

Vsako omrežje ima svoj lastni načrt oštevilčenja signalnih točk. Vsaka signalna točka je v omrežju SS7 enolično določena s kodo vozlišča (PC – point code).



Slika 3: Signalne točke

2.2.1.1.Storitvena komutacijska točka

Storitvena komutacijska točka (SSP) predstavlja lokalno stikalo ali centralo, kjer se klici dejansko začenjajo in zaključujejo. Od tod izvirajo signalna sporočila z zahtevami za vzpostavitev, upravljanje in sproščanje zveze, ki si jih med sabo izmenjujejo različni SSP-ji. V primeru določenih storitev in klicev (številke 800,...) pošilja SSP sporočila za poizvedo in pridobitev informacij (usmerjanje klica) v centralno podatkovno bazo (SCP). V primeru uspešne poizvedbe lahko usmeri določen klic na ustrezno vozlišče.

2.2.1.2.Prenosna signalna točka

Vsa sporočila SS7 potujejo med dvema končnima točkama preko prenosnih signalnih točk (STP). STP deluje kot stikalo, ki na osnovi informacije na 3. sloju (shranjene v sporočilu SS7), usmerja pakete po omrežju do ustrezne končne točke.
Poznamo tri nivoje prenosnih signalnih točk:

- nacionalne prenosne signalne toče,
- internacionalne prenosne signalne točke,
- prehodna prenosna signalna točka.

2.2.1.3.Storitvena krmilna točka

Storitvena krmilna točka (SCP) služi kot vmesnik za dostop do podatkovnih baze telefonskih združb. Podatkovne baze shranjujejo informacije o naročnikih, parametre za usmerjanje posebnih telefonskih številk, varujejo pred zlorabami in nepooblaščenimi uporabniki,... Namen in tip baze je odvisen od samega omrežja. Vsak ponudnik storitev ima različne zahteve, zato se njihove baze ponavadi med seboj razlikujejo. Spodaj je naštetih nekaj tipičnih baz, ki se uporabljajo v raznih omrežjih:

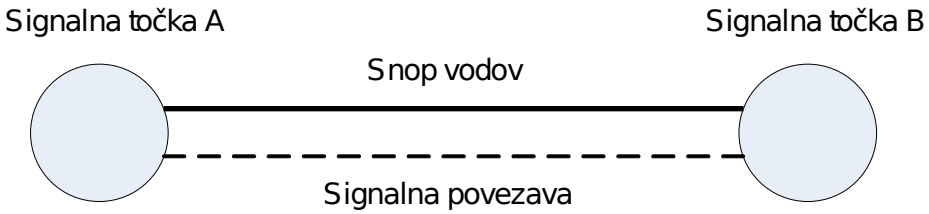
- sistem za podporo obratovanju (OSS – Operational Support System),
- strežnik za upravljanje s klici (CMSDB – Call Management Services Database),
- register domačih naročnikov (HLR – Home Location Register),…

2.2.2.PODATKOVNE SIGNALNE POVEZAVE

Vsa vozlišča v omrežju SS7 so povezana s podatkovnimi signalnimi povezavami. Signalna povezava je sestavljena iz signalne podatkovne povezave (dva podatkovna kanala z isto hitrostjo prenosa, 64kbit/s, neodvisna od smeri) in iz njegovih krmilnih prenosnih funkcij. Sam protokol SS7 je specificiran neodvisno od strukture omrežja, v principu pa je med dvema signalnima točkama več kot ena signalna povezava. Tako zagotovimo strogim zahtevam za razpoložljivost (10 minut izpada na leto) in zanesljivost. Če signalna povezava odpove, funkcije SS7 zagotovijo, da se signalni promet preusmeri na alternativne smeri, na katerih ni okvar. Usmerjanje na dveh signalnih povezavah med dvema signalnima točkama se lahko razlikuje. Vse signalne povezave med dvema signalnima točkama so združene v skupino signalnih povezav.

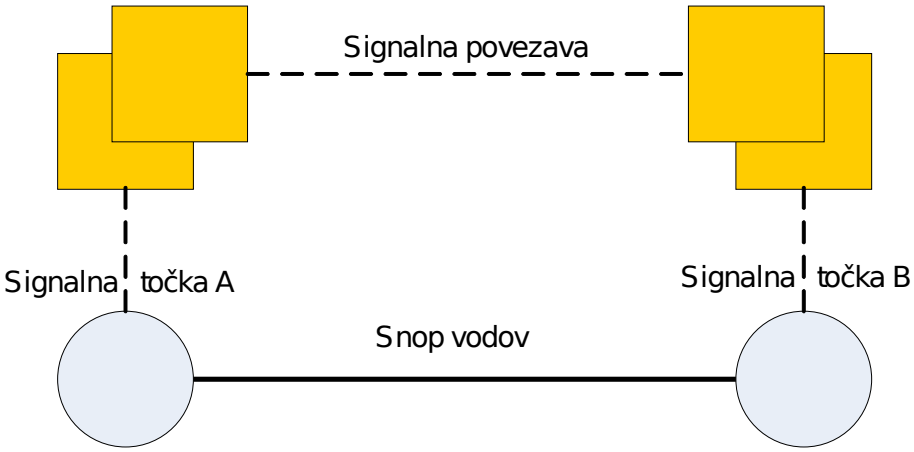
Signalno omrežja uporabljajo tri različne načine signalizacije glede na zvezo med potmi, po katerih potujejo signalna sporočila:

- pridruženi način signalizacije (associated signaling). Pri pridruženem načinu signalizacije se signalna povezava usmerja skupaj s snopom vodov (podatkovni vod), ki pripadajo povezavi. Z drugimi besedami, signalna povezava je neposredno priključena k signalnima točkama, ki sta hkrati končni točki snopa vodov (slika 4). Ta način signalizacije se priporoča tam, kjer je zmogljivost prometne zveze med signalnima točkama A in B polno zasedena.



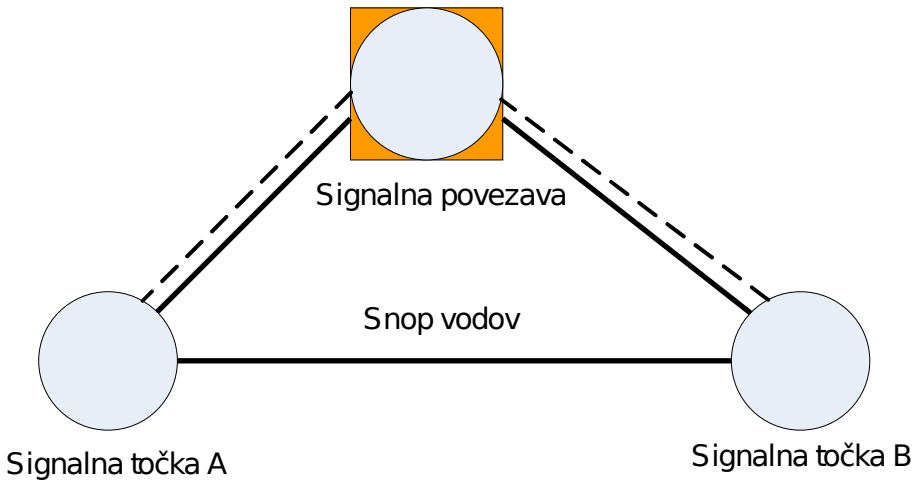
Slika 4: Pridruženi način signalizacije

- nepridruženi način signalizacije (non-associated signaling). Pri nepridruženem načinu signalizacije je signalna povezava ločena od snopa vodov. V večini primerov potuje signalna povezava preko več vmesnih signalnih vozlišč. Nepridruženi način signalizacije se najpogosteje pojavlja v omrežjih SS7.



Slika 5: Nepridruženi način signalizacije

- kvazi pridruženi način signalizacije (quasi-associated signaling). Pri kvazi pridruženem načinu signalizacije potujeta signalna povezava in snop vodov po različnih smereh, vendar snop vodov neposredno povezuje signalno točko A s signalno točko B. V tem načinu se signalizacija za skupino vodov prenaša čez eno ali več določenih signalnih prenosnih točk (slika 6). Ta način signalizacije je primeren za prometne zveze z nizko stopnjo izkoriščenosti zmogljivosti, ker lahko isto signalno povezavo uporabimo za več namembnih točk.

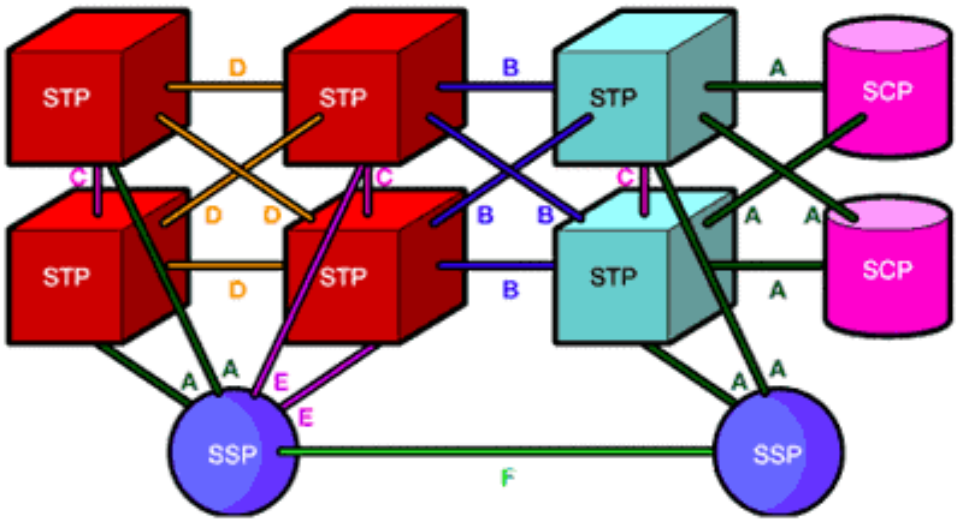


Slika 6: Kvazi pridruženi način signalizacije

2.2.2.1.Definicija signalnih povezav

Signalne povezave so logično razdeljene na različne tipe (od A do F) glede na njihovo uporabo v SS7 omrežju (slika 7).

- Dostopovne povezave (Access links – 'A'). Povezujejo uporabnike signalizacije s prenosnimi signalnimi točkami.
- Mostne povezave (Bridge links – 'B'). Povezujejo prenosne signalne točke na istem hierarhičnem nivoju. Tipično so razporejene v križno strukturo.
- Križne povezave (Cross links – 'C'). Povezujejo dve prenosni signalni točki, ki sta v paru. Prenosne signalne točke so v praksi postavljene v paru, da je zagotovljena redundanca.
- Diagonalne povezave (Diagonal links – 'D'). Povezujejo prenosne signalne točke na različnih hierarhičnih nivojih.
- Razširjene povezave (Extended links – 'E'). Povezujejo storitvene komutacijske točke z alternativnimi prenosnimi signalnimi točkami. Uporabljajo se v primeru zgostitev prometa na osnovnih povezavah.
- Popolnoma združene povezave (Fully associated links – 'F'). Povezujejo dve storitveni komutacijski točki. V omrežjih s prenosnimi signalnimi točkami se te povezave običajno ne uporabljajo, v omrežjih brez prenosnih signalnih točk pa direktno povezujejo končne uporabnike.

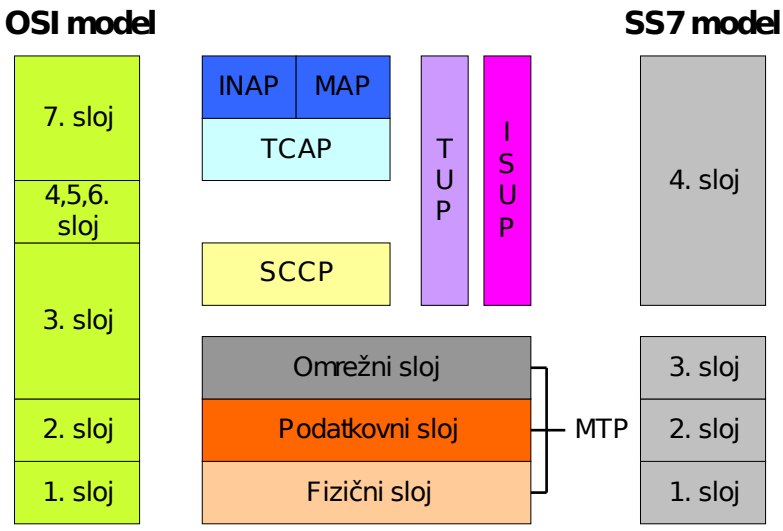


Slika 7: Vrste signalnih povezav [9]

2.3.PROTOKOLNI SKLAD SS7

Arhitektura protokolnega sklada SS7 je prikazana na sliki 8. Z nje je razvidna tudi umestitev posameznih protokolnih slojev v OSI model. Protokolno arhitekturo sestavljajo omrežni storitveni del NSP (Network Service Part) ter uporabniški del (User Part), ki predstavlja višje protokolne sloje in se nanaša na uporabnike signalnega omrežja (uporabniška signalizacija).

NSP sestavljata MTP (Message Transfer Part) in SCCP (Signalling Connection Control Part). Del za prenos sporočil sestavljajo trije sloji, ki opravljajo funkcije signalnega podatkovnega voda, signalnega voda in signalnega omrežja. MTP omogoča nepovezavno usmerjen prenos signalnih sporočil preko omrežja do določenega ponora (uporabnika). Funkcije, ki so vgrajene v MTP, omogočajo, da se v primeru posameznih okvar v signalnem omrežju nadaljuje prenos sporočil brez opaznih sprememb za uporabnika. SCCP zagotavlja dodatne funkcije k MTP za povezavne in nepovezavne omrežne storitve. MTP je bil definiran pred SCCP in je ukrojen po meri "real-time" zahtev telefonskih aplikacij. Zaradi nepovezavnega (datagramskega) prenosa sporočil je potrebno manj administriranja in navideznih zvez. Sčasoma je postalo jasno, da bi druge aplikacije potrebovale dodatne storitve in dodatne možnosti naslavljanja. Povezavno orientiran prenos sporočil SCCP je bil razvit, da zadovolji te potrebe in se uporablja samo za podporo določenih storitev (na primer podpora TCAP protokola).

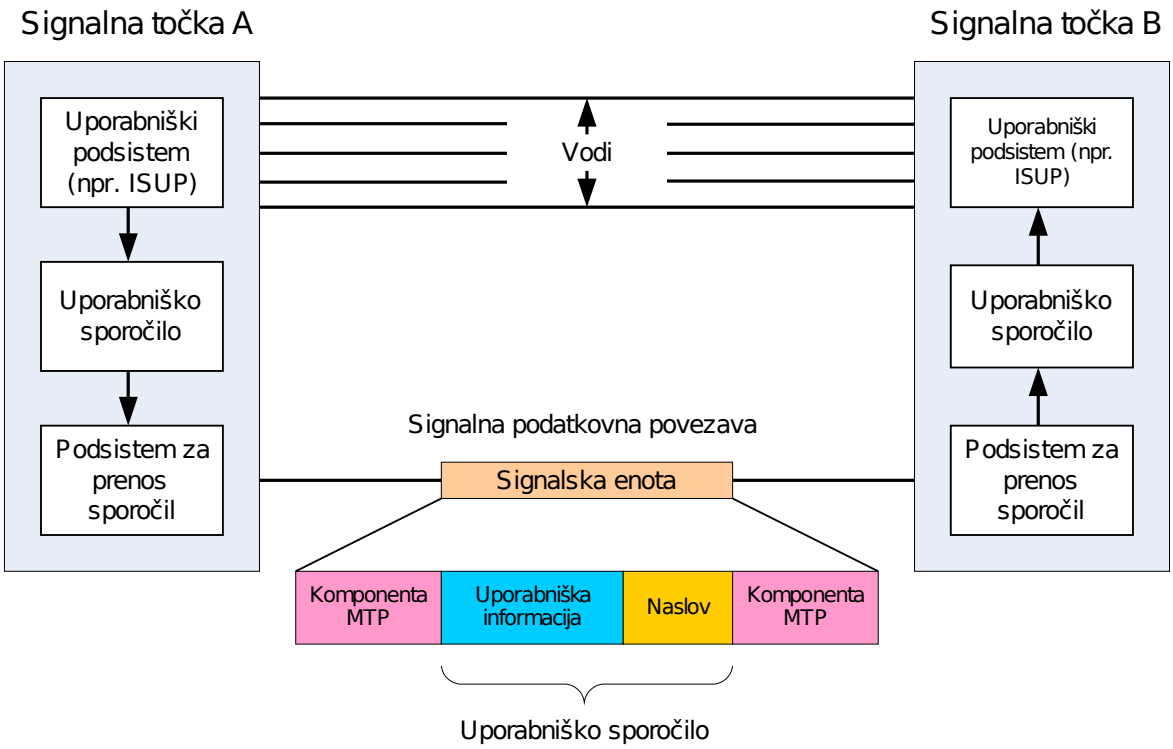


INAP: Intelligent Network Application Part
MAP: Mobile Application Part
TCAP: Transaction Capabilities Application Part
SCCP: Signalling Connection Control Part
TUP: Telephone User Part
ISUP: ISDN User Part
MTP: Message Transfer Part

Slika 8: Protokolni sklad SS7

2.3.1.PODSISTEM ZA PRENOS SPOROČIL

Podsistem za prenos sporočil (MTP – Message Transfer Part)) uporabljajo vsi uporabniški podsistemi v signalizaciji SS7 kot transportni sistem za izmenjavo sporočil. Sporočila, ki se prenašajo od enega uporabniškega podsistema k drugemu, se predajo podsistemu za prenos sporočil (slika 9). Podsistem za prenos sporočil zagotavlja, da bodo sporočila dosegla naslovljeni uporabniški podsistem v pravilnem zaporedju, brez izgube informacije, podvajanja in brez bitnih napak.



Slika 9: Izmenjava sporočil med dvema signalnima točkama

2.3.1.1.Signalni podatkovni vod

Signalni podatkovni vod (MTP1) je dvosmerna prenosna pot za signalizacijo, ki se sestoji iz dveh podatkovnih kanalov, ki delujeta skupno v nasprotnih smereh z isto prenosno hitrostjo. Signalni podatkovni vod se sestoji iz digitalnih prenosnih kanalov in njihove terminalne opreme (DCE - Data Circuit Terminating Equipment) ali opreme za dostop preko časovnih oken (time slot access), ki ima priključek na signalni terminal. Dostop do digitalnega prenosnega kanala je lahko izveden preko bloka digitalnega preklapljanja. Preklapljanje lahko zagotavlja tudi avtomatsko rekonfiguracijo kanalov za signalne povezave. Digitalni prenosni kanali so lahko vzeti iz digitalnega multipleksnega toka, ki ima strukturo okvirjev kot je definirana za PCM (Pulse Code Modulation) opremo ali za podatkovna vezja. Analogna signalna podatkovna povezava je sestavljen iz govornega analognega kanala in modemov. Prenosni kanali so lahko zemeljski ali preko satelita.

Za digitalne signalne podatkovne povezave je od CCITT priporočena hitrost 64 kbit/s. Lahko se uporabljajo tudi nižje hitrosti (do 4.8 kbit/s). Ponekod se uporabljajo tudi višje hitrosti (2.048 Mbit/s).

2.3.1.2.Funkcije signalnega voda

Skupaj s signalnim podatkovnim vodom funkcije signalnega voda (MTP2) omogočajo zanesljiv prenos signalnih sporočil med dvema direktno povezanima signalnima vozliščema. Signalna sporočila se prenašajo preko signalne povezave v sporočilih različne dolžine, ki jih imenujemo signalne stavke (signal unit). Imamo tri vrste signalnih stavkov, ki se ločijo po indikatorju dolžine (LI - length indicator). To so polnilni stavek FISU (Fill In Signal Unit), ki se prenaša kadar ni drugih stavkov, statusni stavek LSSU (Link Status Signal Unit) za prenos kontrolnih informacij in sporočila, ki se prenašajo v MSU (Message Signal Unit) signalnih stavkih. Velikost polja SIF (Signalling Information Field) v sporočilih MSU mora biti manjša od 272 oktetov. Ta omejitev je postavljena zaradi zakasnitve, ki jo eno sporočilo lahko povzroči drugim sporočilom zaradi časa oddajanja (za 64 kbit/s).

2.3.1.3.Funkcije signalnega omrežja

Funkcije signalnega omrežja (MTP3) določajo funkcije in postopke za prenos sporočil med signalnimi točkami, ki so vozlišča signalnega omrežja. Funkcije signalnega omrežja lahko razdelimo na dve osnovni kategoriji:

- rokovanje s signalnimi sporočili (SMH – Signalling Message Handling) in
- upravljanje signalnega omrežja (SNM – Signalling Network Management).

2.3.2.SCCP

Krmilni del signalne zveze (SCCP – Signalling Connection Control Part) dopolnjuje storitve MTP, s čimer je dosežena funkcionalna enakost z OSI omrežnim slojem. SCCP ima razširjene naslovne zmogljivosti v primerjavi z MTP (DPC + SSN). SSN (Subsistem Number) je naslovna informacija, ki jo SCCP uporablja za razlikovanje med posameznimi uporabniki v posameznem vozlišču). Druga razširitev naslavljanja je uporaba globalnih naslovov (GT – Global Title). MTP3 je sposoben samo naslavljanja do sosednjih vozlišč. SCCP (globalni naslovi so "pravi naslovi" končnih uporabnikov omrežnega sloja). MTP teh naslovov ne more direktno uporabiti za usmerjanje, zato mora SCCP sloj zagotoviti

ustrezno prevajanje GT v DPC+SSN. Prevedba se lahko izvede v izvornem ali kakšnem od vmesnih signalnih vozlišč (STP).

SCCP funkcije nadgradijo servise MTP, da zagotovijo funkcionalni ekvivalent z OSI mrežnim slojem 3. SCCP je sicer uporabnik MTP sloja in je torej 4.sloj v protokolnem skladu SS7. Možnosti naslavljanja MTP-ja so omejene na dostavo sporočil v vozlišče in s 4 bitnim indikatorjem SI (podpolje v SIO) za distribucijo sporočil znotraj vozlišča. SCCP omogoča dodatne možnosti naslavljanja, saj k DPC doda številke podsistema SSN (Subsystem Numbers). SSN je lokalna naslovna informacija, ki se uporablja v SCCP za določitev posameznega uporabnika v vozlišču. Dodatna je še možnost naslavljanja sporočil z globalnimi naslovi, ki so lahko klicane številke, in ne vsebujejo eksplicitne informacije uporabne za usmerjanje v MTP. Za globalno naslavljanje imamo v SCCP možnost pretvarjanja iz globalnih naslovov v DPC in SSN. Ta pretvorba se lahko izvede pri izvornem vozlišču sporočila ali pa v drugih vozliščih v omrežju (npr. v STP).

Poleg tega SCCP nudi štiri razrede storitev (dve nepovezavni in dve povezavni storitvi):

- razred 0 : Basic connectionless class
- razred 1 : Sequenced (MTP) connectionless class
- razred 2 : Basic connection-oriented class
- razred 3 : Flow control connection-oriented class

2.3.3.UPORABNIŠKI PODSISTEM

Uporabniški podsistem sestavljajo uporabniki, ki uporabljajo MTP in SCCP transportne storitve:

- TUP (Telephone User Part), DUP (Data User Part). Oba sta s svojo funkcionalnostjo pokrita z ISUP protokolm.
- ISDN User Part (Integrated Services Digital Network User Part)
- TCAP (Transactions Capabilities Application Part)
    - *OMAP (Operations, Maintenance and Administration Part),*
    - *INAP (Intelligent Network Application Part),*
    - *MAP (Mobile Application Part).*

2.3.3.1.TUP

Telefonski uporabniški del skrbi za kontrolo klica pri klasični analogni telefonski liniji. Večinoma se ne uporablja več (razen še v nekaterih vzhodnih državah), saj ga zamenjuje ISUP, ki podpira prenos podatkov, uporabo dodatnih storitev in napredne inteligentne storitve.

2.3.3.2.ISDN User Part

Uporabniški del za digitalno omrežje integriranih storitev predstavlja definicijo postopkov in protokolov, ki se uporabljajo za vzpostavitev, upravljanje in rušenje zvez. Zveze omogočajo med uporabniki ISDN omrežja prenos podatkov ali govorno komunikacijo. Pred ISUP-om je bil specificiran telefonski uporabniški del (TUP), ki je zagotavljal signalizacijske funkcije za podporo krmiljenja telefonskih povezav. ISUP omogoča vse funkcije, ki jih podpira TUP, poleg tega pa še dodatne funkcije za podporo negovornih klicev in naprednih ISDN in IN (Inteligent Network) storitev. ISUP uporablja storitve MTP za zanesljiv zaporedni prenos signalnih sporočil med centralami. Lahko uporablja tudi storitve SCCP kot možnost za signalizacijo od konca do konca (end-to-end). V skladu s OSI modelom poteka izmenjava informacije med ISUP in MTP (ali SCCP) z uporabo parametrov, ki se prenašajo v mednivojskih primitivih. Vsa sporočila imajo usmerjevalno labelo, ki je dejansko glava tretjega sloja. Nato sledita identifikacijska koda kanala - CIC (Circuit Identification Code) in koda za tip sporočila, ki enoumno določa funkcijo ter format vsakega ISUP sporočila (obstaja več vrst sporočil, ki glede na funkcije delijo v skupine).

ISUP protokol natančno določa izmenjavo sporočil in procese krmiljenja zveze. Vzpostavitev zveze med dvema končnima točkama omrežja, vzemimo na primer med centralama ISDN, v grobem poteka na sledeč način:

1. Klicoča stran (izvorna signalna točka) pošlje začetno naslovno sporočilo (Initial Address Message, IAM) svoji sosednji centrali na poti k centrali, na katero je priključen pozvani naročnik. Vsaka vmesna centrala usmeri IAM sporočilo do naslednje centrale v zvezi, glede na klicano naročniško številko v ISUP sporočilu. Obenem rezervira prost komutiran kanal na dohodnem spojnem vodu. V primeru, da na voljo ni prostih zmogljivosti, bo centrala to ustrezno signalizirala.

2. Ponorna centrala najprej pregleda klicano številko, ugotovi ali naročnik obstaja in v primeru prostega naročnika vrne izvorni centrali sporočilo popolnega naslova (Address Complete Message, ACM), ki se vrne po isti poti, kot zahteva za zvezo IAM. Izvorna centrala rezervira kanal na dohodnem spojnem vodu in začne s pozivanjem naročnika. Vmesne centrale ob prejemu ACM rezervirajo še odhodni kanal ter ustrezno nastavijo stikalno polje. Izvorna centrala ob prejemu ACM poveže komutiran kanal z linijo klicočega in klicočemu sproži signal pozivanja.
3. Zveza med naročnikoma se dejansko vzpostavi, ko izvorna centrala prejme odzivno sporočilo (Answer Message, ANM), ki ga je poslala ponorna centrala kot posledica dviga slušalke klicanega naročnika. Obenem lahko začne s tarifiranjem.
4. Po prekinitvi zveze tista stran, ki je prekinitev izvedla, pošlje drugi prekinitveno sporočilo (Release Message, REL), na podlagi katerega klicana stran sprosti prenosno pot in odgovori s sporočilom dovršene prekinitve (Release Complete Message, RCM). Prekinitveno sporočilo se pošilja tudi v primeru zasedenega naročnika. Vsaka centrala po prejemu RCM sprosti zasedene kanale, izvorna centrala pa preneha s tarifiranjem.

2.3.3.3.TCAP

Aplikacijski del za transakcijske zmožnosti uporabljajo za medsebojno komunikacijo aplikacije, ki so raztresene po omrežju. Po terminologiji SS7 predstavlja TCAP protokol aplikacijskega sloja. TCAP direktno uporablja SCCP in zagotavlja skupino orodij v nepovezavnem okolju, ki jih uporablja aplikacija v enem vozlišču, da pokliče izvajanje postopkov v drugem vozlišču. Omogočena je tudi izmenjava rezultatov teh pozivov, ki vsebuje protokole in storitve za izvajanje oddaljenih operacij. V telekomunikacijskem omrežju se porazdeljene aplikacije, ki uporabljajo TCAP, lahko nahajajo v centralah in v podatkovnih bazah. TCAP se uporablja za realizacijo inteligentnih omrežij in storitev (npr. storitev 800 - brezplačen klic) z uporabo nepovezavno orientiranih SCCP storitev.

OMAP

Obratovalno vzdrževalni administrativni del (OMAP – Operation, Maintenance and Administration Part) vsebuje aplikacijske protokole in

procedure za opazovanje, koordiniranje in kontrolo elementov omrežja, ki omogočajo SS7 komunikacijo. Zbirka vseh funkcij opazovanja, kontrole in koordinacije nad aplikacijskim slojem se imenuje SMAP (System Management Application Process). Vsi podatki za vodenje, ki se prenašajo ali spreminjajo, se nahajajo v MIB (Management Information Base). Ti podatki se zbirajo s posredovanjem MIB na vseh slojih preko LMI (Layer Management Interface). SMAP uporablja storitve TCAP preko OMAP-ASE. Primer OMAP-ASE je MRVT (MTP Routing Verification Test), ki uporablja nepovezavno orientirane TCAP storitve. MRVT postopek omogoča odkrivanje napak, ko so: kroženja sporočil, predolge poti, prevelike zakasnitve, nedostopnost signalnih vozlišč in drugih nepravilnosti. Dodatni OMAP postopki omogočajo preverjanje SCCP usmerjanja in pretvarjanja iz globalnih naslovov. OMAP postopki lahko vsebujejo še vodenje podatkov za usmerjanje, testiranje vezij, vodenje ob okvarah opreme za signalne povezave, iskanje napak, zbiranje podatkov, kontrolo v realnem času, itd...

INAP

Aplikacijski protokol inteligentnega omrežja (INAP – Intelligent Network Application Part) je protokol, namenjen uporabi v inteligentnih omrežjih. Protokol omogoča upravljanje storitvenega vozlišča z uporabo nadzornega vozlišča. Uporablja se lahko tudi v zlitih omrežjih.

MAP

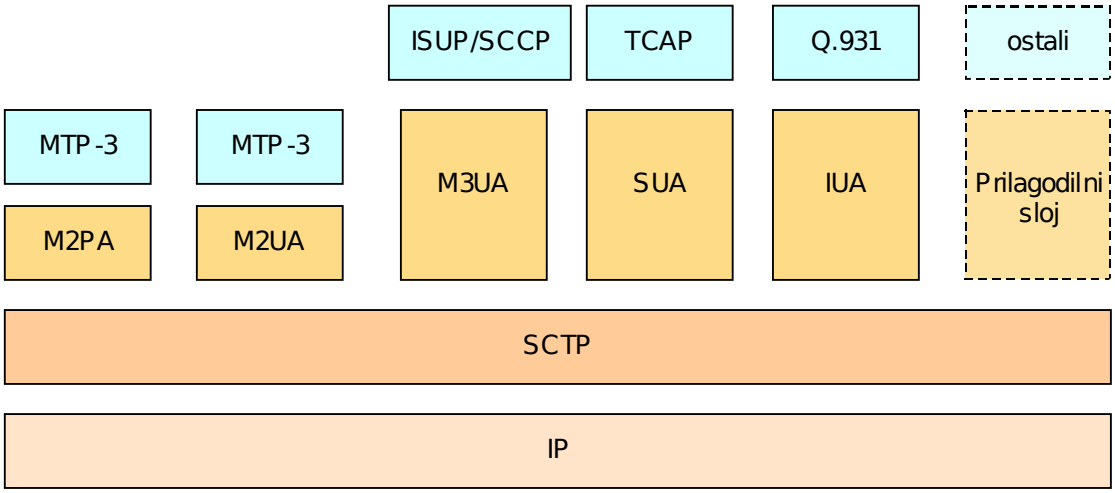
Mobilni aplikacijski del (MAP – Mobile Application Part) je protokol, ki se uporablja v GSM omrežju znotraj omrežnega komutacijskega podsistema za komunikacijo med različni storitvami (gostovanje, SMS sporočila, overitev uporabnika). MAP predstavlja aplikacijski sloj na katerem se gradijo storitve, ki jih podpira GSM omrežje.

3. SIGTRAN

Prenos klasične telekomunikacijske signalizacije prek omrežij IP ponuja več različnih scenarijev uporabe. IETF jih navaja v opisu splošnih zahtev za signalizacijo številka sedem prek omrežij IP, izdanem v RFC 2719 [1]. Delovna skupina SIGTRAN, ki je ta opis izdelala, posebno pozornost posveča prenosu signalizacije med signalnim prehodom (SG – Signaling Gateway) in krmilniku medijskega prehoda (MGC – Media Gateway Controller), ki sta opisana v nadaljevanju.

3.1. PROTOKOLNI SKLAD SIGTRAN

Protokolni sklad SIGTRAN je skupina potrebnih protokolov za zanesljiv prenos signalizacij preko omrežja IP. Na sliki 10 je prikazana struktura sklada. Nad mrežnim protokolom IP je na transportnem sloju uporabljen protokol SCTP. Sledijo prilagodilni sloji (M2UA, M2PA, M3UA, SUA, IUA), ki skrbijo za prilagoditev SCTP protokola višjim uporabniškim slojem protokolnega sklada SS7 (ISUP, SCCP, TCAP, MTP3, Q.931, MAP idr.). S tem je omogočena komunikacija med uporabniškimi sloji v omrežju SS7 prek vmesnega omrežja IP.

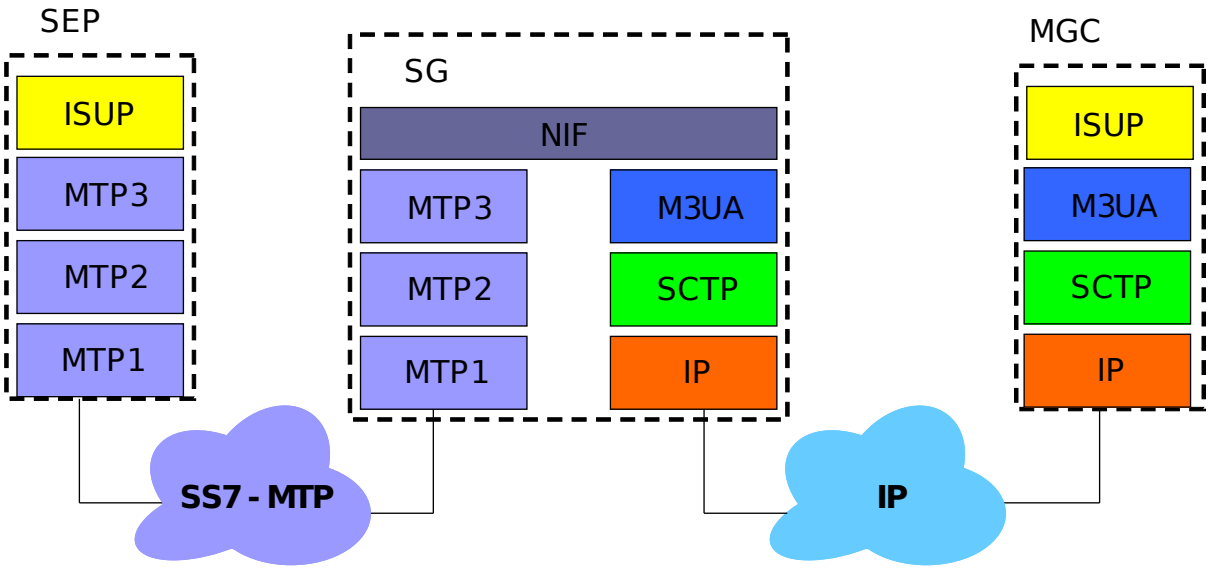


Slika 10: Protokolni sklad SIGTRAN

3.2. SIGNALIZACIJA SS7 V OMREŽJU IP

Spodnja slika prikazuje arhitekturo, v katero je vključen protokol M3UA. Na mestu ISUP sloja lahko nastopa tudi SCCP. Prilagodilni sloji (M2UA, M2PA, M3UA, SUA idr.) omogočajo prehod signalizacije iz

omrežja SS7 na omrežje IP pri različno visokih slojih z različnimi lastnostmi, ki jih podpirajo. V nadaljevanju bom opisal posamezne prilagodilne sloje, protokol M3UA pa bom bolj podrobno in natančno primerjal z SS7 protokolnim skladom, saj je med naštetimi edini, ki je ekvivalenten sloju MTP3 in tudi omogoča največ funkcionalnosti za zanesljiv prenos signalizacije.



Slika 11: Signalni prehod z M3UA

3.2.1.SIGNALNI PREHOD

Signalni prehod je naprava, prek katere si terminali iz omrežij TDM in IP z različnimi signalizacijskimi protokoli izmenjujejo signalna sporočila. SG vsebuje tako protokole iz protokolnega sklada SS7 kot tudi iz SIGTRAN-a. Na sliki 11 je prikazana celotna struktura s prilagodilnim slojem (NIF – Nodal Inter-working Function), ki omogoča posredovanje sporočil med slojema MTP3 in M3UA. Kjer poteka signalizacija ločeno od toka podatkov, izvorni terminal pošilja signalna sporočila (npr. zahteve za vzpostavitev ali rušenje zveze, potrjevanje ipd.) signalnemu prehodu, ta jih pretvori v protokol drugega omrežja in pošlje ponornemu terminalu. Signalni prehod ima podobno vlogo kot medijski, le da prenaša signalna sporočila in ne samih podatkov. Naprava, ki vključuje medijski in signalni prehod, se navadno imenuje prehod IP.

3.2.2.KRMILNIK MEDIJSKEGA PREHODA

Krmilnik medijskega prehoda je naprava, prek katere lahko terminali iz TDM omrežja komunicirajo s terminali v omrežju IP. MGC zaključuje govorne klice iz omrežja TDM, zgoščuje in paketira govor, ter dostavlja zgoščene govorne pakete omrežju IP. Za govorne klice iz omrežja IP opravlja obratno funkcijo. V omrežjih naslednje generacije (NGN – Next Generation Network) so krmilniki medijskega prehoda ključnega pomena. Omogočajo povezljivost različnih dostopovnih omrežij in hrbteničnega paketnega omrežja in s tem uporabo storitev neodvisno od dostopovnega omrežja.

3.3.IP

IP je protokol, ki spada v mrežno plast OSI modela in je opisan v dokumentu RFC 791. Protokol IP omogoča nepovezavno in nezanesljivo dostavo datagramov med dvema končnima IP naslovoma. Usmerjevalniki na podlagi IP naslovov in drugih kontrolnih informacij usmerjajo datagram na poti do cilja. Dostava deluje po metodi »best effort«, kar pomeni, da se na sloju IP z nobenim postopkom ne zagotavlja, da so datagrami zanesljivo dostavljeni končnemu naslovu. Med potjo je omogočena razdelitev datagramov na manjše dele, kateri se kasneje ponovno sestavijo v prvotni datagram. IP na ta način podpira tudi povezave z različno največjo prenosno enoto (MTU – Maximum Transmission Unit).

V omrežju IP ni časovnega dodeljevanja kapacitet povezave. Omrežje je paketno orientirano, zato v njem večinoma ni zagotovljene stalne hitrosti in zanesljivosti prenosa. Njegove kapacitete, kot so fizične povezave, hitrost stikal, usmerjevalnikov, si dinamično razdelijo vsi trenutni uporabniki, t.i. statistični multipleks.

Usmerjevalniki za usmerjanje IP datagramov potrebujejo informacije o svoji neposredni okolici. Za zbiranje teh informacij uporabljajo različne usmerjevalne protokole. Usmerjevalnik obvešča druge neposredno povezane usmerjevalnike, katera omrežja so dostopna preko njega. Za vsako omrežje se navede poleg dostopnosti tudi uteži (metrike), na podlagi katerih se usmerjevalnik kasneje odloči za ustrezno pot. Uteži so različne informacije o poti do cilja, kot na primer število skokov med

usmerjevalniki do cilja, hitrost, zasičenost povezave, arhitektura omrežja ipd.

Za dostavo IP datagrama od začetne do končne točke lahko obstaja več poti, ki se lahko spreminjajo. Omrežje se dinamično odziva na spremembe, torej ni nujno, da bodo datagrami IP z istim končnim naslovom IP vedno potovali po isti poti. Omrežje je tako bolj robustno, saj se v primeru odpovedi usmerjevalnika ali fizične povezave, promet preusmeri preko drugih usmerjevalnikov. Reakcijski čas, ki ga usmerjevalniki potrebujejo, da zaznajo napako in preusmerijo promet, je sicer relativno hiter, približno od 1 sekunde do 1 minute, vendar pa je še vedno prepočasen za zagotavljanje zanesljive signalizacije.

V omrežju, ki temelji na protokolu IP, omogoča potrjevanje in ponovno pošiljanje sporočil šele protokol za krmiljenje prenosa (TCP – Transport Control Protocol), prenosni protokol s krmiljenjem pretoka (SCTP – Stream Control Transmission Protocol) ali kateri drug višje ležeči sloj. Potrjuje se le na relaciji končnih točk, torej čez celotno pot, na kateri ni enostavno hitro določiti točnega položaja in vzroka morebitne napake.

Slika 12: Potrjevanja sprejetih podatkov v omrežju IP

3.4.SCTP

Protokol SCTP je načrtovan za prenos signalnih sporočil prek protokola IP, njegove zmožnosti pa pokrivajo širši spekter uporabe. Specifikacija protokola je bila pripravljena v IETF SIGTRAN delovni skupini in izdana kot RFC 2960 (oktobra 2000).

SCTP nudi zanesljiv, strukturiran in časovno urejen prenos uporabniških sporočil med istoležnimi uporabniki SCTP. Protokol deluje na potencialno nezanesljivih nepovezavnih paketnih storitvah, kakršne nudi IP. SCTP za povečevanje zanesljivosti uporablja:

- kontrolne vsote (ang. checksum) in zaporedne številke oddaje za odkrivanje napak,

- selektivne potrditve sprejema,
- selektivne ponovitve prenosa za popravljanje napak,
- redundančno arhitekturo omrežja IP,
- večdomnost SCTP točk,
- in preklope med aktivnimi potmi.

3.4.1. IZBIRA TRANSPORTNEGA PROTOKOLA ZA SIGNALIZACIJO

Obstoječi sloj TCP za prenos zanesljive signalizacije preko IP ne nudi zadostne podpore in je preveč omejen. Med omejitvami protokola TCP posebej izstopajo naslednje slabosti:

- Oktetno usmerjen prenos podatkov, zaradi česar mora aplikacija dodajati označevanje sporočila ali podatkovne enote ter uporabljati funkcionalnost potiskanja (push) sporočila, da doseže prenos celotnega sporočila s sprejemljivo zakasnitvijo.
- Zakasnitve zaradi blokade sporočilne vrste, ki so posledica strogega ohranjanja zaporednosti dostave in sestavljanja sporočil na sprejemu. TCP namreč zagotavlja zanesljiv prenos in dostavo podatkov višjemu protokolnemu sloju v enakem zaporedju kot pri oddaji. Določeni uporabniški sloji sicer zahtevajo zanesljiv prenos, obenem pa jim ustreza sekvenčno neurejen ali delno urejen prenos protokolnih podatkovnih enot. Blokada nastane zlasti v primerih, ko se del sporočila izgubi, saj TCP čaka na potrditev prejema.
- Omejeno področje uporabe vtičnic TCP (sockets), ki otežujejo zanesljiv prenos podatkov z večdomnimi gostitelji.
- Omejitev števila hkratnih zvez TCP. Običajno je TCP realiziran na nivoju operacijskega sistema, pri tem je največje število hkratnih zvez TCP določeno z omejitvami jedra operacijskega sistema.
- Nezmožnost aplikacije, da krmili inicializacijo TCP protokola in posega v nastavitve časovnikov.

Z namenom, da se premosti zgoraj omenjene omejitve, je bil razvit protokol SCTP. SCTP združuje lastnosti protokolov TCP in UDP in je prilagojen zahtevam, ki jih narekuje zanesljiva in hitra signalizacija.

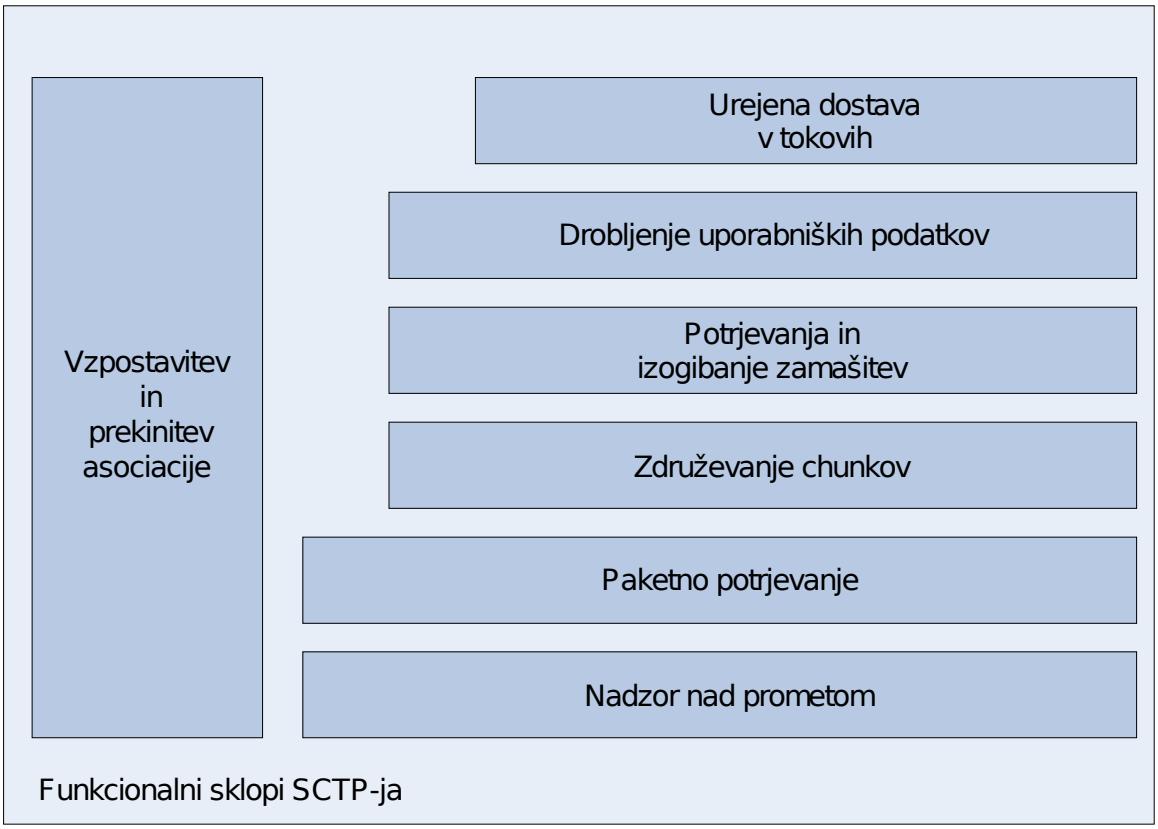
Tabela primerjave SCTP storitev in lastnosti s storitvami in lastnostmi protokolov TCP in UDP:

Lastnosti in storitve	SCTP	TCP	UDP
Full-duplex prenos podatkov	DA	DA	DA
Povezavna usmerjenost	DA	DA	NE
Zanesljivost prenosa podatkov	DA	DA	NE
Urejena dostava podatkov	DA	DA	NE
Neurejena dostava podatkov	DA	NE	DA
Kontrola pretoka in zamašitev	DA	DA	NE
Eksplicitna podpora obveščanja zamašitve	DA	DA	NE
Selektivno potrjevanje	DA	Opcijsko	NE
Večtokovnost	DA	NE	NE
Večdomnost	DA	NE	NE
Varovanje pred SYN napadi poplavljanja	DA	NE	Ni nevarnosti
Polovično odprte povezave	NE	DA	Ni dostopno

Tabela 1: Primerjava protokolnih lastnosti in storitev

3.4.2.POSTOPKI IN LASTNOSTI PROTOKOLA

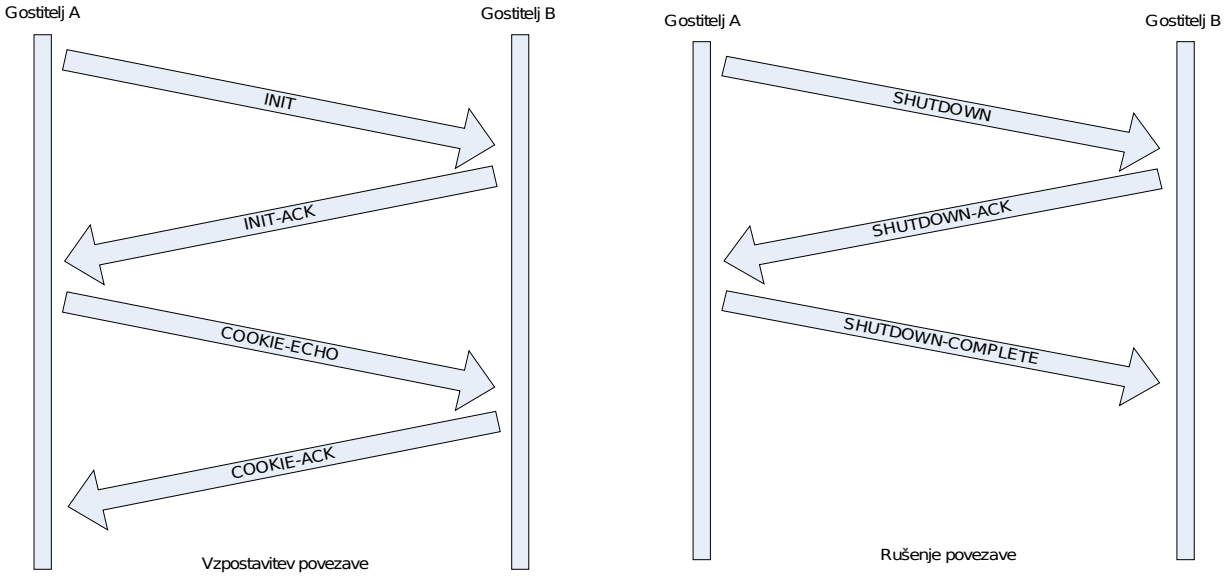
Na sliki 13 je prikazana osnovna razdelitev SCTP protokola na posamezne funkcionalnosti.



Slika 13: Funkcionalnosti SCTP protokola

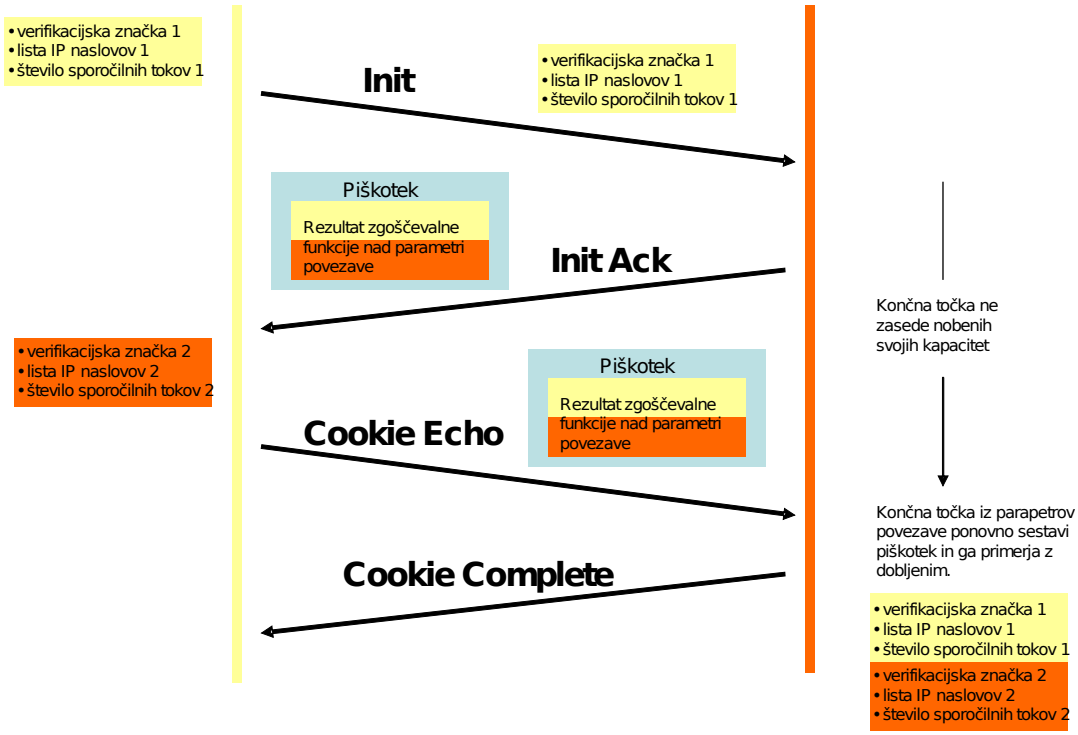
3.4.2.1.Vzpostavljanje in rušenje povezave

Uporabniška aplikacija prek primitivov (ukazov) zahteva vzpostavitev ali rušenje SCTP povezave, prenos podatkov ter izvaja krmilne aktivnosti. Vzpostavitev SCTP povezave poteka na podlagi štirikratne izmenjave sporočil, kot je prikazano na sliki 14. Izmenjava podatkovnih SCTP sporočil (ang. chunkov) steče tako šele po končani vzpostavitveni proceduri. Slednja temelji na izmenjavi naključno generiranih varnostnih značk in piškotkov.



Slika 14: Potek izmenjave sporočil pri vzpostavitvi in rušenju povezave

Potek vzpostavitve povezave s štirikratno izmenjavo je zasnovan tako, da močno otežuje vdiranje v povezavo, spreminjanje in dodajanje vsebine, vzpostavljanje novih povezav in zasedanje kapacitet končne točke. Postopek izmenjave in preverjanja piškotkov povečuje odpornost protokola na slepe storitvene napade (ang. blind denial-of-service), kjer napadalec pošilja zahteve za vzpostavitev povezav in pri tem uporablja lažne IP naslove. Za obe smeri drugačna verifikacijska značka preprečuje dodajanje in spreminjanje zunanje vsebine (paketov SCTP) v pretok povezave.



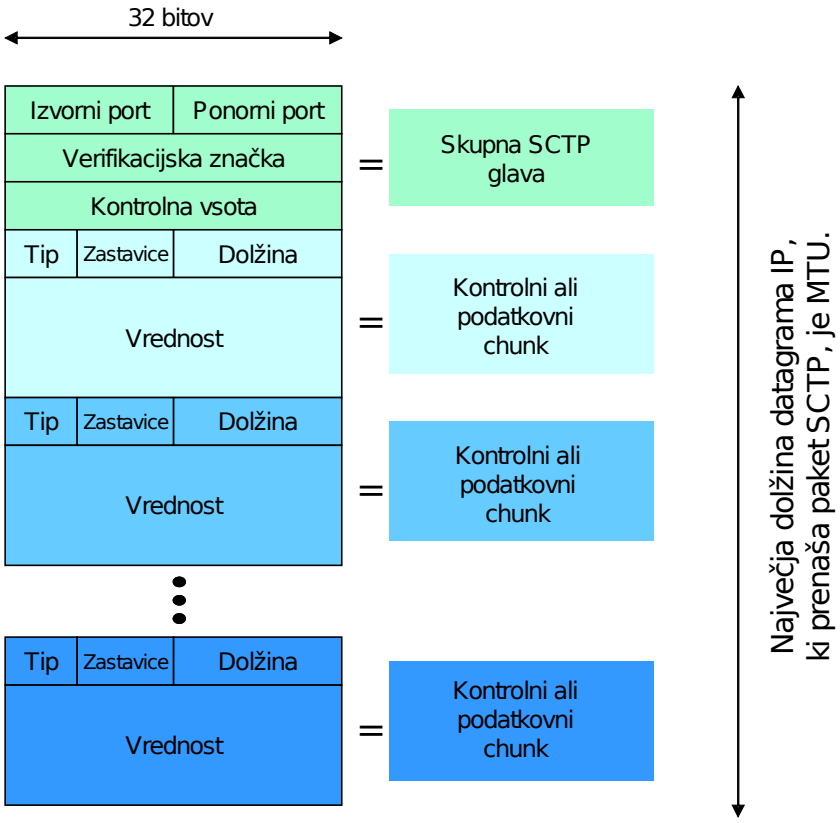
Slika 15: Začetna štirikratna izmenjava sporočil

Čeprav je protokol povezavno usmerjen, je koncept SCTP povezave širši od TCP zveze. Vsaka od dveh SCTP končnih točk pošlje drugi končni točki številko SCTP vrat in listo IP naslovov. Povezava je tako določena z dvema številkama vrat in dvema listama IP naslovov. Dostopnost posamezne SCTP končne točke se spremlja prek vseh njenih transportnih naslovov. Med vzpostavljanjem povezave se končni točki dogovorita o številu dohodnih in odhodnih sporočilnih tokov za dano povezavo. Vsak podatkovni chunk je med prenosom označen z identifikatorjem toka (ang. stream ID).

3.4.2.2.Prenos podatkov

Za razliko od TCP, pri katerem je podatkovni pretok oktetno usmerjen, SCTP prenaša podatkovne sklope v SCTP storitvenih protokolnih enotah, originalno imenovanih chunks. SCTP storitvene protokolne enote vsebujejo uporabniške podatke ali krmilne informacije. Protokol SCTP se je sposoben prilagoditi največji MTU, kar pomeni, da določi največjo velikost protokolne podatkovne enote, pri kateri se IP paketi med prenosom na končno točko ne razstavljajo v manjše enote. Velika sporočila SCTP razstavi v chunke, ki po velikosti ustrezajo prenosu v datagramih IP z največjo velikostjo MTU. Kratka sporočila tvorijo

majhne chunke, ki se lahko sestavljajo v en SCTP paket oziroma en IP datagram. Slika 16 prikazuje sestavljanje paketa SCTP iz več SCTP chunkov.



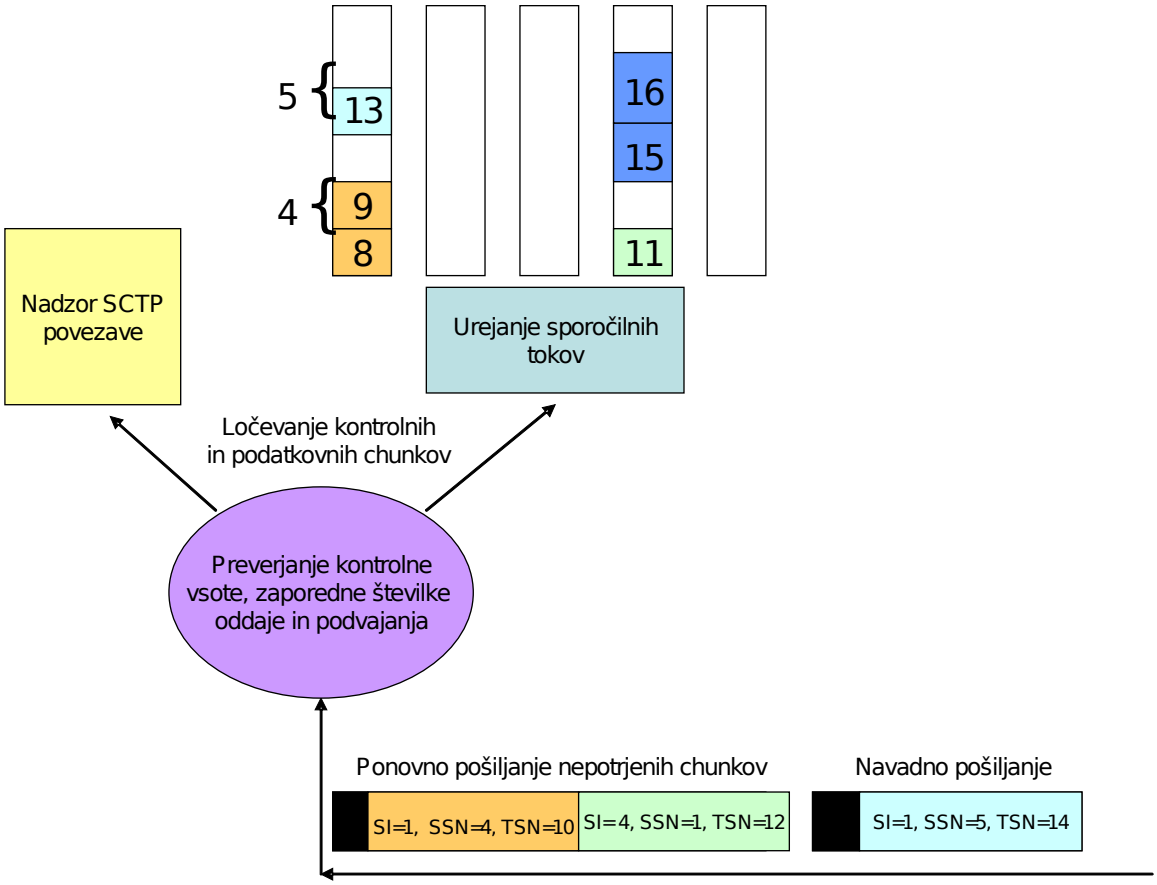
Slika 16: Sestava paketa SCTP

TCP ima strogo shemo urejanja zaporednosti dostavljenih podatkov v okviru celotne povezave. Za razliko od njega ima SCTP prilagodljivo shemo dostave sporočil, ki v okviru ene SCTP povezave ločuje različne sporočilne tokove (ang. stream). Ločevanje med sporočilnimi tokovi pa omogoča dostavno shemo, pri kateri se sporočila razvrščajo glede na pripadnost posameznemu pretoku. Shema ohranja zaporednost dostave sporočila uporabniški aplikaciji samo v okviru posameznega sporočilnega pretoka, zato se tak način pogosto označuje kot delna sekvenčna dostava. Njena prednost je zmanjševanje nepotrebnega blokiranja začetka sprejemne paketne čakalne vrste (ang. head-of-line blocking) med različnimi pretoki. Poleg tega ima SCTP še dodatni postopek, ki omogoča posredovanje sporočila uporabniku takoj, ko je bilo sprejeto v celoti (ang. order-of-arrival delivery).

Funkcije zanesljivega prenosa podatkov so pri SCTP ločene od dostavnega postopka. Slednji se lahko zato neodvisno prilagaja potrebam višjih slojev, ki jim lahko zadošča le delno razvrščanje paketov. SCTP deluje na dveh nivojih, kot prikazuje slika 17:

- Na prvem nivoju povezave se zagotavlja zanesljiv prenos SCTP paketov oziroma v paketih vsebovanih krmilnih in uporabniških chunkov. Omenjena funkcionalnost je dosežena s preverjanjem kontrolne vsote, zaporednih številk oddaje in postopka selektivnega ponavljanja prenosa. Vsak pravilno dostavljen podatkovni - uporabniški chunk se nato odda na višji nivo.
- Drugi nivo izvaja postopek prilagodljive dostave podakovnih chunkov, ki se jih obravnava glede na pripadnost posameznim sporočilnim pretokom. Nadzor sekvenčnosti se tako izvaja samo nad podatkovnimi chunki istega pretoka. Identifikator sporočilnega pretoka se nahaja v glavi podatkovnega chunka.

Slika 17 prikazuje potek razvrščanja prispelih chunkov v sporočilne tokove. Vsak chunk vsebuje zaporedno številko oddaje (TSN – Transmission Sequence Number), identifikator sporočilnega toka (SI – Stream Identificator) in zaporedno številko sekvence v toku (SSN – Stream Sequence Number). Uporabniškemu sporočilu, ki zahteva zaporedno dostavo, se dodeli zaporedni SSN. V primeru, da je sporočilo preveliko, se ga razstavi na manjše chunke ter vsakemu od teh dodeli nov zaporedni TSN. Na sliki je prikazan tudi primer, kjer se zaradi izgube SCTP paketa zakasni posredovanje sporočil na sporočilnih tokovih 1 in 4. Čeprav je v sporočilnem toku 4 v celoti sprejeto naslednje sporočilo (na sliki v modri barvi), se le to ne bo posredovalo višjemu sloju, dokler se v celoti ne sprejme predhodno sporočilo (na sliki v zeleni barvi).



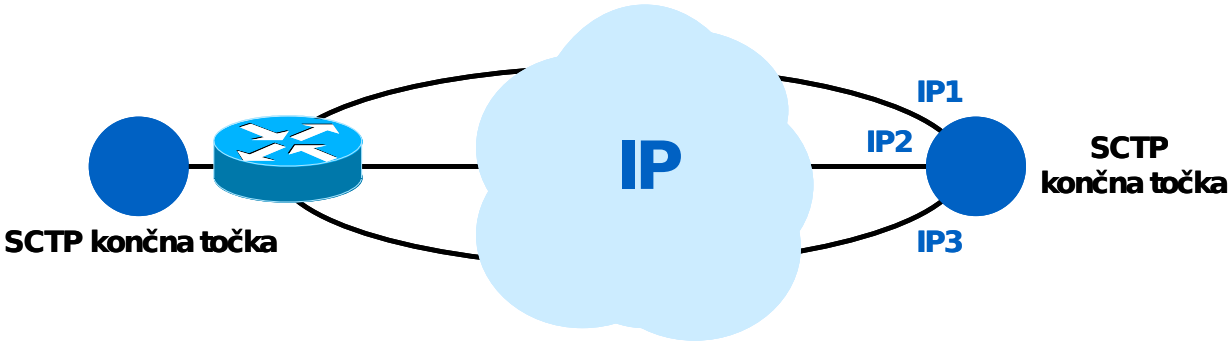
Slika 17: Dostavni postopki SCTP protokola

SCTP je bil načrtovan tako, da se glede krmiljenja pretoka in izogibanja zamašitvam obnaša podobno kot TCP. Pri morebitnem sobivanju noben od protokolov ne sme biti bolj agresiven, saj bi v primeru zamašitev izrinil manj agresivnega ter prevzel večino razpoložljive kapacitete povezave. S tem je poenostavljeno uvajanje SCTP storitev v že obstoječa IP omrežja.

3.4.2.3.Večdomnost

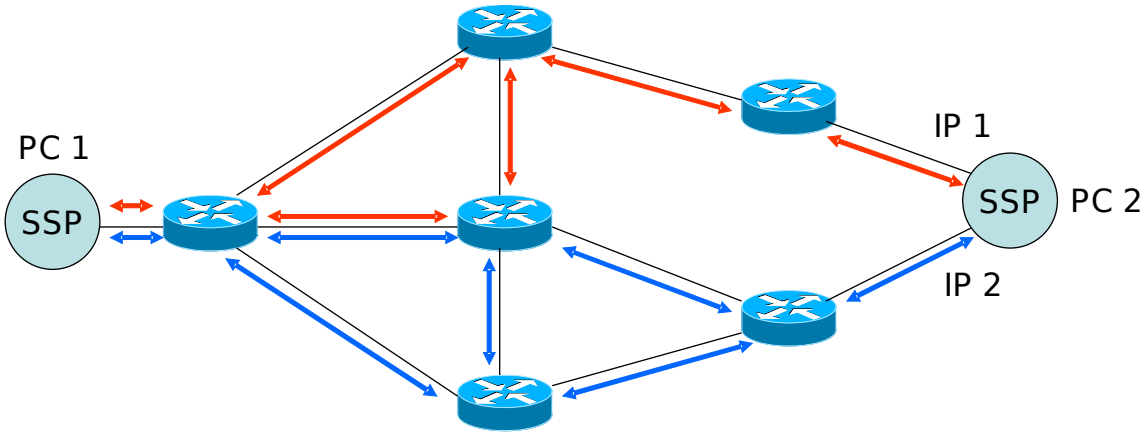
Prednost SCTP pred TCP je podpora tako imenovanih večdomnih gostiteljev. Večdomni gostitelji so vozlišča, oziroma SCTP končne točke, ki so dosegljive na več naslovih IP. Pri protokolu TCP zvezo določa par transportnih naslovov (naslov IP in številka vrat). Pri SCTP vsaka stran povezave ponudi drugi strani listo več IP naslovov v kombinaciji z eno številko SCTP vrat. Velja, da vsako končno točko SCTP določa kombinacija niza razpoložljivih ponornih in izvornih transportnih naslovov. SCTP povezava se nato razširja med vsemi možnimi izvornimi in ponornimi kombinacijami med dvema končnima točkama. Vsaka

večdomna končna točka je tako dosegljiva prek več različnih poti. Transportni naslovi posameznih končnih točk morajo biti pri tem unikatni.



Slika 18: Večdomnost

Krmilni del protokola SCTP nadzira stanje vsake od teh poti z opazovanjem dosegljivosti, zakasnitve in števila zahtev po ponovnih prenosih sporočil. Če se na poti pojavi preveč zaporednih napak, se SCTP pakete poskuša poslati po drugi aktivni poti. IP datagrami z destinacijskimi IP naslovi iz različnih podomrežij ponavadi potujejo tudi po različnih poteh, kot to prikazuje slika 19. Opazovanje poti, ponavljanje prenosov po alternativnih poteh in izbira poti glede na njihovo trenutno stanje znatno povečajo robustnost protokola SCTP na delne izpade v omrežju v primerjavi s protokolom TCP. Opisane lastnosti obenem povečujejo odpornost protokola na naključne napade (npr. na obstreljevanje s prometom).



Slika 19: Primer večdomnosti

3.5.PLASTI PRILAGODITVE UPORABNIKA

SIGTRAN delovna skupina je razvila za različne namene več prilagodilnih slojev, med katerimi ima vsak svoje slabosti in prednosti. V nadaljevanju bodo opisani posamezni prilagodilni sloji.

3.5.1.M3UA

M3UA je prilagodilni sloj oz. protokol, ki omogoča transport MTP uporabniških sporočil (ISUP, SCCP idr.) prek protokola IP. Priporočeno je, da M3UA uporablja storitve SCTP protokola (Stream Control Transmission Protocol), saj predstavlja zanesljiv nižje ležeči signalni transportni protokol.

Sloj M3UA zagotavlja ekvivalenten nabor primitivov višje ležečim uporabniškim slojem na enak način kot MTP3 sloj svojim lokalnim MTP3-uporabnikom v SS7 signalni končni točki SEP (Signalling End Point).

3.5.1.1.Lastnosti protokola

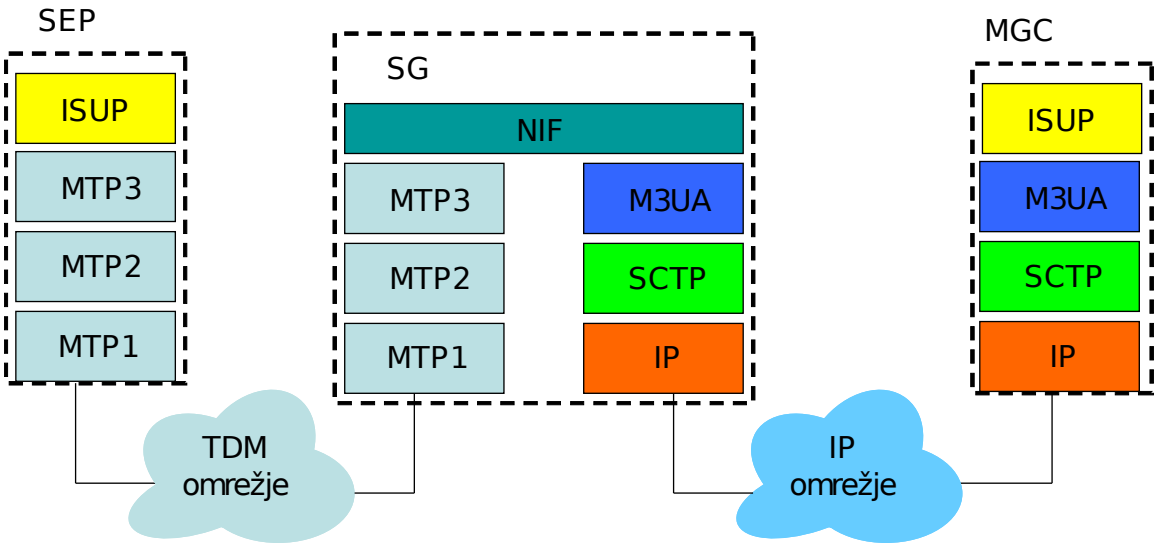
M3UA omogoča naslednje:

- vzpostavljanje in rušenje M3UA povezav,
- prenos MTP uporabniških sporočil (ISUP, SCCP idr.),
- uporabo redundančne arhitekture omrežja,
- nadzor nad statusom vseh M3UA povezav, ki so na voljo,
- opazovanje dosegljivosti signalnih točk preko teh povezav,
- usmerjanje in razdeljevanje prometa,
- preklop ob napakah,
- ukrepanje ob preobremenitvah,
- neposreden nadzor nad slojem SCTP in SCTP povezavami.

3.5.1.2.Uporaba protokola

Protokol M3UA se uporablja predvsem med signalnim prehodom SG in krmilnim protokolom za prehod med mediji (MGC – Media Gateway

Controller) ali za dostop do lokalne IP podatkovne baze. Predpostavlja se, da signalni prehod SG sprejema SS7 signalna sporočila preko standardnega SS7 vmesnika z uporabo MTP.

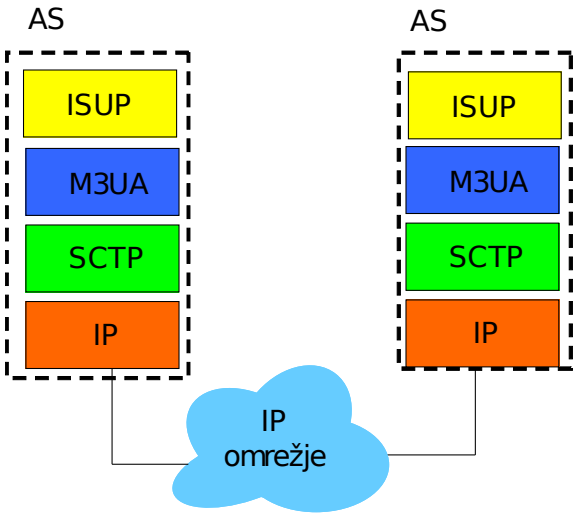


Slika 20: Uporaba M3UA protokola

Protokol M3UA protokolom višjih uporabniških slojev SS7 zagotavlja transparentne storitve omrežnega sloja IP. Sloj M3UA v aplikacijskem storitvenem procesu to zagotavlja s prenosom primitivov na vmesniku med MTP3 in uporabniškim slojem MTP3 (to sta ISUP in/ali SCCP). Ker M3UA nudi enakovreden nabor primitivov, kot jih sicer podpira vmesnik do MTP3, se uporabniški sloj ne zaveda, da se funkcije omrežnih slojev SS7 ne vršijo lokalno, temveč v signalnem prehodu. Po drugi strani se tudi MTP3 sloj v signalnem prehodu ne zaveda, da so navidezno lokalni uporabniki dejansko oddaljeni uporabniki na različnih gostiteljih. M3UA tako razširja storitve MTP3 do oddaljenih uporabnikov v internetnih omrežjih.

M3UA sloj se lahko uporablja tudi v primeru točka-točka (ang. point-to-point) signalne povezave med dvema procesoma IP strežnika IPSP. V tem primeru M3UA zagotavlja enak nabor primitivov in storitev višje ležečim uporabniškim slojem kot MTP3. Storitve pa niso ponujene preko signalnega prehoda SG, saj zaradi poenostavljene povezave točka-točka dveh IPSP te storitve zagotavlja že podnabor MTP3 procedur, ki jih na obeh straneh zagotavlja M3UA.

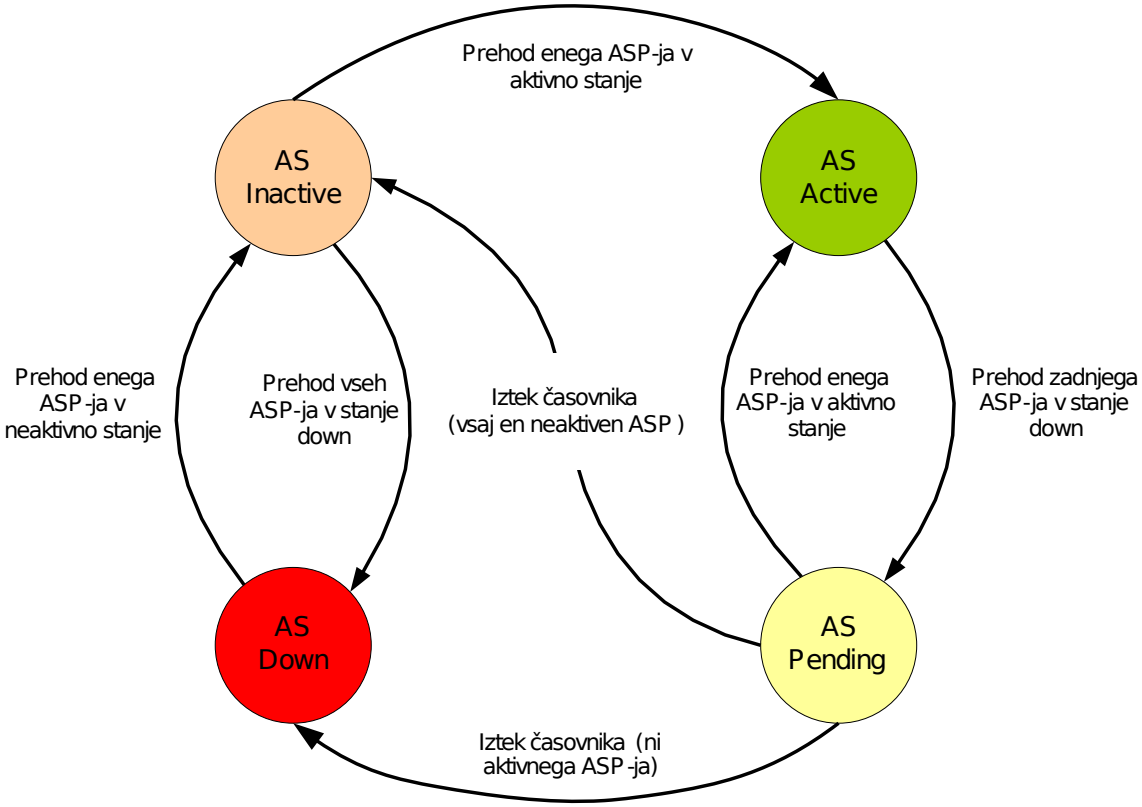
Druga možnost uporabe točka-točka signalne povezave je povezovanje storitvenih krmilnih točk (SCP - Signalling Control Point), to je kontrolnih točk ali specializiranih podatkovnih centrov v inteligentnih omrežjih.



Slika 21: Povezava dveh AS-ov preko M3UA

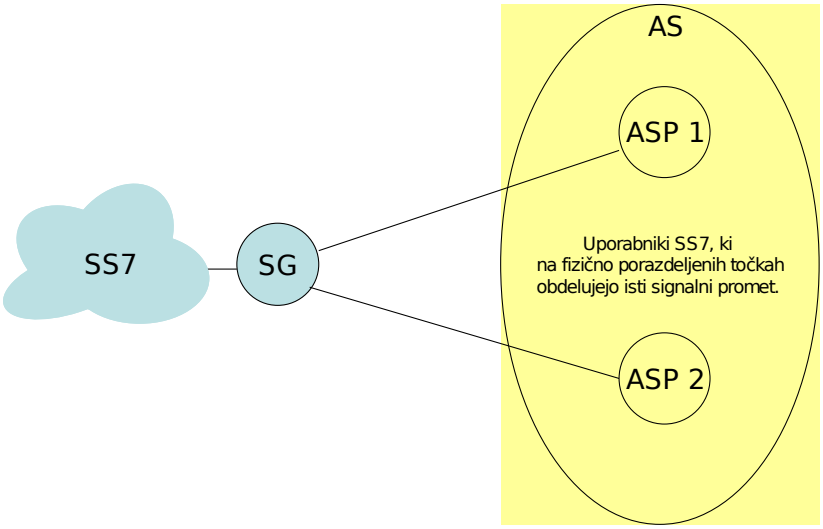
3.5.1.3.Aplikacijski strežnik

Aplikacijski strežnik (AS – Application Server) v omrežju IP predstavlja logično entiteto, ki procesira nabor MTP3 uporabniškega prometa (ISUP, SCCP, TUP, idr.) definiranega z usmerjevalnim ključem. Stanja, v katerih se lahko nahaja aplikacijski strežnik, so prikazana na spodnji sliki (Slika 22).



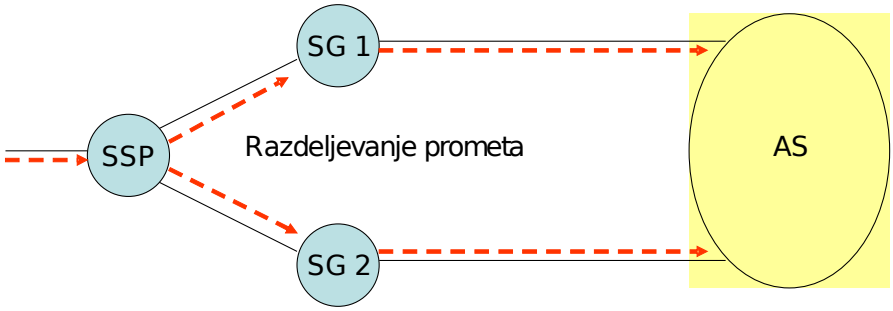
Slika 22: Stanja aplikacijskega strežnika

Sestavlja ga en ali več procesov aplikacijskega strežnika (ASP – Application Server Process). AS je lahko postavljen na enem samem mestu, lahko pa je razporejen po več različnih fizičnih mestih. Porazdeljeni AS prikazuje slika 23.



Slika 23: Porazdeljeni aplikacijski strežnik

AS je določen s signalno točko, zato ga tudi druge signalne točke v SS7 vidijo kot eno samo celoto, čeprav je fizično porazdeljen. Če je AS dosegljiv prek različnih SG-jev oziroma smeri, je omogočena tudi razdelitev prometa, kot prikazuje slika 24.



Slika 24: Razdeljevanje prometa preko redundančnih poti

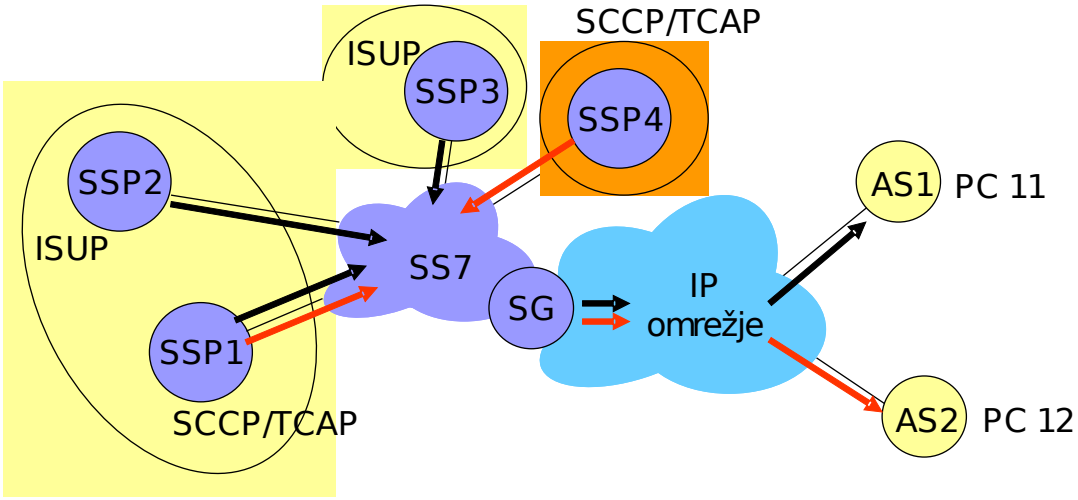
AS servisira oziroma posreduje sporočila SS7 za določen nabor signalnih točk in uporabnikov v omrežju SS7. Ta nabor parametrov kode izvorne točke (OPC - Origination Point Code), kode ponorne točke (DPC – Destination point Code) in indikatorja storitve(SIO - Service Indicator Octet) se imenuje usmerjevalni ključ (RK – Routing Key). Usmerjevalni ključ se lahko med procesi izmenja dinamično v postopku registracije M3UA povezave, lahko pa je že vnaprej določen in ga ni potrebno poslati signalnemu prehodu. Slika 25 prikazuje primer usmerjevalnih ključev.

RK – AS 1

OPC	DPC	SIO
1	11	SI =ISUP
2	11	SI =ISUP
3	11	SI =ISUP

RK – AS 2

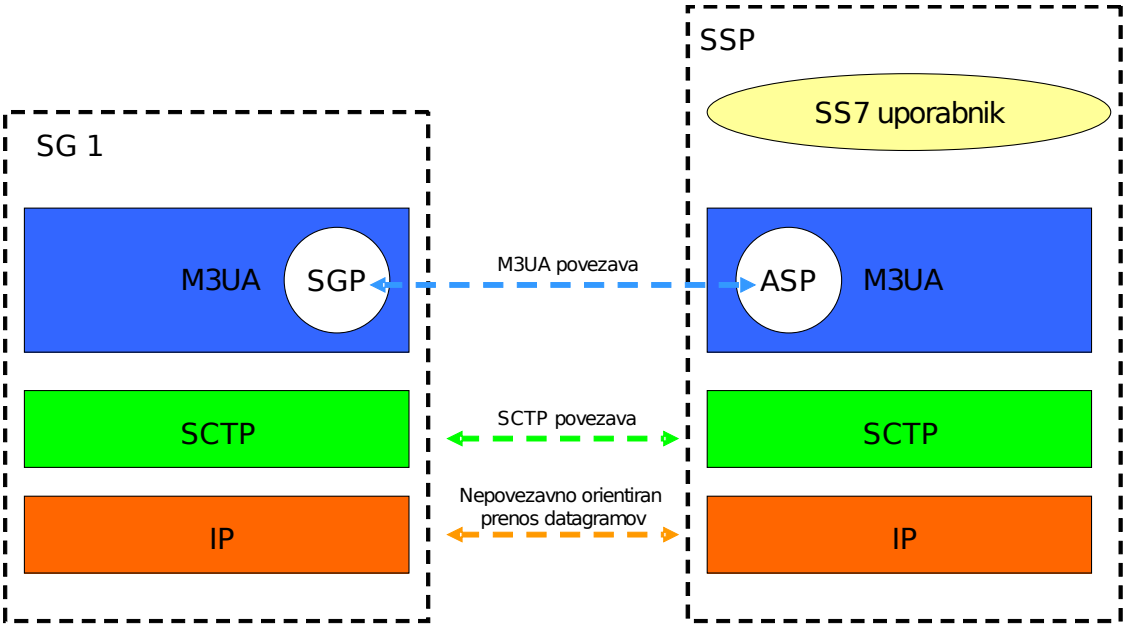
OPC	DPC	SIO
1	12	SI =SCCP
4	12	SI =SCCP



Slika 25: Primer usmerjevalnih ključev

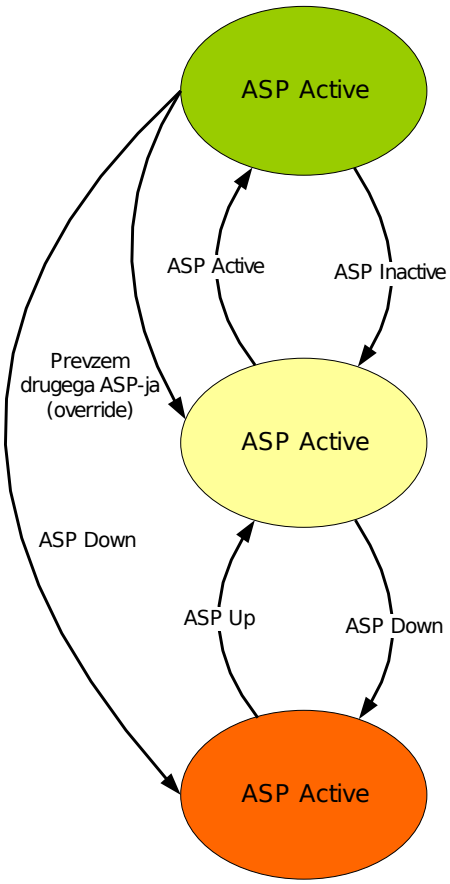
3.5.1.4.Proces aplikacijskega strežnika

AS je logična entiteta, ki servisira specifični RK. Njegov proces je dejanski računalniški proces, ki se izvaja na nekem gostitelju. ASP sprejema vsa sporočila, ki so namenjena njegovemu AS-u, ter jih posreduje ustreznim uporabnikom SS7. Proces signalnega prehoda (SGP – Signalling Gateway Process) je ekvivalenten ASP-ju, le da se nahaja na SG strani.



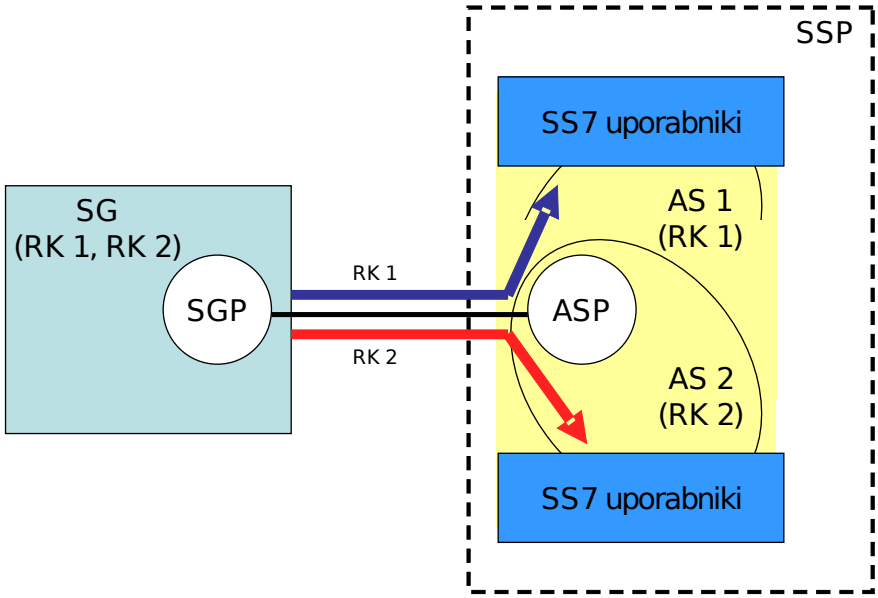
Slika 26: Proces aplikacijskega strežnika

Na spodnji sliki (Slika 27) so prikazan možna stanja v katerih se lahko nahaja proces aplikacijskega strežnika.



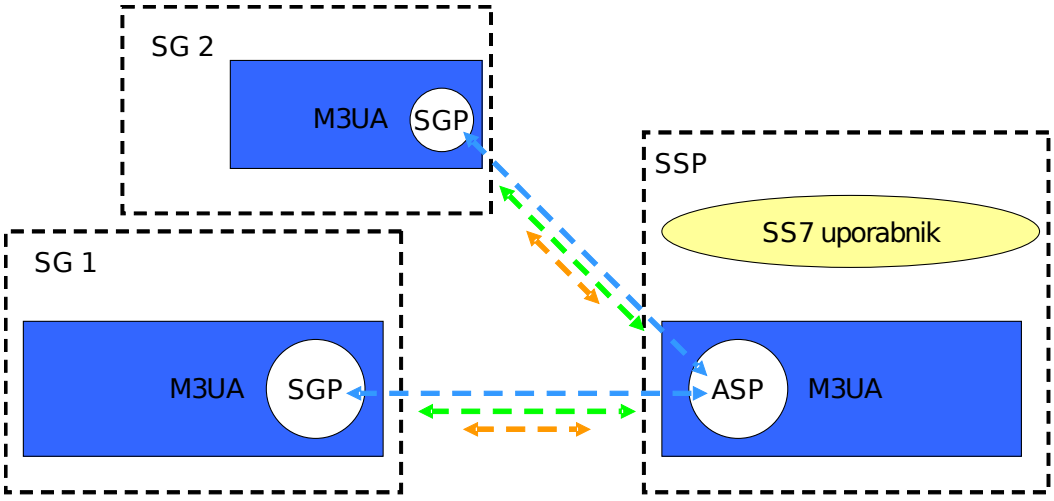
Slika 27: Stanja procesa aplikacijskega strežnika

Proces ASP lahko streže več različnim AS-om, kar pomeni, da se po M3UA povezavi ASP-SGP pošiljajo signalna sporočila, ki ustrezajo več različnim usmerjevalnim ključem. Vsi ti usmerjevalni ključi se morajo uspešno registrirati in aktivirati, od posamezne izvedbe pa je odvisno ali se v tem primeru pošlje več registracijskih in aktivacijskih sporočil ali pa eno samo registracijsko in aktivacijsko sporočilo vsebuje listo vseh usmerjevalnih ključev.



Slika 28: ASP streže dvema AS-oma

ASP je lahko povezan z več različnimi SGP-ji. Tako vzpostavi z vsakim signalnim prehodom svojo M3UA povezavo.



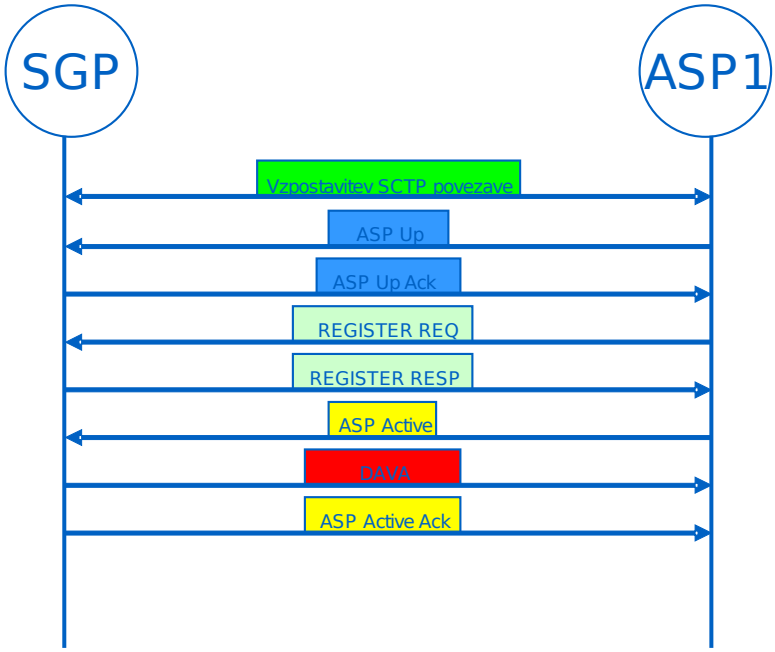
Slika 29: Povezovanje ASP-ja na več SGP-jev

Povezovanje na več SG-jev omogoča redundanco, ki je potrebna za zanesljivo signalizacijo. Nadzor nad stanji vseh parov M3UA povezava-

AS daje AS-u možnost razdeljevanja prometa in preklopa ob morebitnih napakah.

3.5.1.5.Vzpostavljanje M3UA povezave

ASP skupaj s procesom SGP, ki se izvaja na signalnemu prehodu, vzpostavi M3UA povezavo, preko katere si v primeru aktivne povezave izmenjujeta sporočila SS7.



Slika 30: Vzpostavitev M3UA povezave

3.5.1.6.NIF

NIF v okviru SG služi kot vmesnik med MTP3 in M3UA ter nima nasprotno ležečega sloja na SS7 SEP ali MGC strani. Poleg posredovanja uporabniških sporočil med obema protokoloma NIF zagotavlja tudi prenos informacij o dosegljivosti signalnih točk.

M3UA sloj se v signalnem prehodu preko NIF navezuje na MTP3 v omrežju SS7. Na strani aplikacijskega strežnika se M3UA povezuje direktno na ISUP (oziroma SCCP) in nudi enake storitve kot MTP3. SS7 sporočila, ki so namenjena ponornemu MGC-ju, se usmerjajo na končni naslov IP. Sporočila, ki jih sprejme sloj M3UA, so poslana na sloj MTP3 in se usmerijo v SS7 signalno končno točko SEP. Za zagotavljanje indikacije statusa omrežja SS7 NIF iz vmesnika MTP3 sprejema signale

o dostopnosti SS7 destinacij (pause, resume, status) ter jih pošilja lokalni M3UA upravljavski funkciji.

SG		M3UA sporočilo	AS
Stanje v MTPL3	MTPL3->M3UA		M3UA->ISUP
Dest. nedostopna	PauseInd(DestNo)	DUNA ->	PauseInd(DestNo)
Destinacija dostopna	ResumeInd(DestNo)	DAVA ->	ResumeInd(DestNo)
Dest.preobremenjena	StatusInd(DestNo, congested)	SCON ->	StatusInd(DestNo, congested)
Uporabnik nepoznan (neimplementiran)	StatusInd(DestNo, unknown)	DUPU ->	StatusInd(DestNo, unknown)
Uporabnik nedostopen	StatusInd(DestNo, inaccessible)	DUPU ->	StatusInd(DestNo, inaccessible)
Uporabnik neopremljen	StatusInd(DestNo, unequipped)	DUPU ->	StatusInd(DestNo, unequipped)
Destinacija dostopna	<- ResumeInd(DestNo)	ASP active	
Dest. nedostopna	<- PauseInd(DestNo)	ASP inactive, padec SCTP povezave	
		<- DAUD	(nedostopna dest., tm_paud)
Dest.preobremenjena	<- StatusInd(DestNo, congested)	<- SCON	(preobemenitev proti AS)

Tabela 2: Primerjava obveščanja o stanju signalnih točk v MTP3 in M3UA

3.5.1.7.Zanesljivost

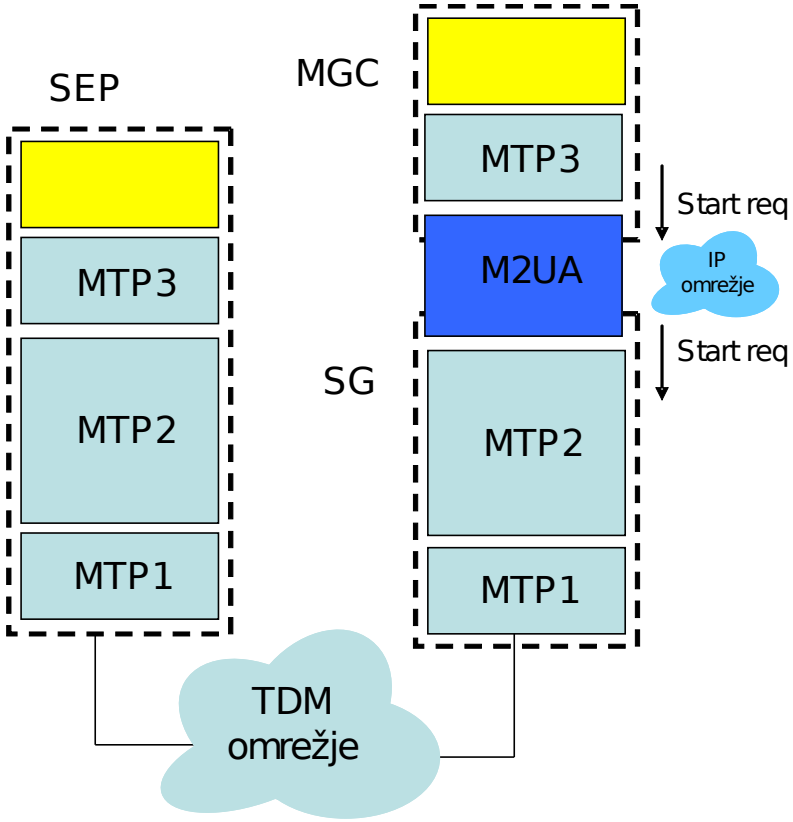
Protokol M3UA sam po sebi ne zadovoljuje zahtev glede zmogljivosti in zanesljivosti prenosa signalizacije. Potrebna je tudi distribuirana arhitektura in redundančno omrežje. M3UA je fleksibilen in omogoča učinkovito delovanje ter nadzor v različnih fizičnih konfiguracijah, kar omogoča operaterjem zadovoljevanje zahtevanih kriterijev glede zanesljivosti, ki so primerljive z lastnostmi omrežja SS7.

3.5.2.M2UA

Protokol M2UA je prilagodilni sloj med SCTP in MTP3 slojema na strani aplikacijskega strežnika. V signalnem prehodu MTP3 sloj ni potreben,

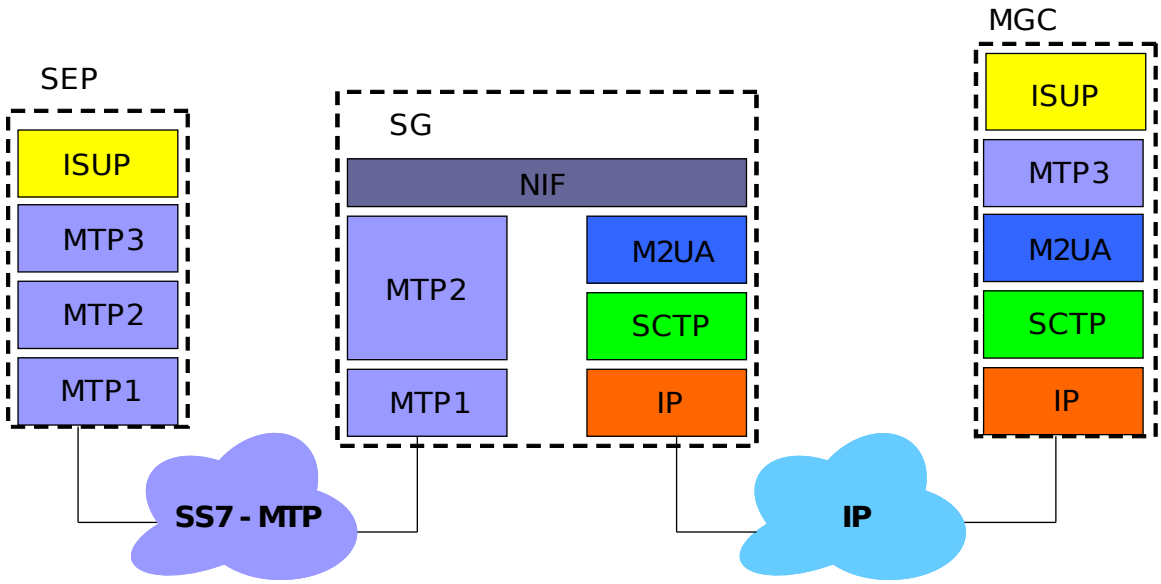
povezavo med istoležnima slojema MTP2 in M2UA pa omogoča povezovalni sloj NIF.

MTP2 se povezuje na oddaljeni MTP3 sloj preko M2UA povezave, ki za zanesljiv prenos uporablja storitve SCTP protokola. Signalni prehod zaključi SS7 povezavo na sloju MTP2 in prenese sloj MTP3 na krmilnik medijskega prehoda (MGC) oziroma drugo IP signalno končno točko z uporabo SCTP/IP protokolov. Signalni prehod, ki vsebuje prehod na M2UA nivoju, nima signalne točke.



Slika 31: M2UA – transparentnost

Uporabnik MTP2 sloja je vedno MTP3 sloj, torej se preko M2UA prenašajo vsa sporočila, ki bi se sicer neposredno posredovala med slojema MTP2 in MTP3.



Slika 32: Uporaba M2UA protokola

3.5.2.1.Procesi M2UA

M2UA nadzira stanja AS-ov in ASP-jev na podoben način kot M3UA (poglavja 3.5.1.3 in 3.5.1.4). Med vzpostavitvijo M2UA povezave je podobno kot pri M3UA povezavi možna registracija ASP-ja s tako imenovanim povezavnim ključem (LK – Link key), ki vsebuje dva parametra:

- SDTI (Signalling Data Terminal Identifier) in
- SDLI (Signalling Data Link Identifier).

Omenjena parametra natančno definirata signalno povezavo med SS7 vmesnikom in SCTP sporočilnim tokom v M2UA povezavi. Povezavni ključ se izmenja le ob registraciji, nato pa ga enoumno definira parameter Interface identifier, ki je prisoten v vsakem sporočilu. Ta relacija je lahko določena tudi statično. V tem primeru registracija ni več potrebna.

Aktiviranje, deaktiviranje ASP-ja ter vse ostale procedure (registracija, failover, pending) potekajo enako kot pri M3UA.

Šele ko je M2UA povezava aktivna, je pripravljena za prenos MTP2 in MTP3 sporočil. Prenos sporočil je za oba sloja transparenten. Tako se

ne zavedata, da sta locirana na fizično različnih mestih, ter povezana z M2UA povezavo.

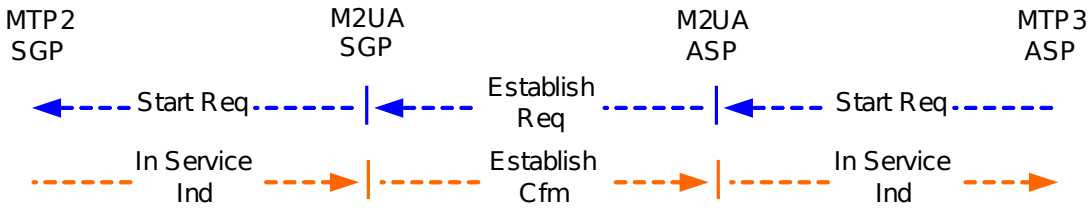
3.5.2.2.M2UA sporočila in primeri izmenjave

M2UA kot uporabniška sporočila prenaša sporočila MAUP (MTP2 User Adaptation):
Skupine MAUP sporočil:

- Data Acknowledge – Sporočila potrjujejo sprejem podatkovnih sporočil, ki jih določa korelacijski identifikator.
- Establish Request and Confirm – ASP pošlje sporočilo Establish Request, ko zahteva vzpostavitev signalne povezave. Po končani proceduri vzpostavitvenega uvrščanja SGP potrdi z Establish Confirm sporočilom.
- Release Request, Indication, and Confirm – ASP pošlje sporočilo Release Request, ko zahteva zaustavitev povezave. Ko signalna povezava preide v stanje Out of service, SGP pošlje potrditveno sporočilo Release Confirm. Če je do prekinitve povezave prišlo iz drugih razlogov, SGP obvesti ASP s sporočilom Release Indication.
- State Request, Indication, and Confirm – ASP pošlje sporočilo State Request v primeru, ko zahteva spremembo načina vzpostavitvenega uvrščanja, obveščanje o zgostitvah ali izpraznitev pomnilnika za določeno signalno povezavo. SGP potrdi sprejem State Request sporočila s sporočilom State Confirm, s sporočilom State Indication pa obvesti ASP o spremembah stanja lokalnih in oddaljenih procesov.
- Congestion Indication – SGP pošlje ASP-ju sporočilo Congestion Indication, ko pride do spremembe statusa zgostitve signalne povezave. Sporočilo omogoča uporabo vseh nivojev zgostitev, ki so definirani v MTP standardu.
- Retrieval Request, Indication, Complete Indication, Confirm – Navedena sporočila se uporabijo pri changeover proceduri. ASP začne postopek s sporočilom Retrieval Request, s katerim zahteva BSN porušene signalne povezave. SGP odgovori s sporočilom Retrieval Confirm. Če na MTP2 sloju na SGP-ju obstajajo kakšna uporabniška sporočila, ki še niso bila dostavljena, lahko MTP3 sloj na ASP-ju zahteva vračilo le teh s

ponovnim sporočilom Retrieval Request. SGP nato ASP-ju pošlje uporabniška sporočila v sporočilih Retrieval Indication in Retrieval Complete Indication.

V spodnjem primeru (Slika 33) vidimo proceduro izmenjave sporočil pri vzpostavljanju signalne povezave (vzpostavitveno uvrščanje). Prikazan je tudi primer (Slika 34), ko povezavo odvzamemo (zahtevamo zaustavitev) iz delovanja.

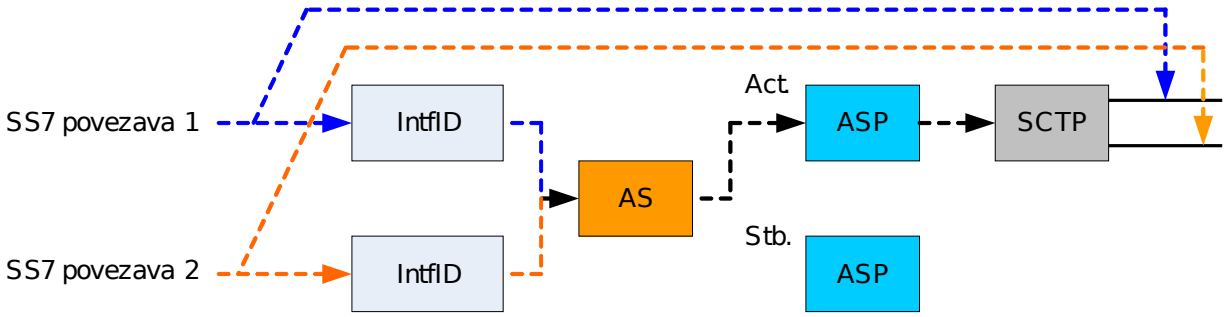


Slika 33: Primer vzpostavitve signalne povezave

Slika 34: Primer zaustavitve signalne povezave

3.5.2.3.Relacija med fizičnim in navideznim vmesnikom

M2UA ohranja informacijo o povezavi med fizičnim vmesnikom (MTP2 povezava) in navideznim vmesnikom (Interface ID). Hkrati se posameznemu navideznemu vmesniku dinamično dodeli en sporočilni tok v SCTP povezavi. Realacija (mapiranje) med fizičnim vmesnikom in sporočilnim tokom je vedno 1:1, saj SG zaključi SS7 povezavo in jo preslika na en sam AS. Tako je lahko v okviru SG aktiven le en sam SGP za določen AS. SGP lahko streže prometu večih AS-ov, AS pa je lahko namenjen več navideznim vmesnikom.



Slika 35: Primer logične povezave med navideznim vmesnikom in sporočilnim tokom v SCTP povezavi

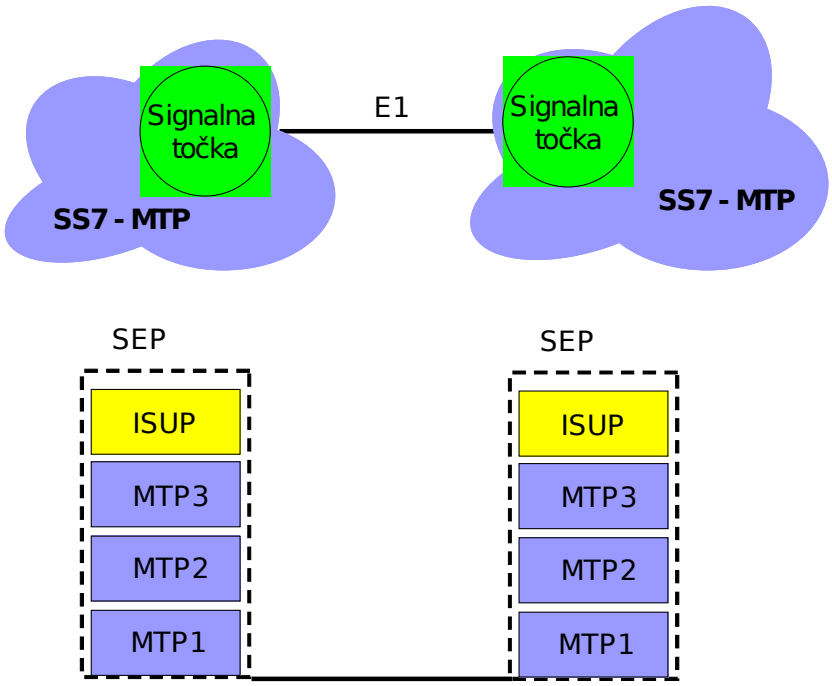
3.5.3.M2PA

M2PA je prilagodilni sloj oziroma protokol, ki omogoča transport SS7 MTP3-uporabniških sporočil (ISUP in SCCP) preko protokola IP. Priporočeno je, da M2PA uporablja storitve SCTP protokola, ki predstavlja zanesljiv nižje ležeči signalni transportni protokol. M2PA sloj zagotavlja višje ležečemu sloju MTP3 ekvivalenten nabor primitivov kot sloj MTP2, ki je definiran v ITU-T priporočilu Q.703 [19]. Skratka, protokolni sklad M2PA/SCTP/IP se uporablja namesto sklada MTP2/MTP1.

V SS7 omrežju je vsaka točka, ki ima MTP3 sloj, predstavljena s kodo (PC – Point Code). Zato mora imeti kodo (PC) tudi vsaka končna točka povezave z uporabo M2PA.

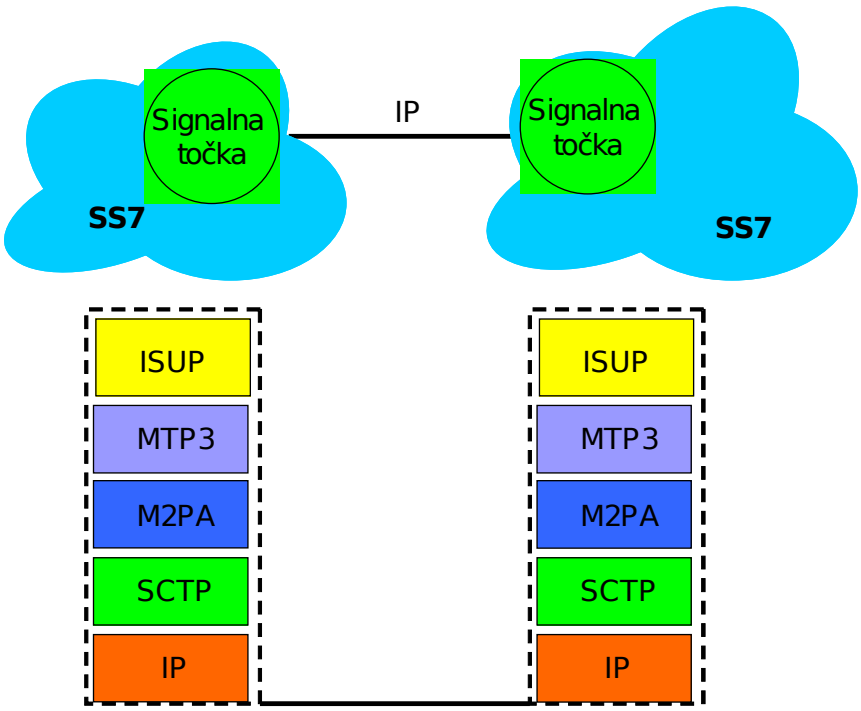
3.5.3.1.Arhitektura M2PA

Na spodnji sliki (Slika 36) je prikazana klasična signalna povezava SS7 preko povezave TDM (signalna povezava E1).



Slika 36: Protokolni sklad klasične SS7 povezave

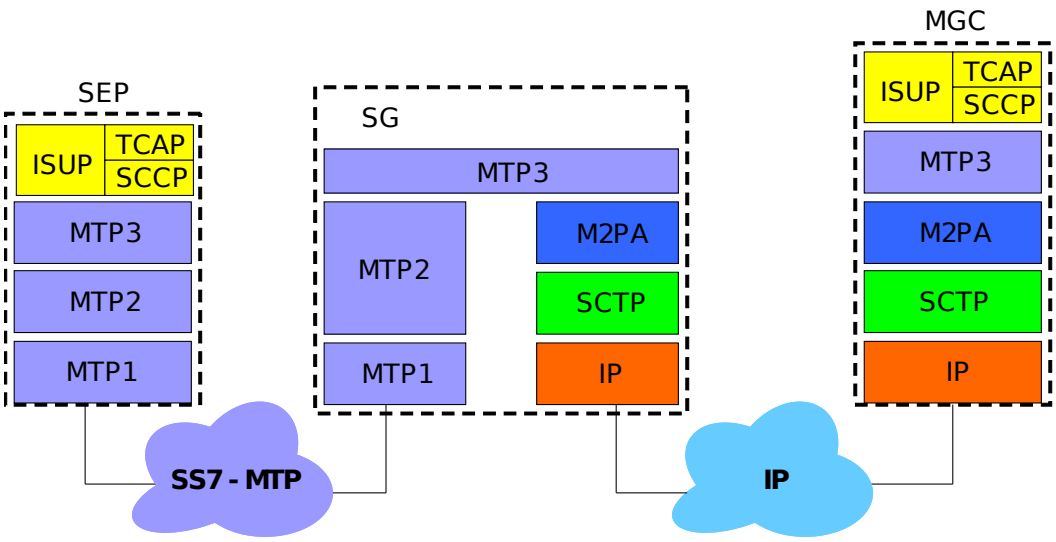
Na naslednji sliki (Slika 37) pa je prikazan signalna povezava SS7 preko omrežja IP z uporabo prilagodilnega sloja M2PA in transportnega sloja SCTP. Povezava je funkcionalno enaka klasični signalni povezavi SS7.



Slika 37: Protokolni sklad SS7 povezave preko povezave IP s prilagodilnim slojem M2PA

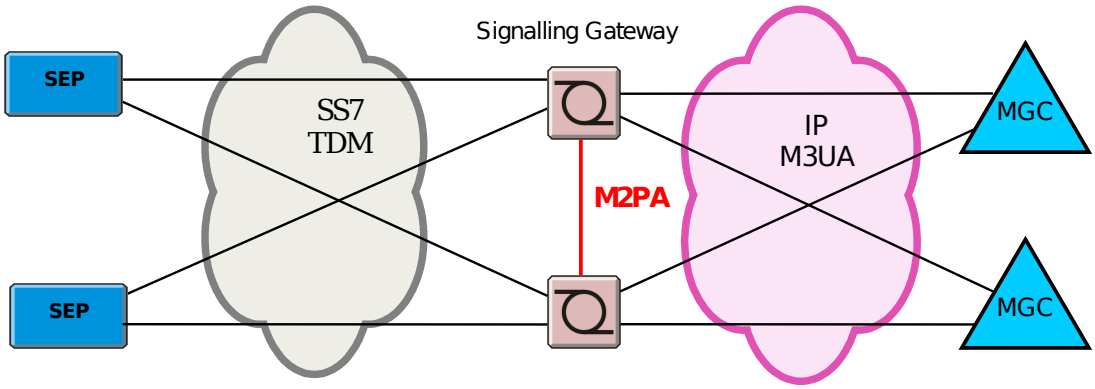
Prikazana povezava se uporablja za nadomeščanje posameznih klasičnih SS7 signalnih povezav ali za povezovanje dveh ločenih SS7 omrežij preko omrežja IP. Na ta način lahko omrežje SS7 postopno prehaja v domeno IP, pri čemer topologija ostaja nespremenjena in se prehoda ostali elementi v omrežju SS7 ne zavedajo.

M2PA se veliko uporablja tudi za povezavo do kontrolnih točk SCP (Servis Control Point), oziroma podatkovnih baz v specializiranih centrih za dodatne in inteligentne storitve, kjer se prenaša samo signalizacija brez govornih kanalov in je povezovanje z E1 signalnimi povezavami drago. Poleg tega proizvajalci SCP želijo imeti samo IP povezave.



Slika 38: Uporaba M2PA v signalnem prehodu

Naslednja možnost uporabe M2PA je za povezovanje med posameznimi signalnimi prehodi SG z npr. M3UA zaradi povečanja zanesljivosti.



Slika 39: Povezovanje signalnih prehodov s M2PA

3.5.3.2.Lastnosti M2PA

Prilagodilni sloj M2PA se uporablja za nadomeščanje običajnih signalnih povezav, torej za povezovanje SS7 signalnih točk. V arhitekturi SS7 povezava preko M2PA predstavlja signalno povezavo. Zato na obeh koncih potrebuje mrežni sloj MTP3 in kodo signalne točke PC (Point Code).

Prednosti M2PA :

- nadomešča fizično SS7 signalno povezavo preko TDM z virtualno IP transportno povezavo,
- ima podobne lastnosti v realnem času, kot jih zahteva signalizacija SS7,
- ni več omejitve pretoka na 64 kbit/s,
- hitro dodajanje signalnih povezav glede na zahteve,
- cenejše,
- manjše geografske omejitve.

Slabosti M2PA :

- signalni prehodi (SG) morajo imeti kodo signalne točke (Point Code),
- zanesljivost signalne povezave preko M2PA je v realnih IP omrežjih običajno nižja kot pri SS7 signalni povezavi,
- problemi z velikostjo FSN, BSN števnikov.

M2PA zagotavlja upravljanje nižje ležečega SCTP transportnega protokola in indikacijo napak M2PA sprejetih sporoči, ki jih sporoči na lokalno upravljanje in/ali soležnemu M2PA sloju.

3.5.3.3.Funkcije M2PA

M2PA skupaj z SCTP izvaja funkcije enako kot MTP2. SCTP zagotavlja zanesljiv prenos sporočil v pravem vrstnem redu.
M2PA funkcije :

- prenos signalnih sporočil med MTP3 sloji,
- postopki vzpostavljanja signalne povezave,
- vzdrževanje SCTP povezave,
- obveščanje MTP3 o stanju signalne povezave,
- postopki vračanja sporočil ob zamenjavi signalne povezave (changeover),
- postopki za »Processor outage« (če MTP2 nima povezave z MTP3).

3.5.3.4.SCTP povezave in MTP signalne povezave

Vsaki MTP signalni povezavi pripada svoja SCTP povezava (asociacija). V primeru, da želimo med dvema IPSP imeti več signalnih povezav z uporabo M2PA, nastopi problem dodeljevanja IP naslovov in portov. SCTP asociacija je namreč določena z IP naslovom in vrati na obeh straneh. IP naslovov je v primeru večdomnosti lahko tudi več.

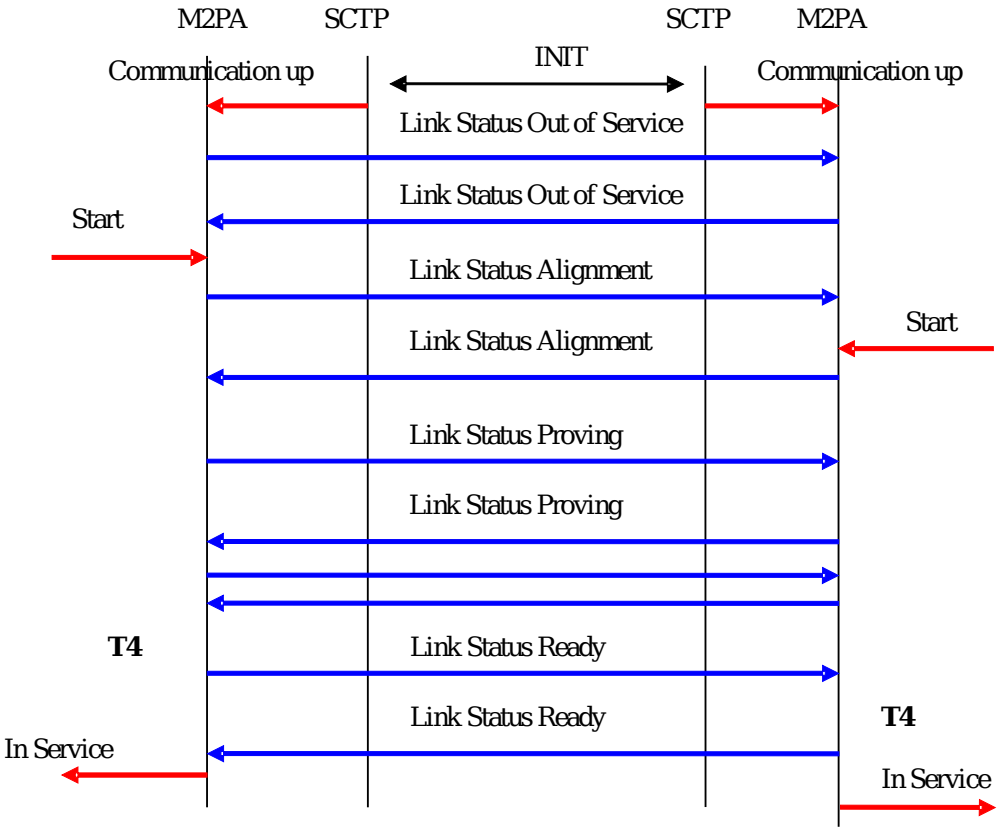
M2PA uporablja 2 tokova (stream) v vsako smer:

- tok 0 za prenos stanja signalne povezave (Link Status),
- tok 1 za uporabniška sporočila (User Data).

Nekaj statusnih sporočil (Processor Outage, Procesor recovered, Ready) se neglede na zgornje pravilo prenaša po toku 1 zaradi sinhronizacije s podatkovnimi sporočili.

3.5.3.5.Vzpostavljanje M2PA povezave

Po vzpostavitvi SCTP povezave poteka vzpostavljanje M2PA povezave ekvivalentno kot pri MTP2 (Q.703), s tem da se statusna sporočila pošiljajo samo enkrat, razen nekaj izjem. Diagram poteka tipične vzpostavitve M2PA povezave je prikazan na spodnji sliki (Slika 40).

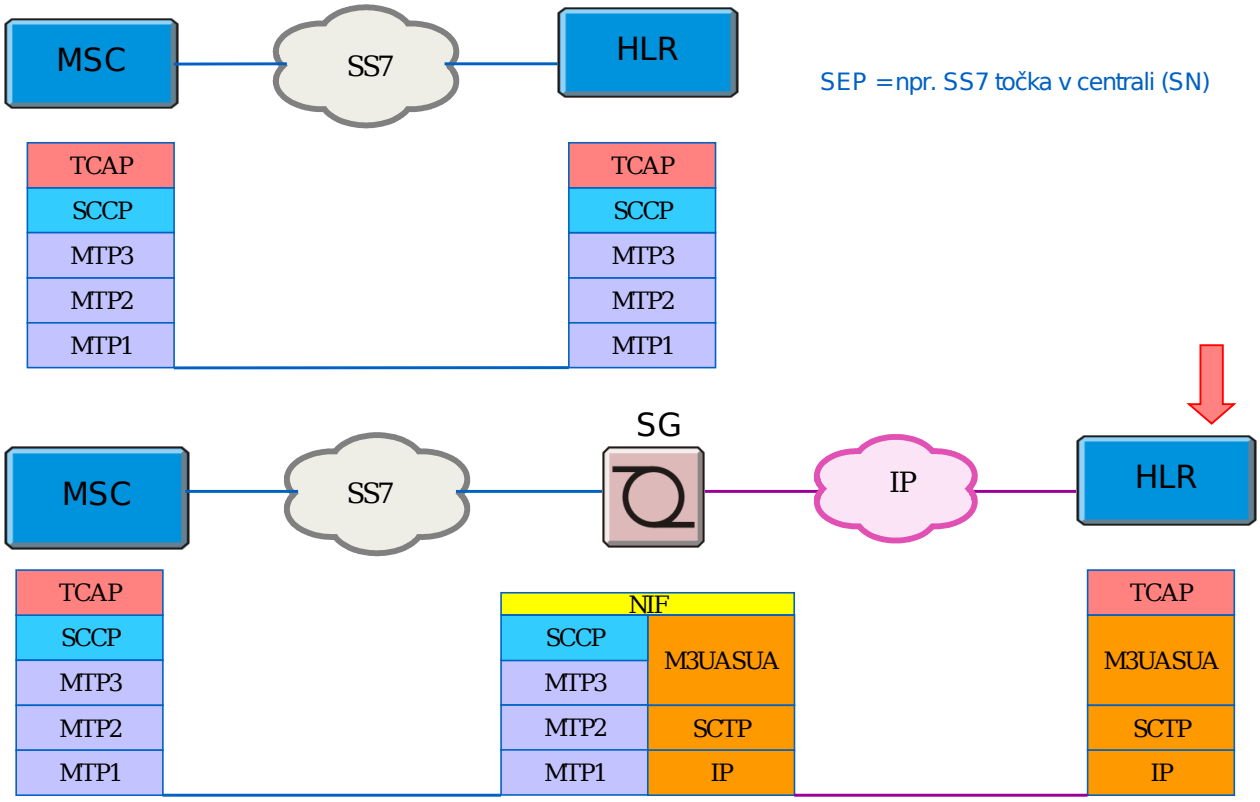


Slika 40: Potek vzpostavljanja M2PA povezave

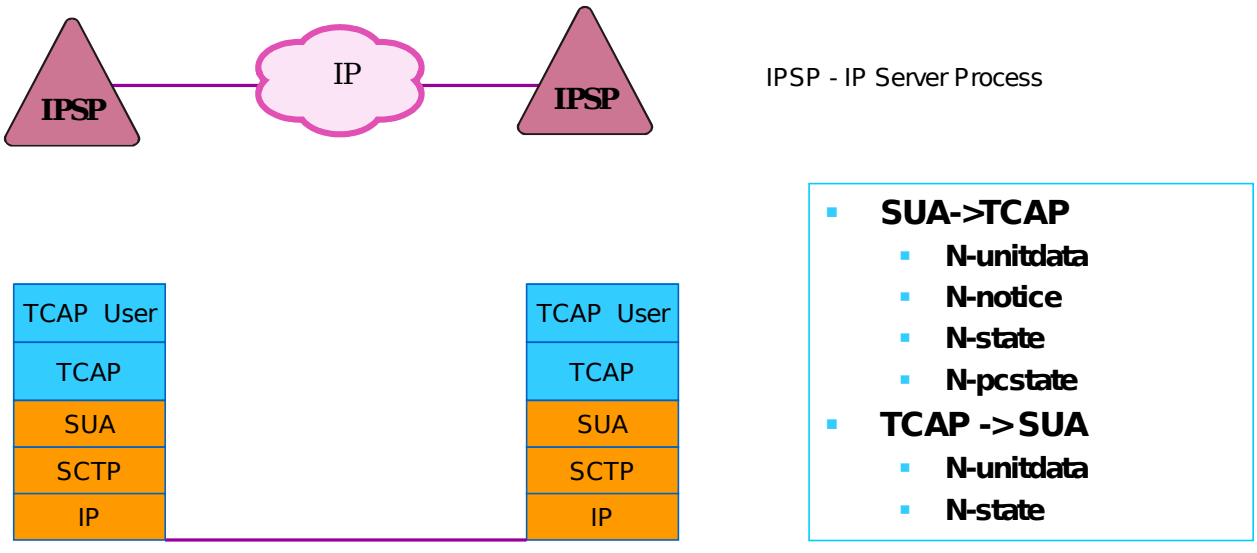
3.5.4.SUA

SUA je prilagodilni sloj oziroma protokol, ki omogoča transport SCCP in TCAP podatkovnih sporočil preko omrežja IP, hkrati pa skrbi za zanesljivost in robustnost omrežja, ki naj bi bila na enakem nivoju kot pri signalizaciji SS7. Čeprav tudi M3UA omogoča prenašanje SCCP sporočil, SUA izloči dodaten del SS7 protokolnega sklada, hkrati pa bolje izkoristi usmerjanje IP.Signalni prehod s SUA ne potrebuje lastne kode. SUA nudi nepovezavno in povezavno orientirane storitve.

Na spodnjih dveh slikah je prikazana uporaba protokola SUA v prehodu iz omrežja SS7 v omrežje IP, ter samo v omrežju IP.



Slika 41: Uporaba SUA v signalnem prehodu



Slika 42: Uporaba SUA v omrežju IP za povezavo dveh IPSP-jev

Prednost protokola SUA je v tem, da lahko prenaša daljša uporabniška sporočila, če je uporabljeno samo omrežje IP (slika 42). Segmentacijo in sestavljanje lahko izvaja SCTP, tako da je omogočeno prenašanje daljših sporočil (SMS sporočila > 160). Poleg tega je SUA je

enostavnejši kot M3UA+SCCP, vendar ima dodatne možnosti prilagojene SCCP aplikacijam. V osnovi podpira osnovno IP naslavljanje in DNS imena.

	M3UA	SUA
Višji sloj	ISUP, SCCP	TCAP
Uporaba	Povezava do MGC	IP podatkovni centri
Potrebuje PC	Da	Ne
Usmerjanje na osnovi	DPC, Usmerjevalni ključ	Global Title (tel. številka)
Povezava je	Vmesnik MTPL3 – ISUP (SCCP) preko IP	vmesnik SCCP – TCAP preko IP

Tabela 3: Primerjava protokola M3UA in SUA

3.5.5.IUA

V vodovno komutiranih omrežjih je ISDN terminalska oprema povezana s komutacijskim vozliščem oz. krajevno centralo preko ISDN vmesnika (Slika 43). V primeru, ko ISDN klice krmili klicni strežnik v omrežju IP, je potrebno signalizacijo DSS1 prenesti preko paketnega podatkovnega omrežja. Signalni prehod na meji med vodovnim dostopovnim omrežjem s časovnim multipleksiranjem kanalov in paketnim podatkovnim omrežjem zagotavlja povezljivost ISDN terminalske opreme s krmilnikom medijskega prehoda, ki izvaja funkcije klicnega strežnika (Slika 44).

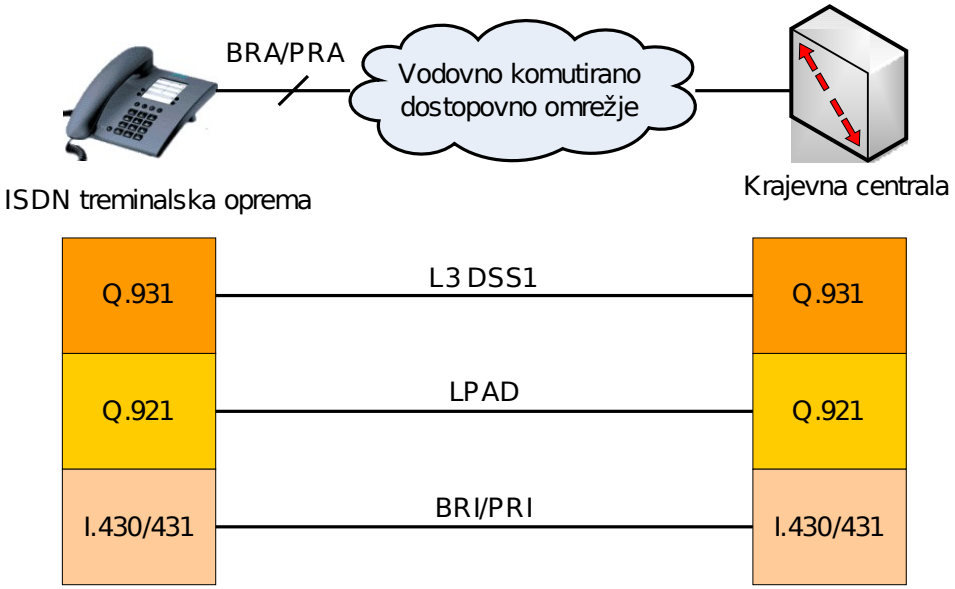
V signalnem prehodu se na uporabniškem dostopu zaključita protokola fizične (I.430 in/ali I.431) in podatkovne povezovalne plasti (Q.921), medtem ko se protokol omrežne plasti (Q.931) zaključi v krmilniku medijskega prehoda. IUA tako podpira uporabniške vmesnike z osnovnim (BRA – Basic Rate Access) in primarnim (PRA – Primary Rate Access) dostopom ter komunikacijske povezave točka-točka ali točka-več točk.

SG vsebuje vozliščno funkcijo medsebojnega delovanja (NIF), ki zagotavlja vzajemno delovanje protokolov uporabniškega dostopa s transportnimi funkcijami omrežja IP. Protokol IUA ima funkcionalnost vmesnika med 2. in 3. plastjo signalizacije DSS1 ter prilagaja informacijski pretok v tem vmesniku za prenos preko omrežja IP med SG in MGC. Informacijski pretok vključuje:

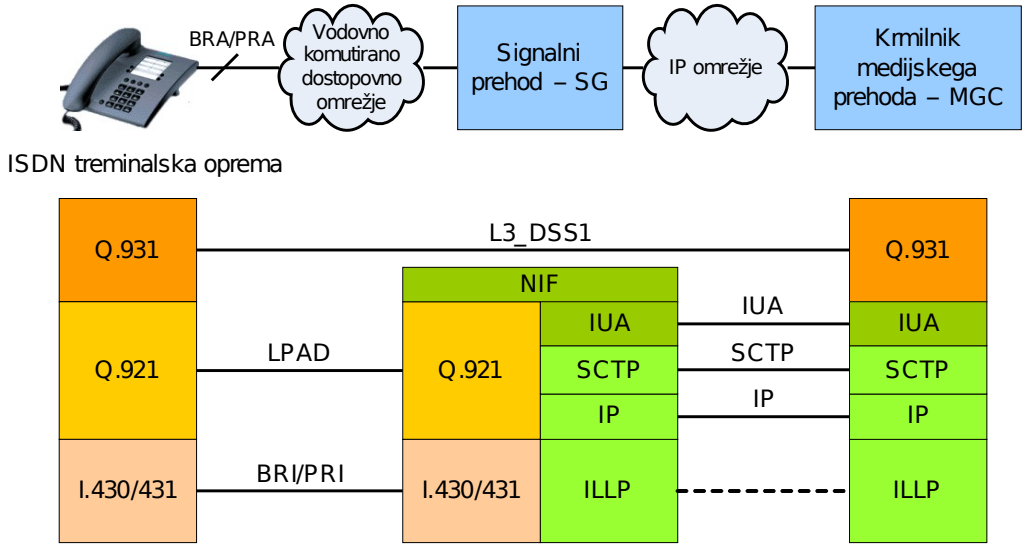
- signalizacijsko informacijo za krmiljenje ISDN osnovnega klica,
- signalizacijsko informacijo za krmiljenje dopolnilnih storitev (lahko pa je tudi brez njih),
- informacijo za nadzor delovanja podatkovne povezave do uporabniške opreme.

Vmesnik uporabnik-omrežje (UNI) na vodu med ISDN uporabniško opremo in signalnim prehodom omogoča priključitev končne terminalske opreme (TE1) in ISDN naročniških central (PINX). IUA zato podpira prenos signalne informacije protokola DSS1 in protokola QSIG.

Medtem ko funkcije plasti IUA prilagajajo DSS1 signalno informacijo paketnemu prenosu, protokol SCTP zagotovi zanesljiv, hiter in varen prenos med končnima točkama omrežja IP. ki prenaša med signalnim prehodom in krmilnikom medijskega prehoda preko omrežja IP.



Slika 43: Arhitektura protokola DSS1 za krmiljenja ISDN klica v lokalni zanki



Slika 44: Uporaba IUA protokola

4. PRIMERJAVA REDUNDANCE IN ZANESLJIVOSTI MED SS7 IN SIGTRAN

V naslednjih podpoglavjih so podrobno predstavljeni posamezni sloji obeh protokolnih skladov SS7 in SIGTRAN. Primerjave in opisi posameznih slojev so logično povezani po posameznih nivojih, ki pa niso istoležni v referenčnem modelu OSI. Tako dobimo boljšo predstavo s čim se posamezni sloj ukvarja in kakšne so njegove naloge.

4.1. PRIMERJAVA NA PRVEM SLOJU

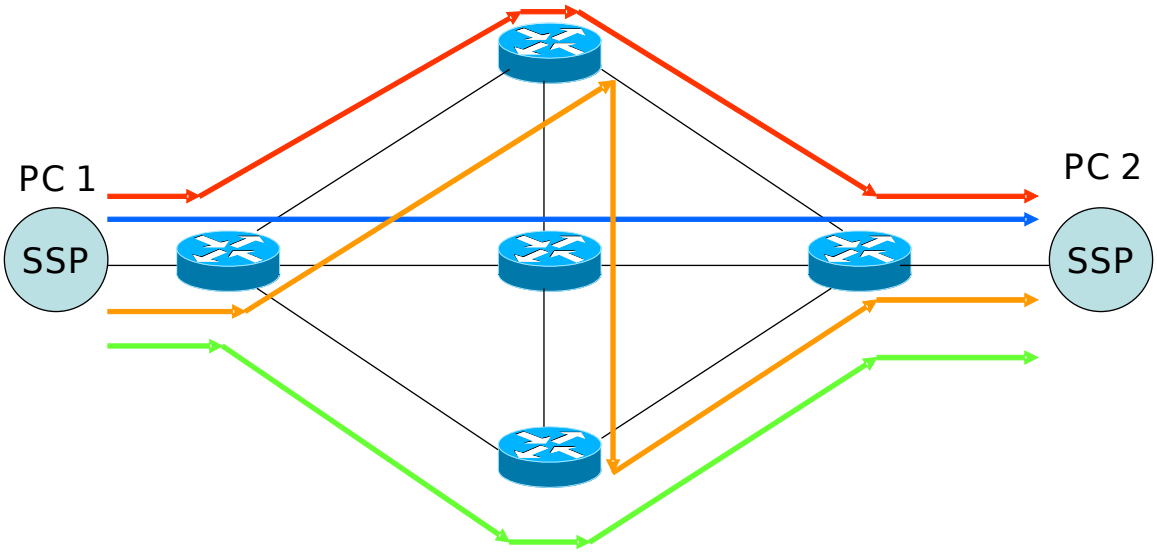
V protokolnem skladu SS7 imamo na najnižjem sloju signalno podatkovno povezavo, ki je v bistvu fizična povezava med dvema končnima točkama. Na prvem sloju v SIGTRAN protokolnem skladu govorimo o povezavi IP, ki ni samo ena fizična povezava, ampak logična povezava med dvema IP naslovoma.

4.1.1. MTP1

MTP1 dejansko ustreza prvemu sloju v modelu OSI. MTP1 določa fizične, električne in funkcijske značilnosti signalne podatkovne povezave in dostopovne enote. Sloj ena predstavlja nosilec, namenjen za signalno povezavo. V digitalnem omrežju se za signalne podatkovne povezave navadno uporabljajo 64 kbit/s kanali. Naloga MTP1 je, da fizično prenese podatkovne enote med dvema točkama. Ne ukvarja se s izgubljenimi, podvojenimi ali celo okvarjenimi podatki. Za vse to je poskrbljeno na višjih nivojih. Navadno je obremenjenost signalnih povezav 0,2 Erlang-a, kar pomeni, da so povezave slabo izkoriščene. Prednost je v tem, da v primeru izpada katere od povezav, lahko alternativna povezava prevzame ves signalni promet.

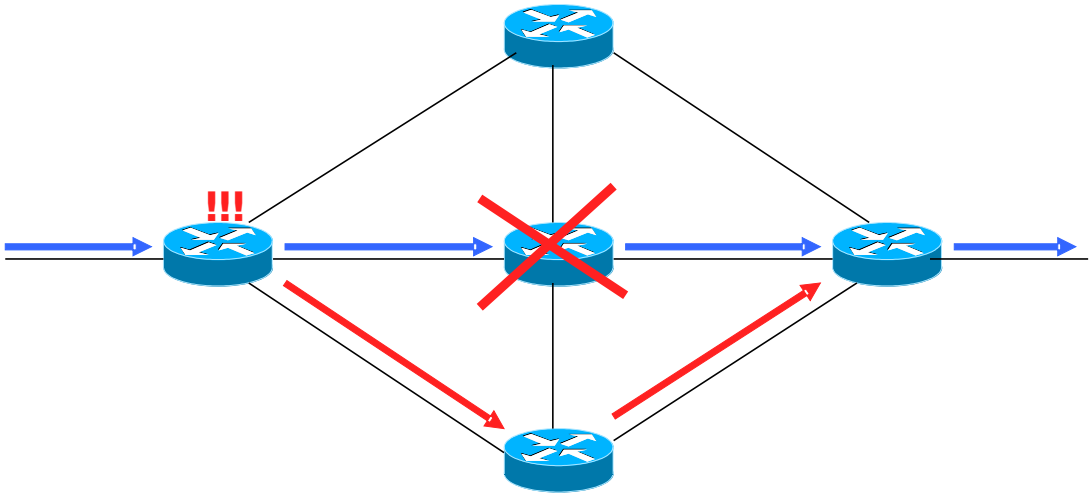
4.1.2. IP

Protokol IP običajno ne pokriva področje ene same neposredne fizične povezave, kot v primeru protokola MTP1. Okolje v katerem IP deluje, je skupek velikega števila med seboj povezanih usmerjevalnikov, ki samostojno usmerjajo datagrame IP. Tako je od ene do druge končne točke možno večje število različnih fizičnih poti. Takšne redundance ni na nižjih slojih MTP1 in MTP2 v SS7.



Slika 45: Različne poti med signalnima točkama v omrežju IP

V omrežju IP si skupni medij, oziroma njegove zmogljivosti, delijo vsi njegovi trenutni uporabniki. Usmerjevalniki, povezave in dostopi so nadzorovani in administrirani s strani različnih ponudnikov internetnih storitev, kar pomeni, da kvaliteta storitev ni enostavno nadzorovana. Pri zgostitvah prometa ali izpadu dela omrežja si usmerjevalniki sami dinamično popravijo usmerjevalne informacije in datagramu IP pripravijo novo pot.



Slika 46: Napaka na omrežju IP

Protokol IP na ta način kompenzira svojo nezanesljivo naravo, medtem ko MTP1 in MTP2 računata na zanesljivost neposrednih fizičnih povezav. Na MTP2 sloju so signalne povezave, posledično pa tudi celotne fizične povezave ves čas pod nadzorom zaradi nenehnega pošiljanja in potrjevanja sporočil. V SS7 na MTP2 ni redundance, saj je

povezava med dvema signalnima točkama nadzorovana in namenjena samo telefonskim storitvam z zagotovljeno hitrostjo prenosa. Praktično to pomeni, da bo povezava delovala, dokler se fizični kabel ne pretrga ali signali nimajo preveč zunanjih motenj.

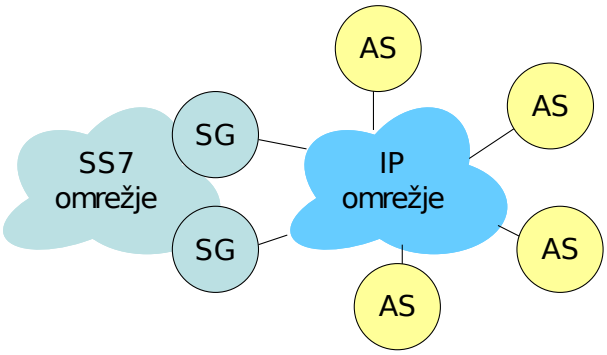
4.1.2.1.Vrste omrežij IP

Protokol IP se lahko uporablja v različnih omrežjih. Javni internet je le največje omrežje IP, ki pa ima specifične lastnosti in posebne zakonitosti. Internet je sestavljen iz več mrež usmerjevalnikov internetnih ponudnikov, ki se med seboj povezujejo s hrbteničnim omrežjem. Internetni ponudniki storitev nadzirajo in administrirajo svoje usmerjevalnike s pomočjo požarnih zidov, NAT-ov, usmerjevalnih tabel, protokolov MPLS, VPN idr. S tem lahko nadzirajo in upravljajo tudi promet, ki potuje skozi usmerjevalnike. Določenemu prometu lahko zagotovijo želeno hitrost oziroma prednost pri prenosu in usmerjanju. Na ta način se lahko zagotovi QoS določeni storitvi na nadzorovanem področju.

Za SS7 preko IP se lahko uporablja namenska lokalna omrežja, ki se preko prehodov povezujejo tudi na javni internet. V lokalnih omrežjih lahko operater vzpostavi celovit nadzor nad prometom in zmogljivostjo omrežja ter tako zagotovi visoko raven QoS. Za mednarodne telefonske klice pa lokalno omrežje verjetno ne bo zadostovalo in bo potrebno do tujega operaterja dostopati preko javnega omrežja, oziroma do tujega operaterja najeti podatkovni vod.

4.1.2.2.Prednosti protokola IP

Prednost signalizacije preko omrežja IP je predvsem v tem, da so smernice razvoja telekomunikacij uprte v univerzalno prenosno omrežje IP. Izboljšujejo se hitrosti omrežnih naprav, kapacitete fizičnih povezav, mrežni protokoli (IPv6) in varnost. Uporablja se tudi omejitev prometa, oddajanje več uporabnikom ter zagotavljanje QoS določenim storitvam. Dodatna prednost je tudi v tem, da se za povezovanje signalnih točk uporabi eno samo omrežje. Kapacitete v njem niso vnaprej zasedene, ampak se izvaja statistični mulitpleks med trenutnimi uporabniki. Tako ni več potrebno skrbeti za hierarhijo pri združevanju večjega števila povezav v časovni multipleks. Kapacitete povezav so na ta način bolj izkoriščene in lažje nadgradljive.



Slika 47: Povezovanje signalnih točk v omrežju IP

4.2.PRIMERJAVA NA DRUGEM SLOJU

V protokolnem skladu SS7 imamo na drugem sloju MTP2, ki skrbi za zanesljiv transport signalnih sporočil. V protokolnem skladu SIGTRAN imamo na drugem sloju protokol SCTP, ki ima podobne naloge kot MTP2 (zanesljiv prenos signalnih sporočil). Lastnosti in mehanizmi za zanesljivost posameznega sloja so podrobneje opisani v nadaljevanju.

4.2.1.MTP2

MTP2 sloj ustreza drugemu sloju referenčnega modela OSI (Open System Interconnection). V bistvu je to najnižji logični protokol v MTP skladu, ki leži na fizičnem nivoju. Skupaj s funkcijami podatkovnega signalne povezave omogoča zanesljiv prenos signalnih sporočil med dvema direktno povezanima signalnima vozliščema.

4.2.1.1.Formati signalnih sporočil

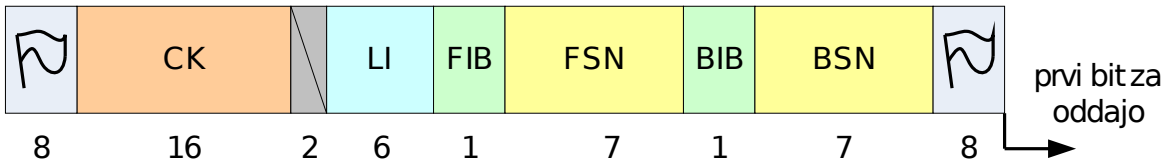
Signalne in druge informacije se prenašajo preko signalne povezave v okvirjih imenovanih signalne enote ali signalna sporočila (SU – signal units). Signalno spročilo je sestavljena iz različno dolgega informacijskega, oziroma sporočilnega polja. Lahko prenaša informacijo uporabnika ali informacijo signalne povezave, v tako imenovanem statusnem polju. Poleg tega vsebuje še določeno število parametrov različnih dolžin, ki vsebujejo podatke za nadzor prenosa sporočil.

Vrste signalnih sporočil, ki se ločijo po dolžini, so naslednje:

- signalno sporočilo za zapolnjevanje (FISU – Fill-In Signal Unit),
- signalno sporočilo o stanju povezave (LSSU – Link Status Signal Unit),
- signalno sporočilo z vsebino višjih slojev (MSU – Message Signal Unit).

Signalna sporočila FISU

Signalna sporočila FISU so najenostavnejše signalne enote na MTP2 nivoju. Prenašajo se med delovanjem, ko ni drugih signalnih sporočil. S tem zagotavljamo stalen bitni pretok in zasedenost povezave. V vsakem sprejetem FISU signalnem sporočilu izračunamo CRC (Cyclic Redundancy Check) zaščitno kodo za odkrivanje napak, ter tako lahko hitro odkrijemo okvarjeno povezavo in jo odstranimo iz uporabe.



Slika 48: Signalna enota FISU

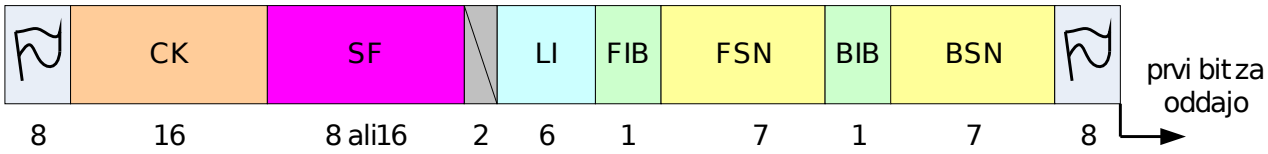
– zastavica (flag), "01111110".
CK – 16 bitov za detekcijo napak (check bits).
LI – kazalec dolžine (length indicator), število oktetov za LI in pred CK:

- LI = 0 - FISU,
- LI = 1 (ali 2) – LSSU,
- LI > 2 – MSU.

FSN – zaporedna številka SU, v katerem se prenaša (forward sequence number).
BSN – zaporedna številka zadnjega potrjenega SU (backward sequence number).
FIB, BIB – skupaj s FSN in BSN se uporabljata za sekvenčno kontrolo in potrjevanje pri osnovni metodi potrjevanja (forward indicator bit, backward indicator bit).

Signalna sporočila LSSU

Signalna sporočila LSSU se uporabljajo za izmenjavo informacije o statusu signalne povezave med dvema signalnima točkama. Pošiljajo se med vzpostavitvenim uvrščanjem za kontrolo signalne povezave.



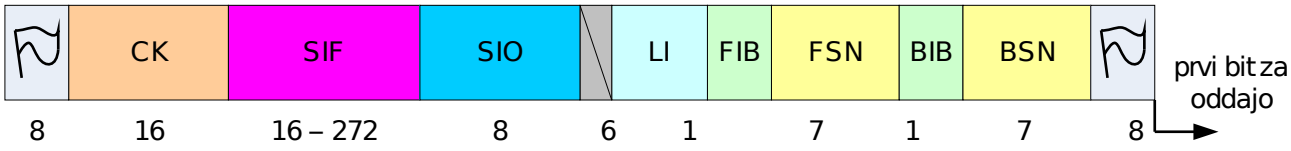
Slika 49: Signalna enota LSSU

SF – informacija o statusu povezave (status field):

- 0 - "SIO" - out of alignment,
- 1 - "SIN" - normal alignment,
- 2 - "SIE" - emergency alignment,
- 3 - "SIOS" - out of service,
- 4 - "SIPO" - processor outage,
- 5 - "SIB" - busy.

Signalna sporočila MSU

Signalna sporočila MSU so namenjene za prenašanje informacij iz višjih nivojev. Sporočilo lahko vsebuje signalne informacije iz tretjega nivoja MTP (MTP3) ali signalne informacije o uporabnikih na četrtem nivoju (TUP, ISUP, SCCP). Tip uporabniku se nahaja v polju SIO (Service Information Octet), uporabniške ali informacije za upravljanje z omrežjem pa se nahajajo v polju SIF (Signaling Information Field).



Slika 50: Signalna enota MSU

SIO – tip uporabnika, katerega informacija se nahaja v polju SIF.
SIF – vsebuje labelo za usmerjanje in "koristno" vsebino sporočila.

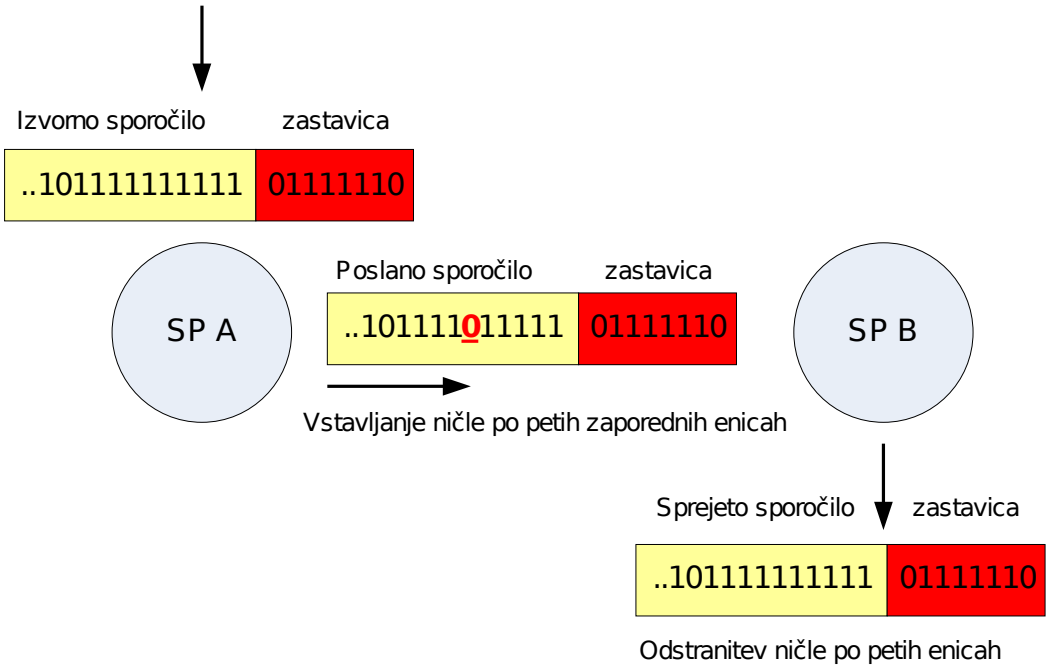
Osnovne funkcije, ki jih opravlja MTP2 sloj, so naštete spodaj:

- tvorba (razmejevanje) signalnih sporočil,
- uvrščanje signalnih sporočil,
- odkrivanje napak,
- popravljanje napak s ponovnim pošiljanjem,
- vzpostavitveno uvrščanje,
- opazovanje pogostosti napak,

- kontrola pretoka.

4.2.1.2.Tvorba in uvrščanje signalnih sporočil

Na začetku in koncu vsakega signalnega sporočila je postavljena zastavica (*flag*). To je poseben 8 bitni vzorec "01111110". Končna zastavica enega signalnega sporočila je lahko hkrati začetna zastavica naslednjega signalnega sporočila. Med dvema signalnima sporočiloma se lahko odda tudi več zastavic (na primer zaradi preobremenitve). Vzorec zastavice se ne sme nikoli pojaviti znotraj signalnega sporočila. To zagotovimo tako, da pri oddaji preverimo, ali se v signalnem sporočilu pojavi več kot pet zaporednih enic. V takem primeru vstavimo ničlo (*bit stuffing*). Na sprejemni strani signalnega linka nato odstranimo vsako ničlo, ki direktno sledi zaporedju petih enic. Na sprejemni strani zastavica, ki ji ne sledi takoj druga zastavica, pomeni začetek signalnega sporočila. Naslednja sprejeta zastavica določa konec signalne enote. Do izgube uvrščanja pride, če je sprejmemo zaporedje več kot šestih enic ali predolgo signalno sporočilo (279 sprejetih oktetov brez zastavice). Poleg tega preverjamo, da je dolžina signalnega sporočila mnogokratnik osmih bitov (po odstranitvi vstavljenih ničel) in dolžine najmanj šestih oktetov. V primeru izgube uvrščanja, označimo signalno povezavo za nesposobno, in začnemo tako imenovani postopek vzpostavitvenega uvrščanja, kjer ponovno integriteto povezave. Slika 51 prikazuje tvorbo signalnih sporočil v primeru, ko imamo zaporedno več kot pet enic.



Slika 51: Tvorba signalnih sporočil

4.2.1.3.Odkrivanje napak

Pri prenosu sporočil lahko pride do napake. Napake pomenijo izgubo sinhronizacije oziroma uvrščanja na sprejemni strani. Odkrivanje napak v signalnih stavkih se izvaja s pomočjo 16 bitne zaščitne kode (CK bits – Check bits), ki je dodana na koncu vsakega signalnega sporočila. Na oddajni strani je CK koda generirana s pomočjo 16 bitnega CRC polinoma ($x^{16}+x^{12}+x^5+1$) nad celotnim oddanim signalnim sporočilom. Na sprejemni strani se po posebnem postopku preveri ustreznost zaščitne kode. V primeru neujemanja sprejeto signalno sporočilo uničimo in pošljemo sosednji signalni točki negativno potrditev.

4.2.1.4.Popravljanje napak s ponovnim pošiljanjem

Naloga drugega sloja je, da potrdi vsako sprejeto signalno sporočilo. Sprejemna stran mora v primeru pravilno sprejetega sporočila poslati pozitivno potrditev. Oddano sporočilo ostane shranjeno na oddajni strani, dokler ne dobimo pozitivne potrditve. V določenih pogojih lahko signalno sporočilo pošljemo še enkrat.

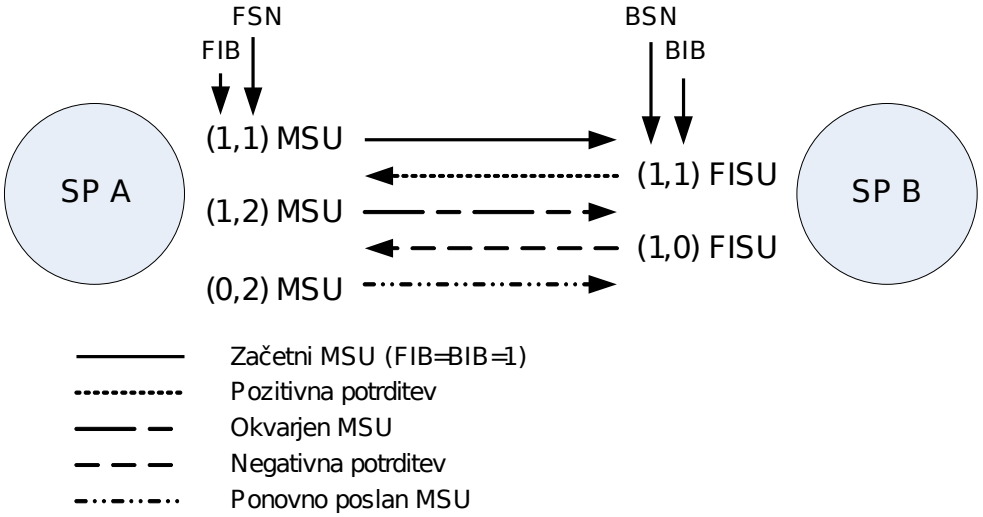
Predvidena sta dve metodi popravljanja napak:

- osnovna metoda popravljanja napak (BEC – Basic Error Correction),
- popravljanje napak s preventivno cikličnim ponovnim pošiljanjem (PCR – Preventive Cyclic Retransmission), ki se uporablja pri satelitskih signalnih povezavah in povezavah, kjer je zakasnitev razširjanja v eno smer večja od 125 ms.

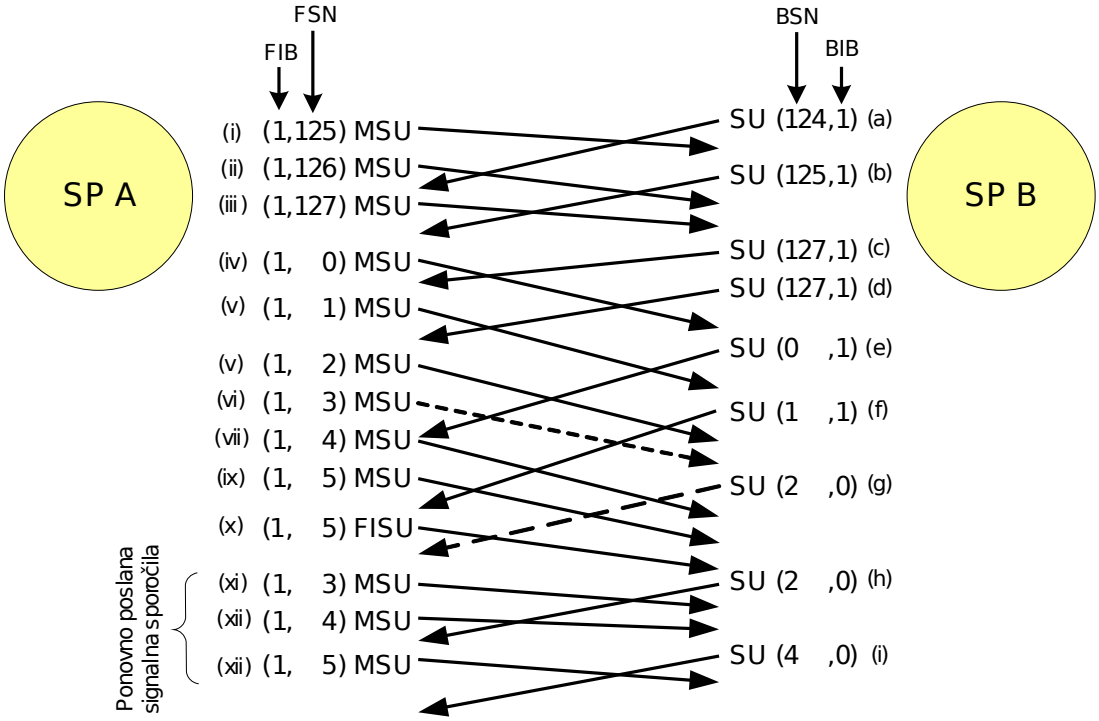
Obe metodi temeljita na ponovnem prenosu signalnih sporočil, ki so bile sprejete z napako. Pri osnovni metodi popravljanja napak se izrecno zahteva ponovljen prenos vseh signalnih sporočil poslanih za nepravilno sprejetim sporočilom. Pri metodi s preventivno ciklično ponovnim pošiljanjem pa ponovno pošljemo vsa sporočila, ki niso bila še potrjena.

Osnovna metoda popravljanja napak

Osnovna metoda popravljanja napak se uporablja pri zemeljskih signalnih povezavah, kjer je zakasnitev razširjanja v eno smer manjša od 15 ms. Pri osnovni metodi uporabljamo pozitivno in negativno potrjevanje. Pri pozitivnem potrjevanju ima indikator BIB enako vrednost kot indikator FIB v predhodnem potrditvi. Pri negativnem potrjevanju pa sta vrednosti indikatorjev BIB in FIB različni. V primeru sprejema negativne potrditve prenehamo s prenosom novih signalnih sporočil in oddamo sporočilo, za katerega je prišla negativna potrditev. Nato v pravilnem zaporedju prenesemo še vsa ostala sporočila, ki niso bila še potrjena. Pri ponovno poslanih sporočilih je indikator FIB invertiran glede na predhodno poslana sporočila pred napako. Tako zagotovimo, da nasprotna stran prepozna ponovno poslana signalna sporočila. Na spodnjih dveh slikah vidimo princip osnovne metode popravljanja napak in dejanski primer pri pošiljanju več zaporednih sporočil.



Slika 52: Princip osnovne metode popravljanja napak



Slika 53: Osnovna metoda popravljanja napak

Popravljanje napak s preventivno cikličnim ponovnim pošiljanjem

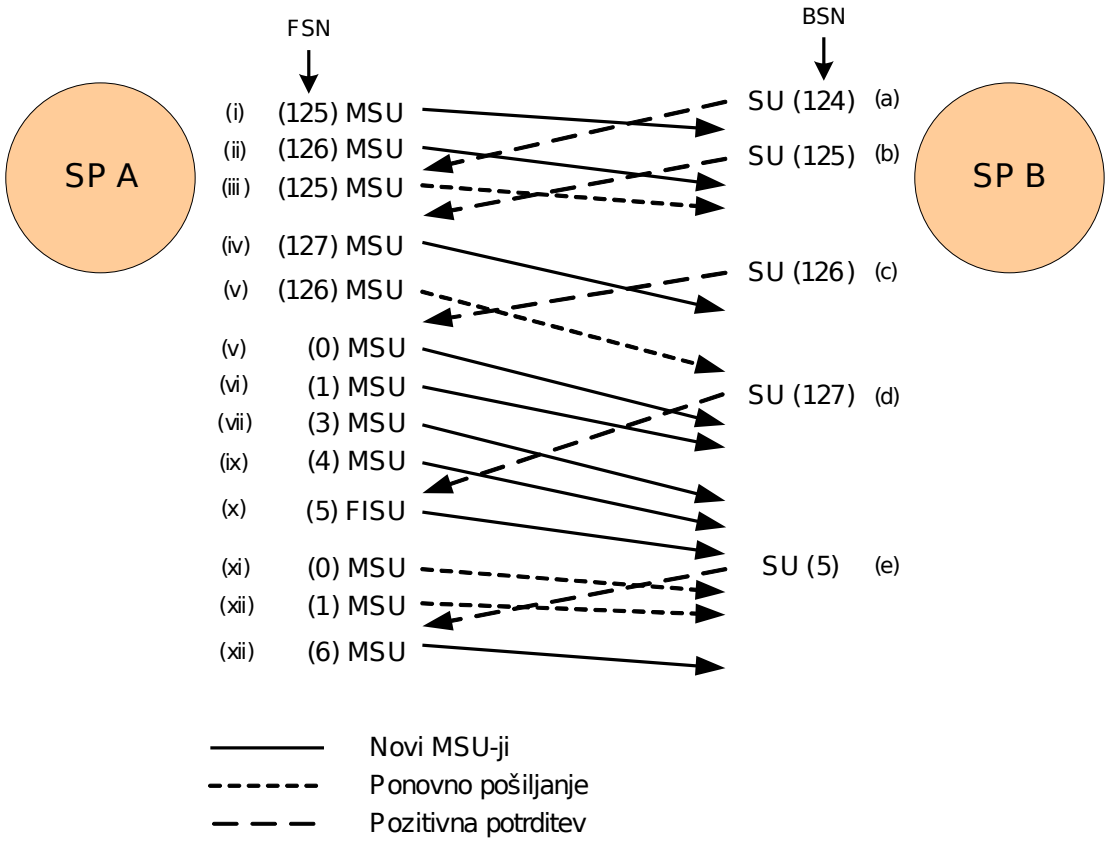
Preventivna metoda naj bi se uporabljala za medcelinske signalne povezave, kjer je enosmerna prenosna zakasnitev večja od 15 ms in za vse signalne povezave preko satelitov. Novejše meritve in testi na realnih povezavah so pokazali, da so rezultati boljši z osnovno metodo

vse do prenosne zakasnitve 45 ms, torej praktično za vse zemeljske povezave.

Pri preventivni metodi imamo pozitivno potrjevanje in ciklično preventivno ponavljanje (*cyclic retransmission*). Oddano signalno sporočilo shranimo dokler ne sprejmemo pozitivne potrditve. Ko nimamo novih sporočil za oddajo, se ciklično ponovno oddajajo vsa nepotrjena sporočila. V primeru, da pride ob tem času novo sporočilo, prekinemo s cikličnim oddajanjem nepotrjenih sporočil. Pri velikem prometu lahko postane ta metoda neučinkovita, zato uporabimo prisilno pošiljanje nepotrjenih sporočil. Postavljena sta dva kriterija, na osnovi katerih se odločimo za ponovno pošiljanje:

- število nepotrjenih sporočil,
- število nepotrjenih oktetov.

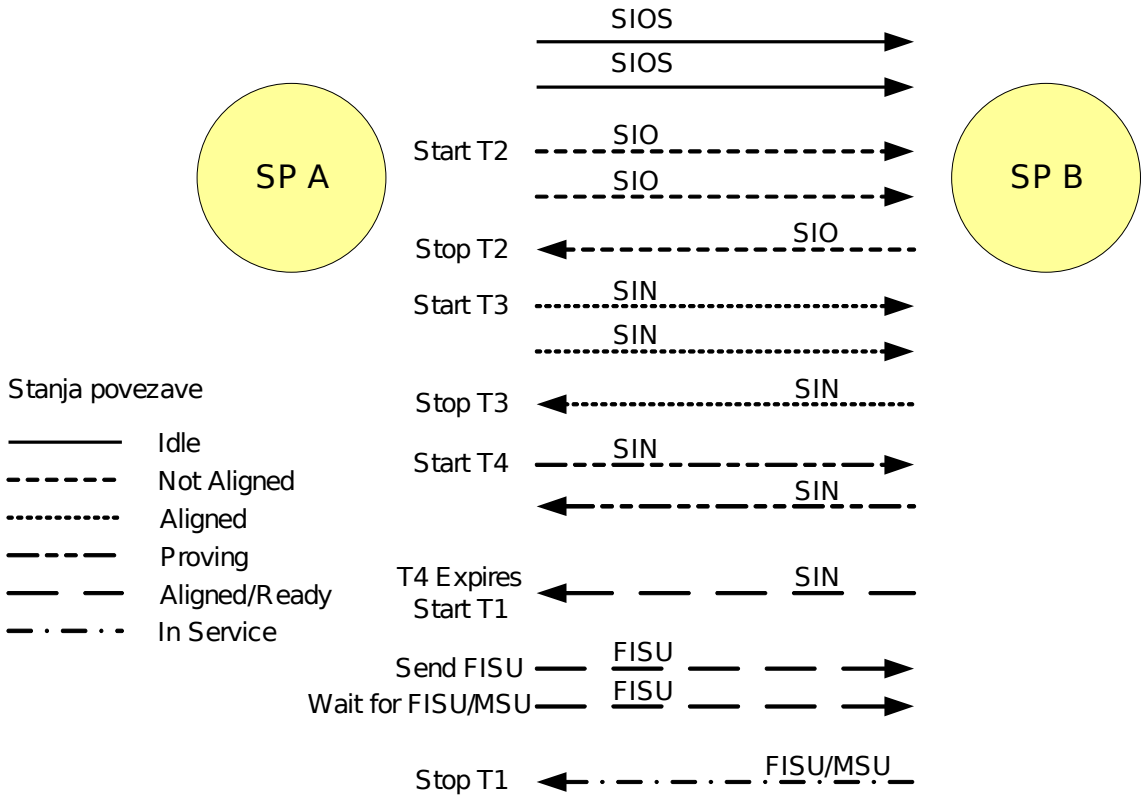
Če presežemo enega od navedenih pragov ustavimo pošiljanje novih signalnih sporočil in sprožimo prisilno pošiljanje. Načrtovanje pragov mora biti pazljivo, ker je od tega odvisna stabilnost povezave. Indikator FIB in BIB se ne uporabljata in sta postavljena na 1.



Slika 54: Metoda s preventivnim cikličnim ponovnim pošiljanjem

4.2.1.5.Vzpostavitveno uvrščanje

Postopek vzpostavitvenega uvrščanja (Initial alignment) se izvede ob začetni inicializaciji in ob ponovnem vzpostavljanju okvarjene signalne povezave. Po signalni povezavi, ki se vzpostavlja, se določen čas prisilno izmenjujejo sporočila s statusno informacijo o povezavi (LSSU) in se tako preverja kvaliteto ter zanesljivost signalne povezave. Če je stopnja napak previsoka, se postopek ponovi do petkrat, nato pa signalno povezavo označimo za nesposobno (Out of service). V nasprotnem primeru označimo signalno povezavo za sposobno (In service). Normalno izmenjevanje statusnih sporočil (SIN) traja približno 8,2 s, ob določenih pogojih pa lahko tretji sloj (MTP3) zahteva pospešeno preizkušanje signalne povezave (SIE se izmenjujejo približno 0.5 sek).



Slika 55: Vzpostavitveno uvrščanje

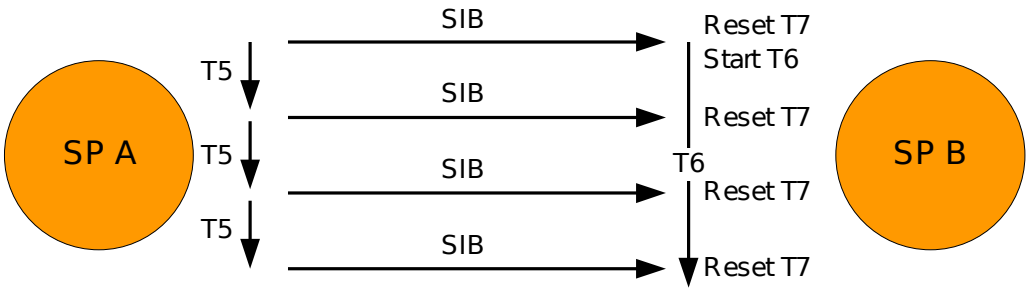
4.2.1.6.Opazovanje pogostosti napak

Predvidena sta dva načina opazovanja napak (Signalling link error monitoring). SUERM (Signalling Unit Error Rate Monitor) uporabljamo, ko je signalna povezava v normalnem obratovanju, in je opazovanje napak eden od kriterijev za izločitev signalne povezave iz prometa. Postopek je zasnovan na povečevanju in zmanjševanju števca napak. Števec povečamo za ena pri vsakem napačno sprejetem sporočilu. Števec se zmanjša za ena po 256 sprejetih signalnih sporočilih, toda ne pod nič. Če ni sinhronizacije (dobrega sprejema), se števec povečuje vsakih 16 oktetov (octet counting mode), dokler ne pravilno sprejmemo signalnega sporočila. Če števec doseže prag napak, izločimo signalno povezavo iz prometa.

AERM (Alignment Error Rate Monitor) se uporablja med vzpostavitvenim uvrščanjem in je kriterij za nadaljnjo uporabo povezave. V tem postopku uporabljamo linearen števec napak, ki ga v začetku postavimo na nič. Ob vsakem sporočilu sprejetem z napako (ali na 16 sprejetih oktetov pri izgubi uvrščanja) se števec poveča za ena. Vzpostavitveno uvrščanje prekinemo, če je presežen prag napak pred iztekom preizkuševalnega časa.

4.2.1.7.Kontrola pretoka

Kontrola pretoka uporabljamo v primeru prometne preobremenjenosti. Merilo za preobremenitev je zasedenost sprejemne vrste za sporočila MSU. Sprejemna stran v stanju preobremenitve periodično (80 – 120 ms) obvešča sosednjo stran z signalnim sporočilom SIB (Status Indicator Busy) in zadrži potrjevanje. Če ima možnost, sprejemna stran shranjuje in potrjuje sprejeta signalna sporočila MSU. Po odpravi tega stanja prenos steče normalno naprej. V primeru, ko stanje preobremenitve traja predolgo (3 do 6 sekund), oddajna stran postavi signalno povezavo iz uporabe.



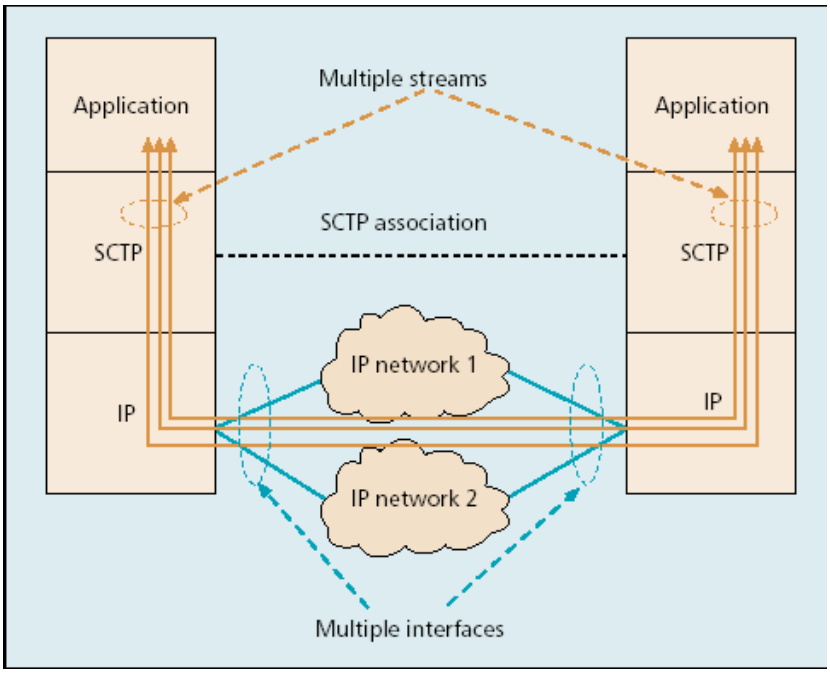
Slika 56: Kontrola pretoka s signalnim sporočilom SIB

4.2.2.SCTP

SCTP ima podobno vlogo kot drugi sloj v SS7 protokolnem skladu (MTP2). Višje ležečim protokolom zagotavlja zanesljiv prenos uporabniških informacij na način, da je sprejem vseh informacij potrjen, brez napak pri prenosu in da uporabniške informacije pri prenosu niso podvojene. V ta namen uporablja več postopkov, ki so opisani v nadaljevanju.

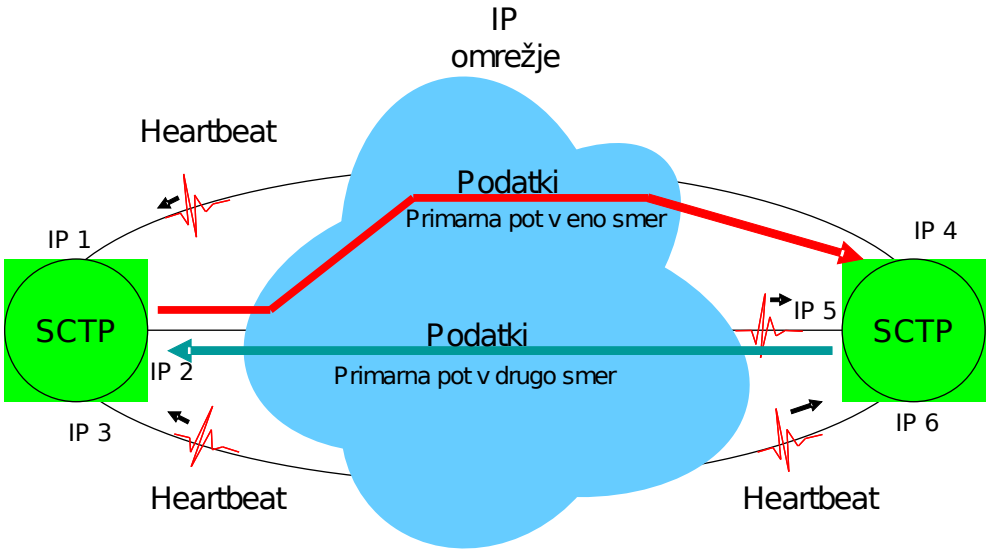
4.2.2.1.Večdomnost

Večdomnost pomeni, da je končna točka v SCTP povezavi (signalna točka) lahko predstavljena z več IP naslovi, ki omogočajo hkratno uporabo več različnih dostopov do omrežja IP. Zaradi narave protokola IP je tako signalna točka dostopna preko fizično različnih poti. Če se na eni od teh poti pojavijo napake, zaradi katerih postane ta dostop nedosegljiv (npr. zaradi interference, napake na povezavi, močne preobremenjenosti omrežja, ipd.) lahko končna točka še vedno prejema podatke preko drugega dostopa oziroma poti.



Slika 57: Večdomnost

SCTP uporablja večdomnost samo za redundanco in ne za razdeljevanje prometa (ang. loadshare). Vsaka končna točka izbere en primaren IP naslov kamor pošilja vse nove podatkovne chunk-e med normalnim prenašanjem podatkov. Nepotrjene podatkovne chunke ponovno pošlje na drug naslov IP ter pri tem domneva, da druga pot poveča verjetnost, da bo ta podatek prispel na drugo stran. Nadaljnja nezmožnost doseganja primarnega naslova povzroči zaznavo napake, ki ima za posledico to, da začne končna točka pošiljati vse podatke na drug naslov IP. To izvaja, dokler prekinjena primarna pot ne postane ponovno dostopna ali pa dobi navodilo zgornjega sloja, da zamenja primarno pot.



Slika 58: Primarne in alternativne poti

SCTP torej omogoča vzpostavitev in nadzor več različnih fizičnih poti med dvema signalnima točkama. Ekvivalentna funkcionalnost se v SS7 protokolnem skladu razdeli na dva dela:

1. MTP2 vzpostavlja in nadzoruje posamezno signalno povezavo.
2. MTP3 zbira informacije, ki jih pridobi od različnih MTP2 procesov, o vseh možnih signalnih povezavah v enem signalnem snopu. Med aktivnimi povezavami nato enakomerno razdeljuje promet in izvaja preklope pri morebitnih napakah.

SCTP med vsemi možnimi potmi izbere eno samo primarno, skozi katero pošilja ves promet. Druge povezave uporabi le v skrajnih primerih, ko pride do napak ali zamud pri potrjevanju. Večdomnost torej ne omogoča razdeljevanja prometa po fizično različnih poteh.

Približek razdeljevanja prometa v SCTP povezavi omogoča večtokovnost (ang. multistreaming), ki promet usmerja enakomerno preko več sporočilnih tokov. To delovanje je omejeno le na logični nivo celotne SCTP povezave. Ker se podatki večinoma prenašajo le preko primarne poti, je razdeljevanje prometa na sporočilne tokove omejeno na eno samo fizično pot. Razdeljevanje prometa med signalnimi točkami v SIGTRAN protokolnem skladu izvaja šele prilagodilni sloj M3UA.

4.2.2.2.Dostopnost poti

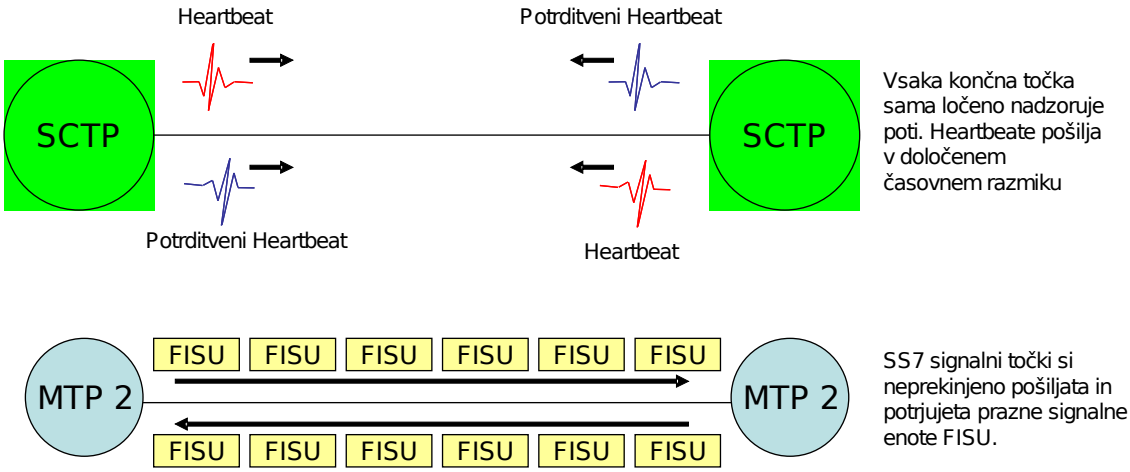
SCTP spremlja dostopnost vsake poti s pomočjo dveh postopkov:

- potrjevanja (SACK) podatkovnih chunk-ov,
- pošiljanje heartbeat chunk-ov.

Heartbeat je kontrolno sporočilo, ki ga SCTP pošilja končni točki z namenom, da preveri dosegljivost točke preko določenega naslova IP. Prejemnik heartbeata nato odgovori s potrditvenim heartbeatom, ki mora vsebovati identične informacije, kot jih vsebuje prejeti heartbeat.

Sposobnost vseh poti se ves čas preverja s pošiljanjem heartbeatov, razen ko se po poti prenaša uporabniški promet, saj končna točka že s potrditvami sprejema pridobi informacijo o dostopnosti druge točke. Heartbeati se pošiljajo periodično z določenim časovnim razmikom. Na ta način ima SCTP ves čas pripravljeno informacijo o aktivnih alternativnih poteh. Uporabniški sloj lahko v času, ko je povezava vzpostavljena, spreminja periodo pošiljanja heartbeatov, ima pa tudi možnost zaustavitve njihovega pošiljanja.

V primeru, ko se zaradi nepotrditev doseže največje še dovoljeno število zaporednih iztekov časovnikov za ponovno pošiljanje, pošiljatelj domneva, da je končna točka preko danega naslova IP nedosegljiva. V SS7 preverja dosegljivost signalne točke preko ene logične povezave sloj MTP2. Namesto heartbeatov uporablja MTP2 princip nenehnega pošiljanja podatkov. Kadar signalnega prometa ni na voljo, se pošiljajo polnilni stavki FISU. Če promet preko povezave preneha ali stopnja napak preseže prag, MTP2 predpostavi, da je na povezavi prišlo do napake. Primerjavo prikazuje slika 59.

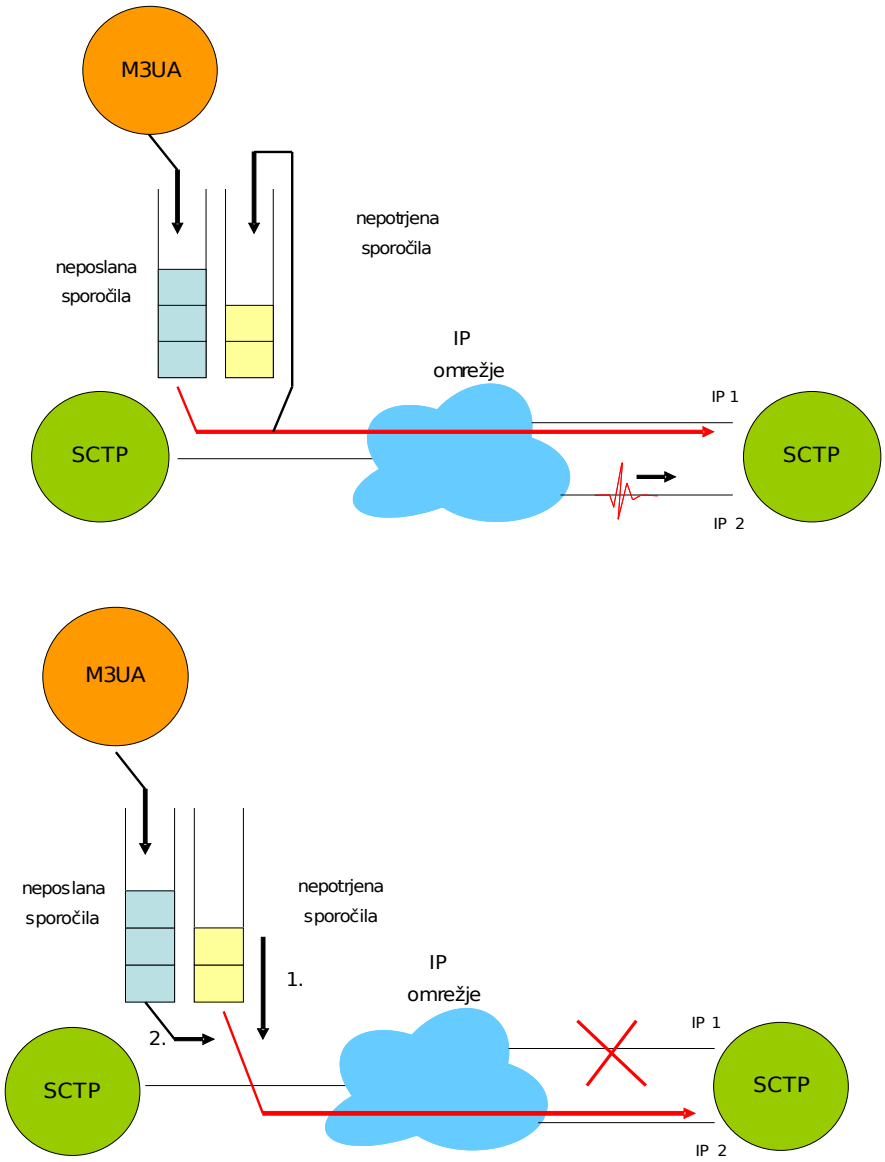


Slika 59: Primerjava preverjanja dostopnosti pri SCTP in MTP

4.2.2.3.Preklopi

Alternativne poti

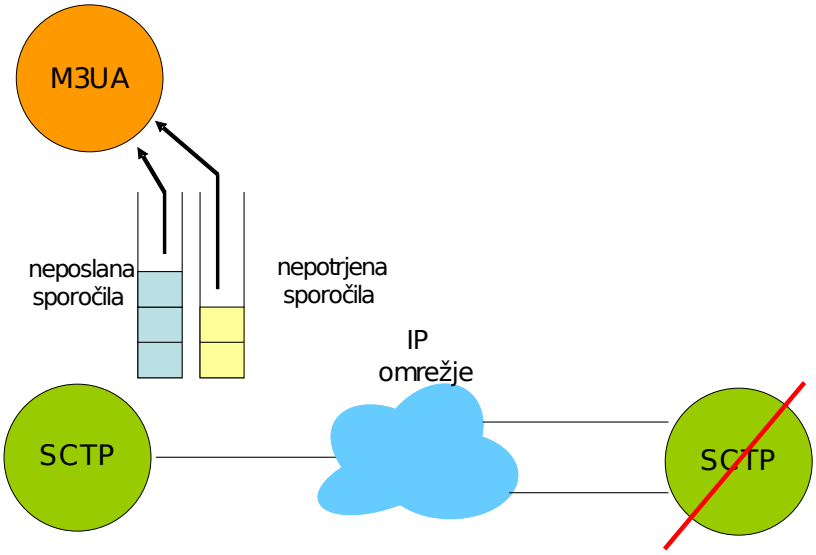
SCTP hrani v svojem pomnilniku vse poslane podatkovne chunke, dokler od prejemnika ne dobi potrditve njihovega sprejema. V primeru napake, ko naslov IP ni več dosegljiv po primarni poti, SCTP poskusi ponovno poslati nepotrjene chunke po drugi poti oziroma na drug naslov IP, ki ga je imel označenega kot aktivnega. Ker se uporabniški sloj še ne zaveda napake, še vedno pošilja svoja sporočila za transport. SCTP ločeno shranjuje nepotrjena in neposlana sporočila kot prikazuje slika 60.



Slika 60: Shranjevanje sporočil za potrebe preklopa oziroma ponovnega pošiljanja

Vračanje sporočil na prilagodilni sloj

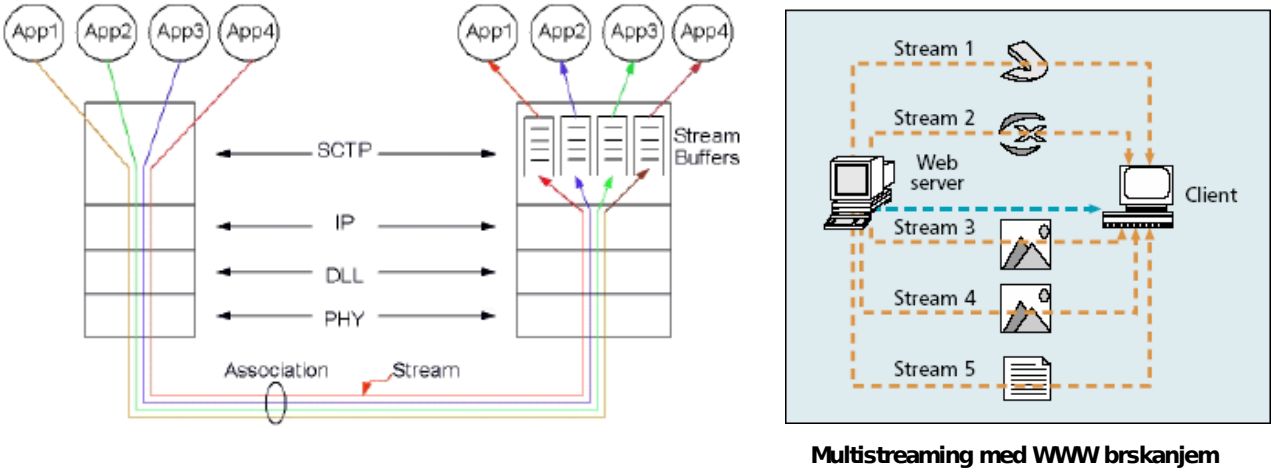
Ko končna točka ni več dosegljiva preko nobene od možnih poti, SCTP sporoči izgubo povezave višjemu uporabniškemu sloju. Uporabniški sloj lahko zahteva vrnitev vseh nepotrjenih in neposlanih sporočil. To funkcijo vračanja sporočil M3UA uporabi pri preusmeritvi prometa na drugo povezavo.



Slika 61: Vračanje nepotrjenih in neposlanih sporočil

4.2.2.4.Večtokovnost

SCTP razdeli povezavo na več logičnih sporočilnih tokov. Podatki potujejo navidezno vzporedno preko iste fizične poti, trenutno izbrane primarne poti.



Slika 62: Večtokovnost

SCTP zagotavlja zaporedno dostavo glede na posamičen sporočilni tok. Če se izgubi paket SCTP s podatkovnih chunkom, ki zahteva dostavo v pravilnem vrstnem redu, bo prekinjeno zaporedno dostavljanje le preko njegovega sporočilnega toka. Podatki ostalih sporočilnih tokov se bodo nemoteno dostavljali višjim slojem v pravilnem zaporedju. Postopek več sporočilnih tokov uspešno blaži manjše napake, kot so izguba ali daljše

zakasnitve posamičnega paketa SCTP, kratke zgostitve prometa in preklopi med potmi.

4.3.PRIMERJAVA NA TRETJEM SLOJU

V protokolnem skladu SS7 imamo na tretjem sloju MTP3, ki ima nadzor nad signalnim omrežjem in skrbi za pravilno dostavo uporabniških sporočil. V protokolnem skladu SIGTRAN imamo na tretjem nivoju več prilagodilnih slojev (M3UA, M2UA, M2PA, …), od katerih ima vsak svoje specifične lastnosti in naloge. V nadaljevanju so podrobneje opisane lastnosti in funkcije prilagodilnega sloja M3UA, ki je funkcionalno najbolj podoben MTP3, obenem pa tudi najbolj kompleksen.

4.3.1.MTP3

Funkcije omrežnega nivoja morajo zagotoviti zanesljiv prenos signalnih sporočil od izvornega do ponornega uporabnika (UP – User Part). Prenosa ne sme prekiniti v primeru okvare posameznih elementov signalnega omrežja (signalna povezava, signalna točka, …). Za sporočila z enako SLS (Signaling Link Selection) kodo je zagotovljeno sosledje na sprejemu. Nobeno signalno sporočilo ne sme manjkati, nobeno ne sme biti podvojeno, sprejeta morajo biti v enakem vrstnem redu, kot jih je oddal uporabnik na oddajni strani. Omrežni nivo stalno avtomatsko vzdržuje signalne povezave in skrbi, da je usmerjanje signalnih sporočil kar najbolj učinkovito. Ob okvarah rekonfigurira omrežje.

Funkcije omrežnega nivoja so ločene na dva dela:

- rokovanje s signalnimi sporočili (SMH – Signaling Message Handling). Funkcija skrbi za prenos signalnih sporočil, sprejemanje sporočil od uporabnikov in usmerjanje na signalno povezavo proti ponornemu vozlišču. Signalna sporočila sprejeta iz signalnih povezav se posredujejo določenemu uporabniku ali pa jih v primeru prehoda usmerimo na določeno signalno povezavo proti ponornemu vozlišču.
- upravljanje signalnega omrežja (SNM – Signaling Network Management). Funkcija določa na podlagi stanja signalne mreže trenutno usmerjanje sporočil. Ob spremembi stanja posameznih elementov v signalnem omrežju (signalna povezava, tranzitna

signalna točka) izvede rekonfiguracijo in druge akcije, da ohranimo ali obnovimo sposobnost prenosa signalnih sporočil. Z opisano metodo skušamo signalno omrežje vzdrževati v čim bolj propustnem stanju in zato aktiviramo oziroma restavriramo signalne povezave. Med signalnimi vozlišči se izmenjujejo informacije o stanju (dostopnost, preobremenitve).

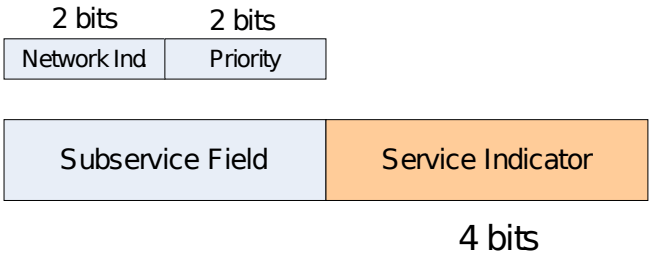
4.3.1.1.Format sporočil

Delež MTP3 signalnega sporočila se sestoji iz dveh delov:

- SIO (Service Information Octet) polja, ki določa uporabnika,
- SIF (Signaling Information Filed) polja, ki vsebuje usmerjevalno labelo (ang. routing label) in uporabniško informacijo (User Data).

SIO

SIO polje je sestavljeno iz SI (Service Indicator) polja in SSF (Subservice Field) polja. MTP3 uporablja SI za dostavo signalnih sporočil pravemu MTP3 uporabniku. Spodnja tabela (Tabela 3) prikazuje vrednosti in tipe MTP3 uporabnikov. Polje SSF vsebuje NI (Network Indicator) in polje z prioriteto, ki se uporablja samo v ANSI (American National Standards Institute) omrežjih. V tabeli 4 so prikazane vrednosti NI.



Slika 63: SIO polje

Binarna vrednost	Tip uporabnika
0000	Signaling Network Management Messages
0001	Signaling Network Testing and Maintenance

	Messages
0010	Signaling Network Testing and Maintenance Special Messages (ANSI) or Spare (ITU-T)
0011	SCCP
0100	Telephone User Part
0101	ISDN User Part
0110	Data User Part (call and circuit-related messages)
0111	Data User Part (facility registration and cancellation messages)
1000	Reserved for MTP Testing User Part
1001	Broadband ISDN User Part
1010	Satellite ISDN User Part
1011-1111	Spare

Tabela 4: Tipi MTP3 uporabnikov

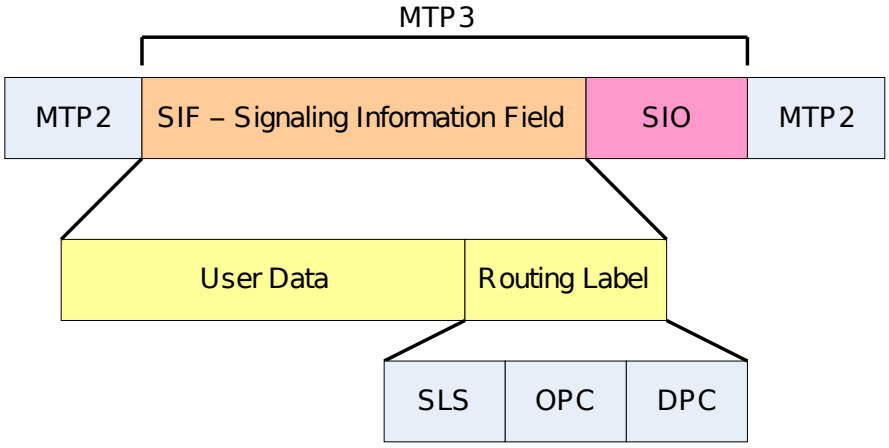
Binarna vrednost	**Tip sporočila**
0000	International
0001	International Spare
0010	National
0011	National Spare

Tabela 5: Vrednosti NI (Network Indicator)

SIF

SIF polje vsebuje dejansko uporabniške podatke MTP3 ali višjih nivojev (npr. telefonska številka, kontrolna sporočila, sporočila za vzdrževanje). Uporabniška vsebina je odvisna od tipa uporabnika, ki določen z SI (Service Indicator) poljem. Poleg uporabniškega dela je prisotna še usmerjevalna tabela, ki je določena s tremi komponentami:

- SLS (Signaling Link Selection) – izbira signalne povezave,
- OPC (Originating Point Code) – koda izvornega signalnega vozlišča,
- DPC (Destination Point Code) – koda ponornega signalnega vozlišča.

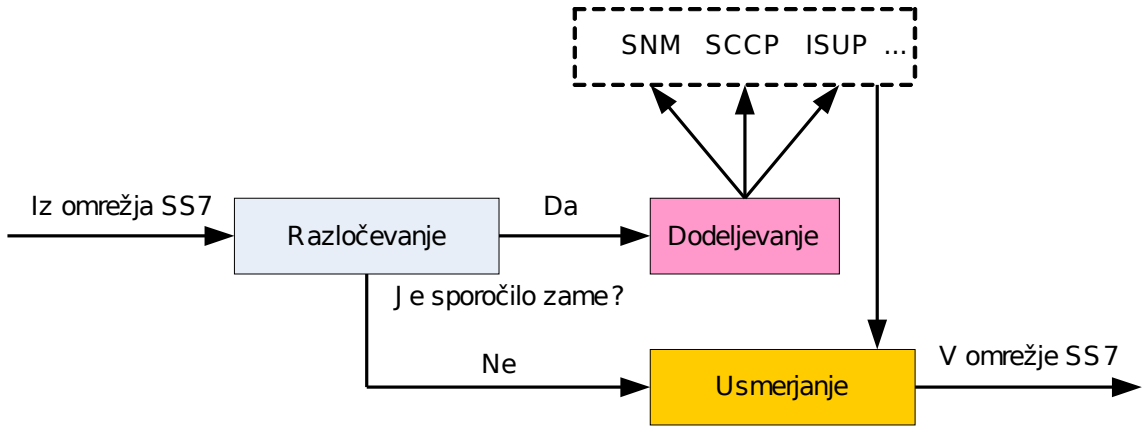


Slika 64: Vsebina MTP3 sporočila

Polje SLS se uporablja za izbiro signalne povezave in/ali signalne smeri v primeru delitve signalnega prometa (loadsharing). V primeru telefonskih sporočil je to zadnji del identifikacije govornega kanala (Circuit ID code). Pri vseh uporabnikih velja, da imajo vsa sporočila, ki se nanašajo na določeno uporabniško zvezo (ali transakcijo), isto SLS kodo.

4.3.1.2.Rokovanje s signalnimi sporočili

Funkcije rokovanja s signalnimi sporočili vsebujejo funkcije razločevanja (discrimination), dodeljevanja (distribution) in usmerjanja (routing) signalnih sporočil. Te funkcije se izvajajo v vsakem vozlišču signalnega omrežja in temeljijo na usmerjevalni labeli (routing label) in polju SIO (Service Indicator), ki določa uporabnika. Usmerjevalna labela je sestavljena iz kode ponornega vozlišča (DPC), kode izvornega vozlišča (OPC) in izbire signalnega povezave (SLS). Po mednarodnih CCITT standardih sta DPC in OPC velika 14 bitov, SLS pa 4 bite.



Slika 65: Rokovanje s signalnimi sporočili

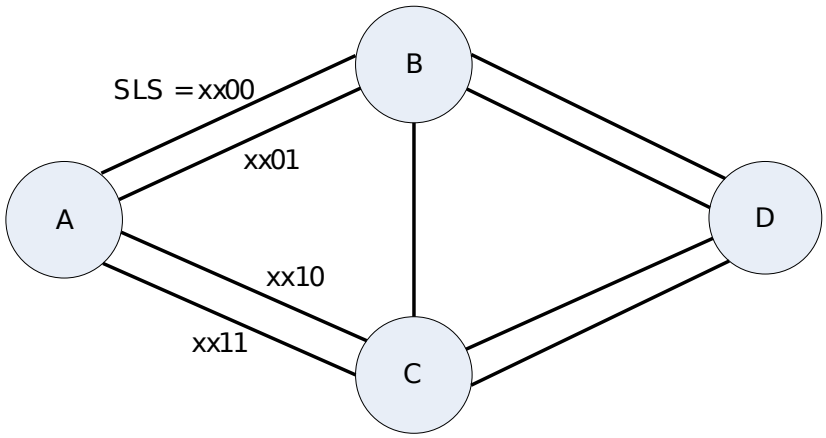
Za vsako sprejeto signalno sporočilo v okviru funkcije razločevanja na osnovi kode ponornega signalnega vozlišča (DPC) ugotovimo, ali je sporočilo namenjeno tukajšnjemu vozlišču ali drugemu. V primeru, ko je sporočilo namenjeno drugemu vozlišču, preverimo prenosne zmožnosti vozlišča, ter sporočilo pošljemo v funkcijo usmerjanja. V nasprotnem primeru, ko je sprejeto sporočilo naslovljeno na le-to vozlišče, se v funkciji dodeljevanja na osnovi SIO polja dostavi sporočilo pravemu uporabniku ali funkcijam MTP.

Usmerjanje signalnih sporočil v signalnih povezavah proti ponornemu vozlišču je skupno za vsa sporočila, ki izvirajo od uporabnikov v tem vozlišču in za tranzitna sporočila. Za usmerjanje uporabljamo usmerjevalne tabele, ki se kreirajo glede na trenutno stanje omrežja (za obveščanje stanja skrbijo procesi upravljanja signalnega omrežja (SNM). Usmerjanje se izvaja na osnovi DPC in SLS.

V splošnem lahko uporabljamo več signalnih povezav za usmerjanje sporočil proti določenemu ponoru. Izbira določene signalne povezave se izvede na osnovi polja SLS. To imenujemo delitev prometa (loadsharing). Delitev lahko poteka znotraj snopa povezav med dvema signalnima vozliščema (link set), lahko pa tudi med signalni povezavami, ki pripadajo dvema snopoma. Zbirko vseh signalnih povezav iz enega ali več snopov za delitev prometa proti določenemu ponoru, imenujemo kombinirani snop povezav (combined link set). Poleg normalnih smeri imamo običajno še rezervne smeri, ki prevzamejo signalizacijski promet v primeru izpada osnovnih smeri.

Namen delitve prometa je v tem, da imamo enakomerno obremenitev signalnih povezav znotraj kombiniranega snopa povezav. Za sporočila ki morajo ohraniti vrstni red, uporabljamo isti SLS. V tem primeru bodo sporočila šla po isti poti. Z namenom da zagotovimo pravilno razporeditev prometne obremenitve z uporabo SLS polja je kritično, da so SLS kode dodeljene na pravilen način. Metoda delitve prometa na podlagi SLS kode ne zagotavlja popolnoma enakomerne obremenjenosti signalnih povezav v vseh primerih (v primer, ko imamo 3, 5, 6,.. signalnih povezav v kombiniranem snopu). Na spodnji sliki (Slika 66) vidimo delitev prometa med vozliščema A in D. Promet se

deli med štirimi signalnimi povezavami, ki pripadajo dvema snopoma (dvema smerema).



Slika 66: Delitev prometa na osnovi SLS-a

Potek usmerjanja:

- iz signalnega sporočila izluščimo DPC in SLS.
- če je DPC dostopna, izberemo signalno povezavo. V nasprotnem primeru obvestimo izvorni uporabniški sloj o nedostopnosti.
- glede na bite SLS, izbere ustrezno signalno povezavo (loadsharing).
- Signalno sporočilo oddamo na izbrano signalno povezavo.

Signalno vozlišče je lahko:

- samo tranzitno signalno vozlišče (STP). Vozlišče nima priključenih uporabnikov in služi samo usmerjanju in prenosu sporočil.
- samo končno signalno vozlišče. Vsa sporočila, ki pridejo v to vozlišče so temu vozlišču tudi namenjena (uporabnikom ali tretjemu nivoju).
- signalno vozlišče, ki ima vse funkcije. Je torej tranzitno in končno signalno vozlišče.

4.3.1.3.Upravljanje signalnega omrežja

Namen funkcij upravljanja signalnega omrežja je zagotavljanje sprememb signalnega omrežja v primeru okvar signalnih povezav ali vozlišč, ter upravljanje signalnega prometa v primeru preobremenitev ali blokad. V primeru okvare naredimo spremembe tako, da se sporočila ne izgubijo, da pridejo na cilj v pravem vrstnem redu in da

zakasnitev ni prevelika. Seveda obstajajo tudi funkcije, ki ob odpravi okvar vrnejo omrežje v prvotno stanje.
Preureditve se izvršijo s preusmeritvijo signalnega prometa na alternativne signalne povezave ali preko alternativnih signalnih točk (STP-jev). Za opravljanje teh funkcij ima SNM naslednje postopke:

- aktiviranje, obnovitev in deaktiviranje signalne povezave,
- aktiviranje snopa signalnih povezav,
- prepoved prometa za določen ponor,
- dovolitev prometa za določen ponor,
- testiranje signalne smeri,
- zamenjava signalne povezave (changeover),
- povratek signalne povezave (changeback),
- pospešena preusmeritev prometa na drugo signalno smer (forced rerouting),
- kontrolirana preusmeritev prometa nazaj na osnovno smer (controlled rerouting),
- kontrola pretoka signalnega prometa (signalling traffic flow control).

Za izvrševanje teh postopkov je potrebno komunikacija med 3.nivoji signalnih vozlišč. Za vsak postopek pošiljamo določena sporočila. Funkcije upravljanja signalne mreže (SNM), ki so opisane zgoraj, so sestavljene iz treh delov:

- Upravljanje s signalnim prometom (STM – Signalling Trafic Management) skrbi za prenos prometa iz okvarjenih signalnih povezav ob okvarah na alternativne povezave, ob obnovitvi okvarjenih povezav pa prenos na osnovne. Pri preobremenitvah začasno zmanjša signalni promet.
- Upravljanje s signalnimi povezavami (SLM – Signalling Link Management) vodi evidenco o signalnih povezavah, ter skrbi za njihovo vključevanje in izključevanje.
- Upravljanje s signalnimi smermi (SRM – Signalling Routing Management) skrbi za izmenjavo informacij glede na sposobnosti signalnih smeri med signalnimi vozlišči. Izpadle smeri periodično testira.

Ob spremembi statusa signalne povezave, signalne smeri ali signalnega vozlišča, se aktivirajo funkcije, ki so podrobneje naštete in opisane v nadaljevanju.

Upravljanje s signalnim prometom

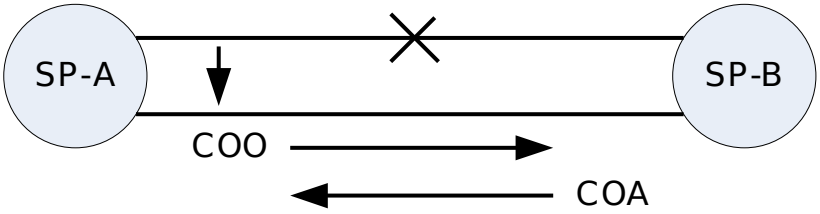
Funkcije upravljanja signalnega prometa (STM) uporabljamo, da brez izgub ali podvajanja preusmerimo signalni promet iz nesposobne signalne povezave ali smeri na eno ali več alternativnih signalnih povezav ali smeri, oziroma da zmanjšajo signalni promet v primeru preobremenitve (congestion). Pri signalnih povezavah imamo postopka zamenjave (changeover) in vrnitev (changeback) signalne povezave. Pri signalnih smereh pa poznamo postopek prisiljene preusmeritve (forced rerouting), ter postopek kontrolirane preusmeritve (controlled rerouting). Vsi našteti postopki so opisani v nadaljevanju. Ko postane signalno vozlišče uporabno, postopek ponovne vzpostavitve signalne točke (signalling point restart) poskrbi, da se usmerjanje postavi v skladu z novimi možnostmi.

Izpad signalne povezave
Ob izpadu signalne povezave (zaradi okvare na drugem ali prvem nivoju, blokiranja ali prepovedi iz upravljanja omrežja) se izvršijo naslednji postopki:

- Sprožimo postopek zamenjave signalne povezave (changeover).
- Če obstaja sposobna povezava (ali več) v istem snopu, preusmerimo promet nanjo.
- Če izpade zadnja povezava v snopu, preusmerimo promet na druge snope.
- Če promet do katerega od ponorov ni več možen, ustavimo postopek zamenjave, uporabnike (UP) in sosednja signalna vozlišča pa obvestimo o nedostopnosti.
- Če obstaja sposobna povezava v istem snopu, sprožimo postopek za vrnitev neprenesenih sporočil. Neprenesena sporočila prestavimo na alternativno povezavo.
- Če od sosednje strani ni mogoče dobiti podatka o zadnjem sprejetem sporočilu, so neprenesena sporočila izgubljena. Pošiljanje novih sporočil po alternativnih smereh nekaj časa zadržujemo (1 sekundo), da ohranimo zaporedje signalnih sporočil.

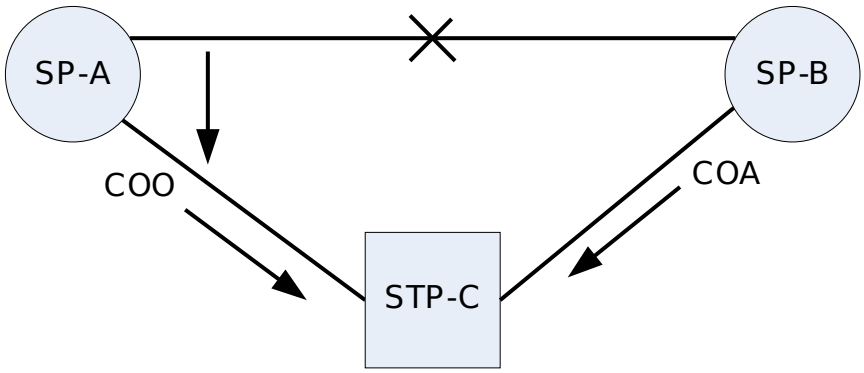
- Med trajanjem postopka sporočila shranjujemo v pomnilnik in ob koncu postopka pošljemo kot prva na alternativno povezavo.

Na sliki 67 imamo primer izpada signalne povezave. Po vzporedni povezavi pošljemo sporočilo COO (Changeover Order). Sosednje vozlišče odgovori s sporočilom COA (Changeover Acknowledgement), ki nosi tudi številko zadnjega sprejetega sporočila. Promet se preusmeri po sposobni povezavi.



Slika 67: Zamenjava (changover) v istem snopu

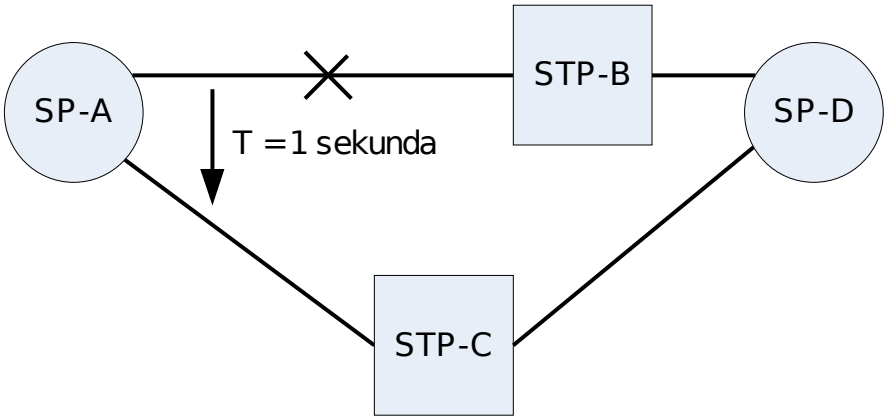
Na sliki 68 imamo primer, ko nimamo vzporedne povezave. Promet preusmerimo na povezavo, ki poteka preko STP-ja. Sporočilo COO lahko pošljemo v SP-B preko STP-C. Tudi v tem primeru zanesljivo ne pride do izgube ali podvajanja sporočil. Ravno tako je zagotovljen pravilen vrstni red sporočil.



Slika 68: Zamenjava (changover) na drug snop

Na sliki 69 imamo primer časovno kontrolirane zamenjave povezave. Ker sporočila do vozlišča SP-D potujejo po popolnoma drugi poti, ne moremo zagotoviti vrstnega reda sporočil. Zato ne pošiljamo sporočil COO in COA, temveč v signalni točki SP-A počakamo določen čas (1 sekunda) in potem usmerjamo sporočila na povezavo proti STP-C. Med

čakanjem se sporočila shranjujejo v pomnilnik in se ob koncu časovne kontrole oddajo prva.



Slika 69: Časovno (changover) kontrolirana zamenjava

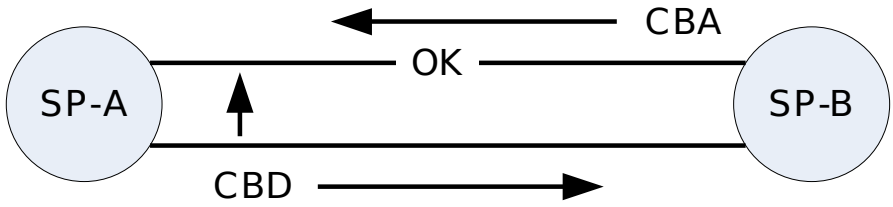
Obnovitev signalne povezave

Obnovitev signalne povezave poteka na sledeč način:

- Ko postane signalna povezava znova (ali prvič) aktivna, sprožimo postopek vrnitve signalnega prometa (changeback) na usposobljeno signalno povezavo.
- Če je obnovljena signalna povezava v sposobnem snopu, pošljemo signalni točki na sosednjo stran preko vseh alternativnih povezav (iz katerih bo promet preusmerjen na obnovljeno povezavo) sporočilo CBD (Changeback Declaration). Po sprejemu vseh potrditev CBA (Changeback Acknowledgement) postopek zaključimo.
- V primeru, ko je z obnovitvijo signalne povezave postal sposoben signalni snop, preusmerimo promet iz drugih snopov na obnovljeno signalno povezavo. V tem primeru imamo časovno kontrolirano preusmeritev – začetek prometa po obnovljeni signalni povezavi odložimo za določen čas.
- Če je snop postal na novo dostopen, pošljemo sosednjim signalnim vozliščem obvestilo.

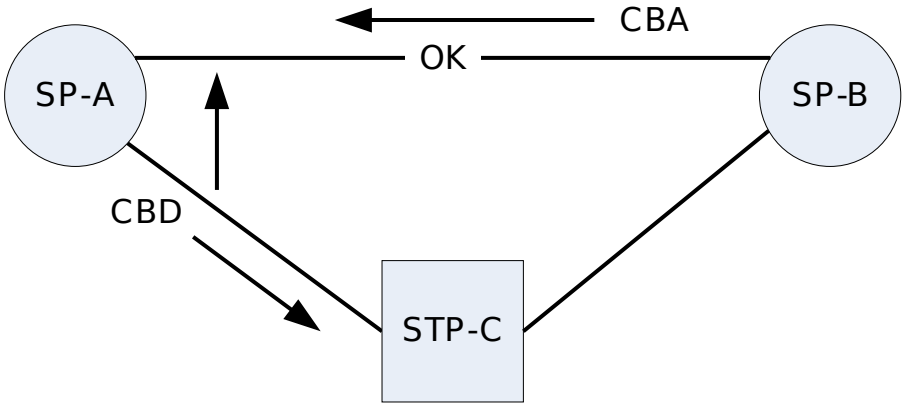
Slika 70 prikazuje primer, ko imamo v snopu dve signalni povezavi. Po obnovitvi neaktivne signalne povezave, si povezavi delita promet (loadsharing). Promet, ki gre na obnovljen signalno povezavo, začasno shranjujemo v pomnilnik. Po drugi signalni povezavi (vseskozi aktivni) pošljemo sporočilo CBD. SP-B signalna točka odgovori s sporočilom CBA. Tako je zagotovljeno, da ne prihaja do prehitevanja sporočil. Ko

SP-A signalna točka sprejme sporočilo CBD, najprej odda na obnovljeno signalno povezavo sporočila iz pomnilnika in nato promet steče normalno.



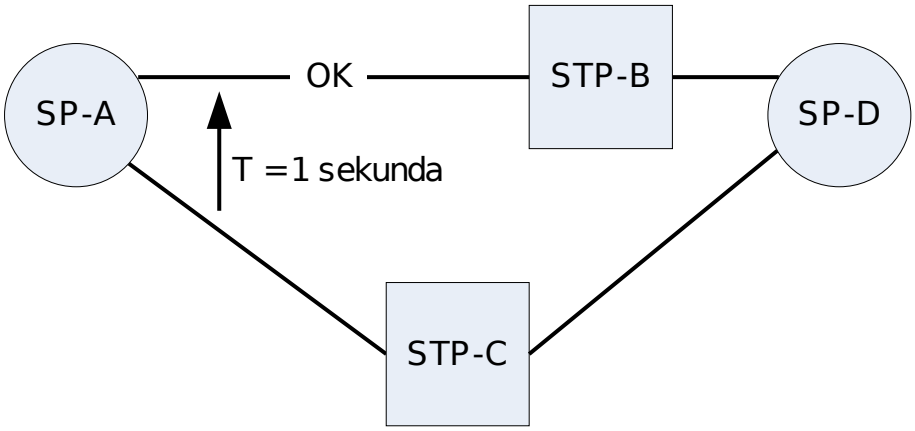
Slika 70: Vrnitev (changeback) v istem snopu

Na sliki 71 vidimo primer, ko se izvede vrnitev signalnega prometa na drug snop. Postopek je enak kot v prejšnjem primeru.



Slika 71: Vrnitev (changeback) na drug snop

Slika 72 prikazuje primer obnovitve signalne povezave do STP. V tem primeru ne moremo zagotoviti vrstnega reda sporočil. Zato uporabimo časovno kontrolirano vrnitev signalne povezave.

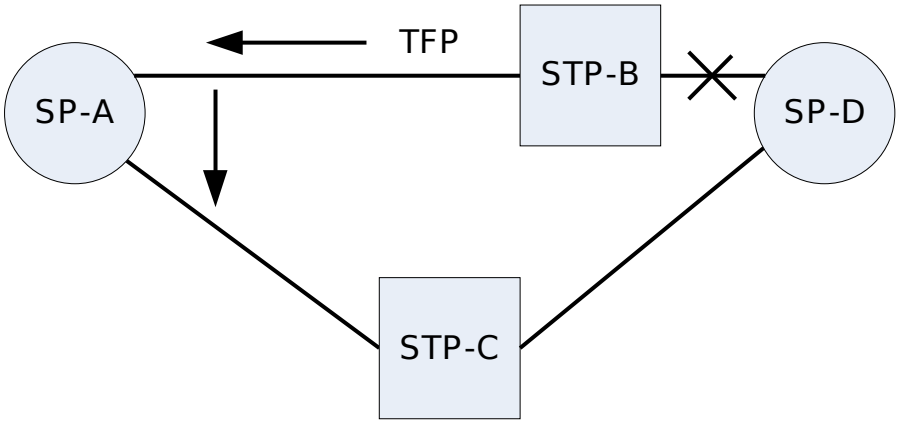


Slika 72: Časovno (changeback) kontrolirana vrnitev signalne povezave

Izpad signalne smeri

Ob izpadu signalne smeri izvršimo naslednje postopke:

- Sosednje signalno vozlišče pošlje sporočilo TFP (Transfer Prohibited) o nedostopnosti ponora. Sprožimo postopek prisiljene preusmeritve na alternativno smer (forced rerouting).
- Če ne obstaja alternativna smer, ustavimo promet proti ponoru. Uporabnikom (UP) in sosednjim STP pošljemo sporočilo TFP o prepovedi prometa.
- Med trajanjem postopka, se signalna sporočila shranjujejo v pomnilnik.
- Izpad neuporabljene signalne smeri samo zabeležimo.
- Izpadlo smer pričnemo periodično preizkušati (Route Set Test).

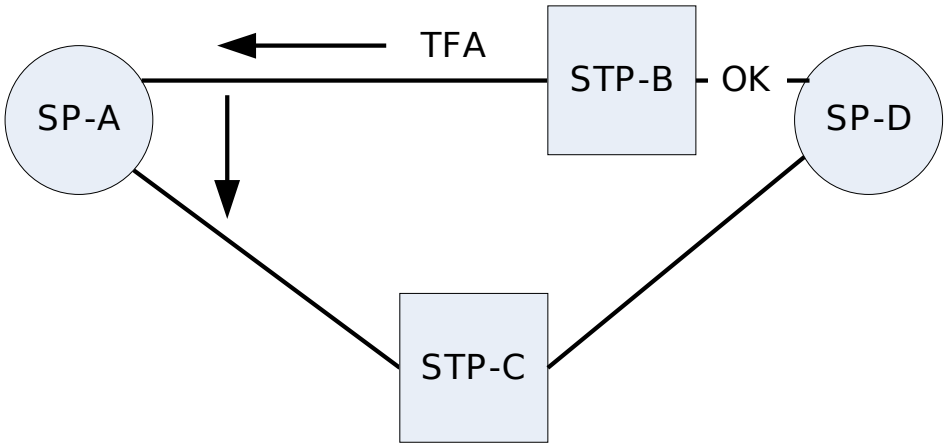


Slika 73: Prisiljena preusmeritev

Obnovitev signalne smeri

Ob vključitvi signalne smeri v promet stečejo naslednji postopki:

- Sosednje signalno vozlišče pošlje sporočilo TFA (Transfer Allowed) o ponovni dostopnosti nekega ponora. Sprožimo postopek kontrolirane preusmeritve (controlled rerouting).
- Če obnovljena signalna smer ni v uporabi, se obnovitev samo zabeleži.
- Na obnovljeno signalno smer, ki je v uporabi, ob izteku časovne kontrole najprej oddamo sporočila iz pomnilnika. Ostali promet nato steče normalno.



Slika 74: Kontrolirana preusmeritev

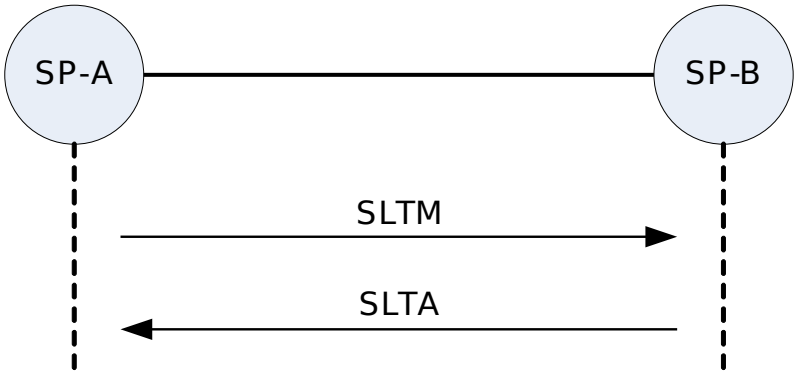
Upravljanje s signalnimi povezavami

Funkcije upravljanja signalnih povezav (SLM) uporabljamo za aktivacijo novih signalnih povezav, obnovo okvarjenih signalnih povezav in deaktivacijo že uvrščenih signalnih povezav.
Osnovni (obvezni) nabori postopkov v mednarodnem in nacionalnem omrežju so:

- aktiviranje neaktivne signalne povezave, ki še ni bila aktivna ali pa je bila vzeta iz prometa,
- obnova (restavriranje) signalne povezave, ki je bila okvarjena,
- deaktiviranje signalne povezave.

Spodnja slika 75 prikazuje testiranje signalne povezave po končanem vzpostavitvenem uvrščanju. Signalna točka A pošlje sporočilo SLTM (Signaling Link Test Message) z določenim vzorcem. Signalna točka B odgovori s sporočilom SLTA (Signaling Link Test Acknowledgement), ki vsebuje vzorec iz sporočila SLTM. S tem je zagotovljeno pravilno

delovanje tudi na tretjem nivoju in posledično je signalna povezava lahko predana prometu.



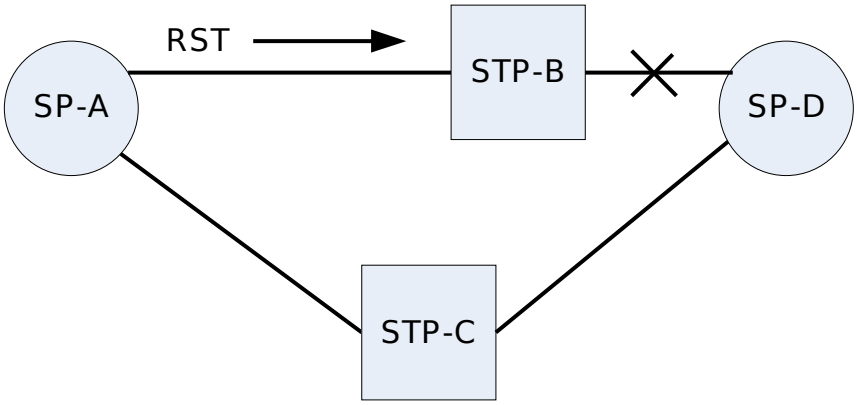
Slika 75: Testiranje signalne povezave

Upravljanje signalnih smeri

Funkcije upravljanja signalnih smeri (SRM) uporabljamo za obveščanje vozlišča o statusu signalnega omrežja z namenom, da poiščemo najboljše usmerjanje. Postopek kontroliranega prenosa izvedemo v signalni točki (STP) v primeru preobremenitve signalne povezave. Postopek prepovedanega prenosa uporabljamo za obveščanje sosednjih signalnih točk v primeru, ko signalna točka nima več sposobnih smeri do ponora. Postopek dovolitve prenosa uporabljamo za obveščanje sosednjih signalnih točk, da je usmerjanje do določenega ponora spet normalno. Postopek testiranja signalnih smeri uporabljamo v signalnih točkah, ki so dobile obvestilo o prepovedi prometa z namenom, da periodično testiramo prizadete smeri.

Testiranje signalnih smeri
Smeri, ki so nesposobne, se občasno testirajo (vsakih 30 do 60 sekund). SP-A pošlje v STP-B sporočilo RST (Routeset Test). STP-B odgovori s sporočilom TFA ali TFP. S tem zagotovimo, da so usmerjevalne tabele osvežene in s tem delovanje omrežja optimalno.

Na spodnjem primeru (Slika 76) vozlišče SP-A testira dostopnost vozlišča SP-D preko tranzitnega vozlišča STP-B tako, da periodično pošilja sporočilo. Če je ponor SP-D dostopen po eni izmed signalnih povezav (razen po signalni povezavi preko SP-A), odgovori tranzitno vozlišče s sporočilom TFA (v nasprotnem primeru ni odgovora).



Slika 76: Testiranje signalne smeri

4.3.2.M3UA

M3UA je prilagodilni sloj oz. protokol, ki omogoča transport SS7 MTP3-uporabniških sporočil (ISUP in SCCP) preko IP protokola. Priporočeno je, da M3UA uporablja storitve SCTP protokola, ki predstavlja zanesljiv nižje ležeči signalni transportni protokol. Na ta način lahko izkorišča naslednje lastnosti SCTP protokola:

- eksplicitno paketno orientiranost,
- sekvenčna dostava uporabniških sporočil znotraj več tokov z omogočenim sortiranjem individualnih uporabniških sporočil,
- opcijsko multipleksiranje uporabniških sporočil v SCTP datagrame,
- odpornost na poplavljanje in navidezne napade.

M3UA je specificiran je za elemente protokola, ki zagotavljajo normalno delovanje v SS7 in IP domeni. Protokol se uporablja med signalnim prehodom SG in MGC ali lokalno IP podatkovno bazo. Predpostavlja se, da signalni prehod SG sprejema SS7 signalna sporočila preko standardnega SS7 vmesnika z uporabo sporočilno-prenosnega dela MTP.

Protokol M3UA protokolom višjih – uporabniških slojev (ISUP, SCCP) zagotavlja transparentne storitve IP omrežnega sloja. V aplikacijskem storitvenem procesu (ASP) to zagotovi s prenosom primitivov na vmesniku med MTP3 (na SG stani) in uporabniškim slojem MTP3 (ISUP in/ali SCCP na AS strani). Ker M3UA nudi enakovreden nabor primitivov, kot jih sicer podpira vmesnik do MTP3, se uporabniški sloj (ISUP ali SCCP na AS strani) ne zaveda, da se funkcije omrežnih slojev

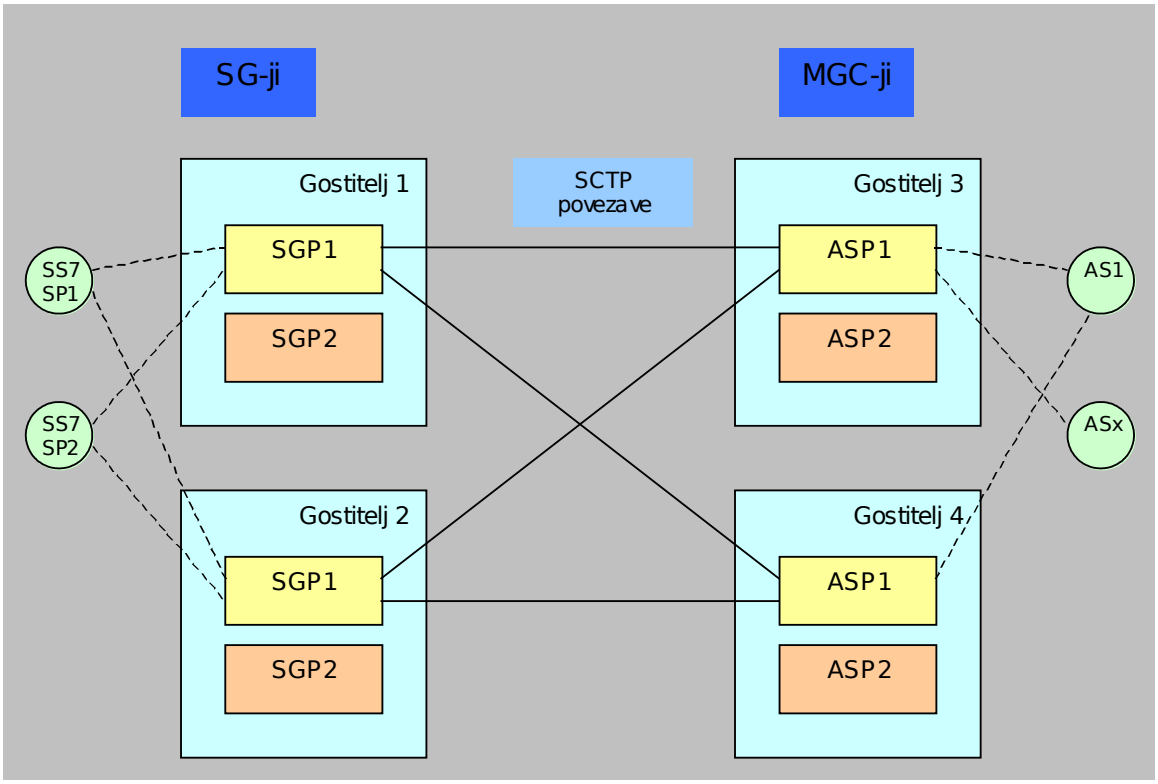
SS7 ne vršijo lokalno (na SS7 SEP strani), temveč v signalnem prehodu. Tako uporabniki niso lokalni temveč oddaljeni uporabniki, ki se nahajajo na različnih gostiteljih.

4.3.2.1.Redundančna arhitektura M3UA

Slika 77 prikazuje primer redundančne arhitekture povezovanja preko prilagodilnega sloja M3UA. Primer obsega vse možnosti redundančnih povezav, signalnih prehodov, aplikacijskih strežnikov ter njunih procesov. Na sliki je prikazano podvajanje, ki je v realizaciji tudi največkrat uporabljena možnost. M3UA sloj podpira tudi večje število redundančnih elementov. V praktičnih izvedbah se uporabi le tiste redundančne možnosti, ki so za določeno storitev primerne in prispevajo k večji zanesljivosti in odzivnosti sistema.

Redundančne možnosti:

- Signalni promet, ki je namenjen AS-u, se servisira na več fizično ločenih gostiteljih.
- Proces ASP usmerja na višji uporabniški sloj signalni promet, ki je namenjen več različnim AS-om.
- Proces SGP usmerja na SCTP povezavo prek omrežja IP signalni promet, ki je namenjen več različnim AS-om.
- ASP ima M3UA in SCTP povezavo z več SGP-ji, ki se nahajajo na fizično ločenih gostiteljih.

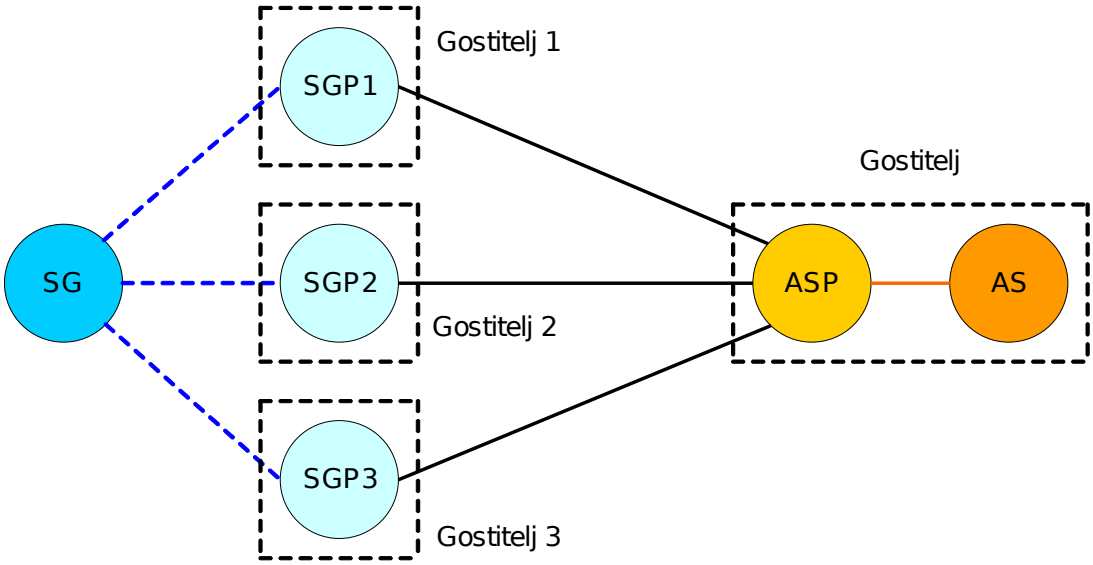


Slika 77: Redundančna arhitektura M3UA

Navadno sta glede na sliko 77 gostitelj 1 in gostitelj 2 dva signalna prehoda in dve STP točki v omrežju SS7. Aplikacijski strežnik vsebuje vse procese ASP, ki so konfigurirani za procesiranje nabora MTP3 uporabniškega prometa, definiranega z usmerjevalnim ključem. V M3UA standardu (RFC3332) je ASP zelo širok pojem, saj je sinonim za povezovanje več različnih AS-ov z več različnimi povezavami na SG-je.

Redundanca signalnega prehoda

ASP lahko usmerja signalna sporočila v omrežje SS7 preko več SGP-jev. Na lokalni ravni se vsak proces SGP izvaja na svojem gostitelju (centrali). Vsak proces je povezan z SCTP povezavo do ASP-ja, ki se lokalno izvaja na svojem gostitelju. Navadno je ena povezava (ASP – SGPx) aktivna in sposobna prenašanja uporabniških sporočil. Ostali dve povezavi sta neaktivni ali pa celo nesposobni. V primeru izpade prve povezave, zahtevamo vzpostavitev ali aktivacijo ene izmed ostalih dveh povezav.

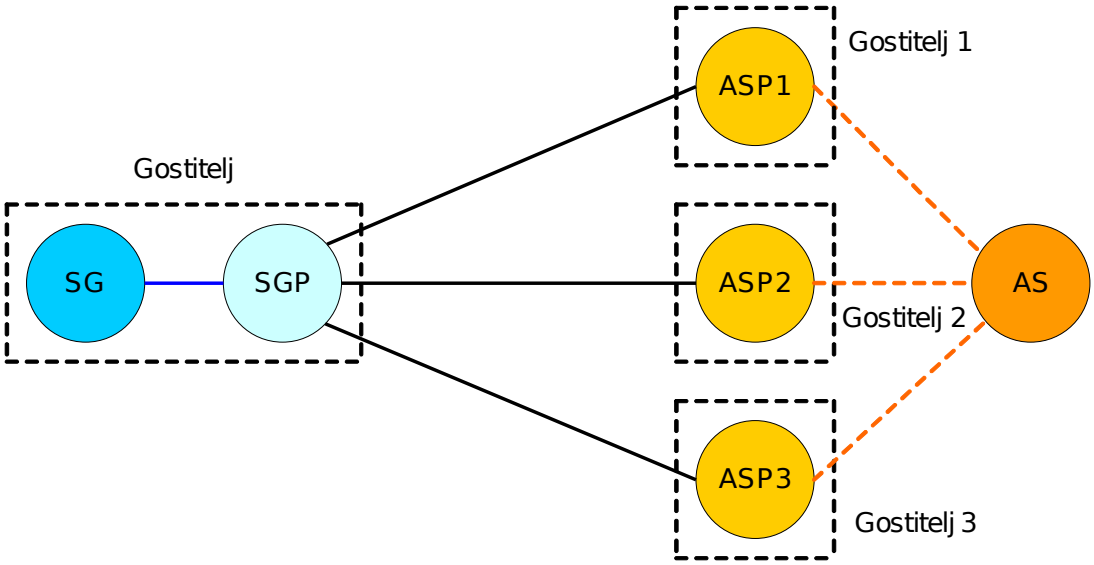


Slika 78: Redundanca signalnega prehoda

Mogoča je realizacija prioritetnega (osnovni/rezervni) redundančnega modela, kjer se nezmožnost SCTP povezljivosti odraža kot preusmeritev prometa na alternativni SGP. Model z delitvijo prometa pa omogoča deljenje aktivnih prometnih kapacitet na več procesov signalnega prehoda SGP.

Redundanca aplikacijskega strežnika

Podobno kot SG je tudi AS lahko sestavljen iz enega ali več procesov ASP, ki so distribuirani na več gostiteljih. SGP nadzira stanja ASP-jev, v katerih se prav tako lahko uporabljata prioritetni model in model z delitvijo prometa.



Slika 79: Redundanca aplikacijskega strežnika

Za aktiviranje SGP-ja vedno poskrbi ASP, SG lahko AS obvesti le o pomanjkanju aktivnih ASP-jev za določen signalni promet (Notify – InsufficientResources sporočilo).

4.3.2.2.Načini za prenos prometa

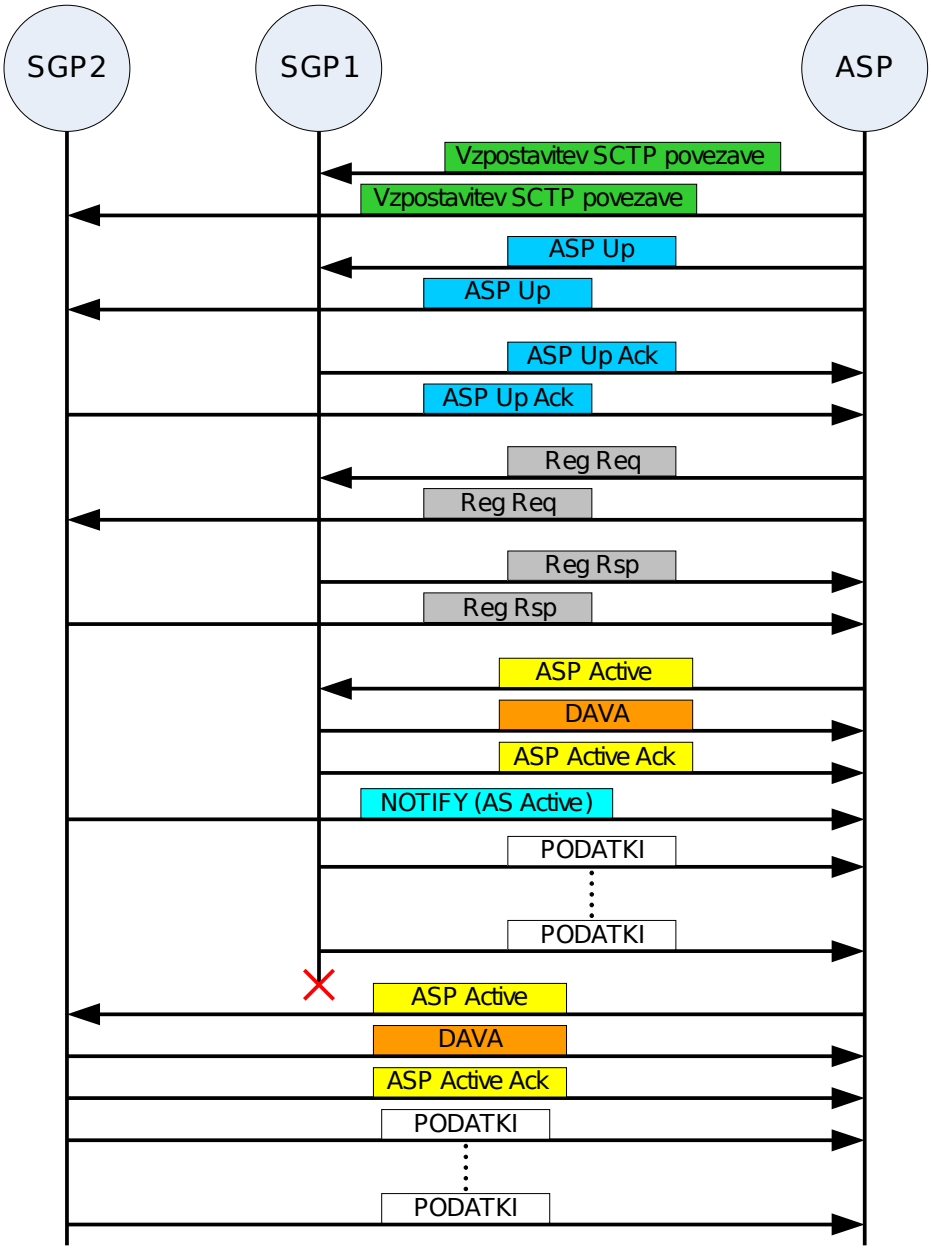
Prometni način (ang. Traffic Mode) določa, na kakšen način naj se signalni promet v posamezni signalni točki usmerja. Neposredno sta s tem povezana izraba kapacitet gostiteljev ter način aktiviranja M3UA povezav (ASP-SGP). Na relaciji AS-SG je prometni način ločen za vsako smer posebej in je lahko tudi različen.

Prometni način je lahko prevzem (ang. override), delitev prometa (ang. loadshare) in razpršena oddaja (ang. broadcast). Za prenos signalizacije broadcast večinoma ni primeren, zato zanj ne bom podajal obširnejšega opisa .

Prevzem prometa (override)

V smeri SG->AS je lahko v načinu prevzema prometa hkrati aktiven le en sam strežnik-gostitelj (AS), ki tudi obdela ves signalni promet. Ostali strežniki so v pripravljenosti (backup), da prevzamejo aktivno vlogo v primeru, ko se primarni strežnik deaktivira. So že registrirani in se aktivirajo, ko jim SG pošlje ustrezno obvestilo NOTIFY(Insuficient resources), NOTIFY(Pending) ali NOTIFY(Inactive).

V smeri AS->SG je lahko v načinu prevzema prometa aktivna samo povezava do enega SG-ja. Ostale povezave se registrirajo in čakajo v pripravljenosti. V primeru, da se aktivna povezava prekine, AS določi naslednji razpoložljivi SG ter sproži ustrezno aktiviranje. Na sliki 80 imamo prikazano opisano delovanje. Po prekinitvi primarne povezave med signalnim prehodom in aplikacijskim strežnikom, prevzame promet rezervna povezava.



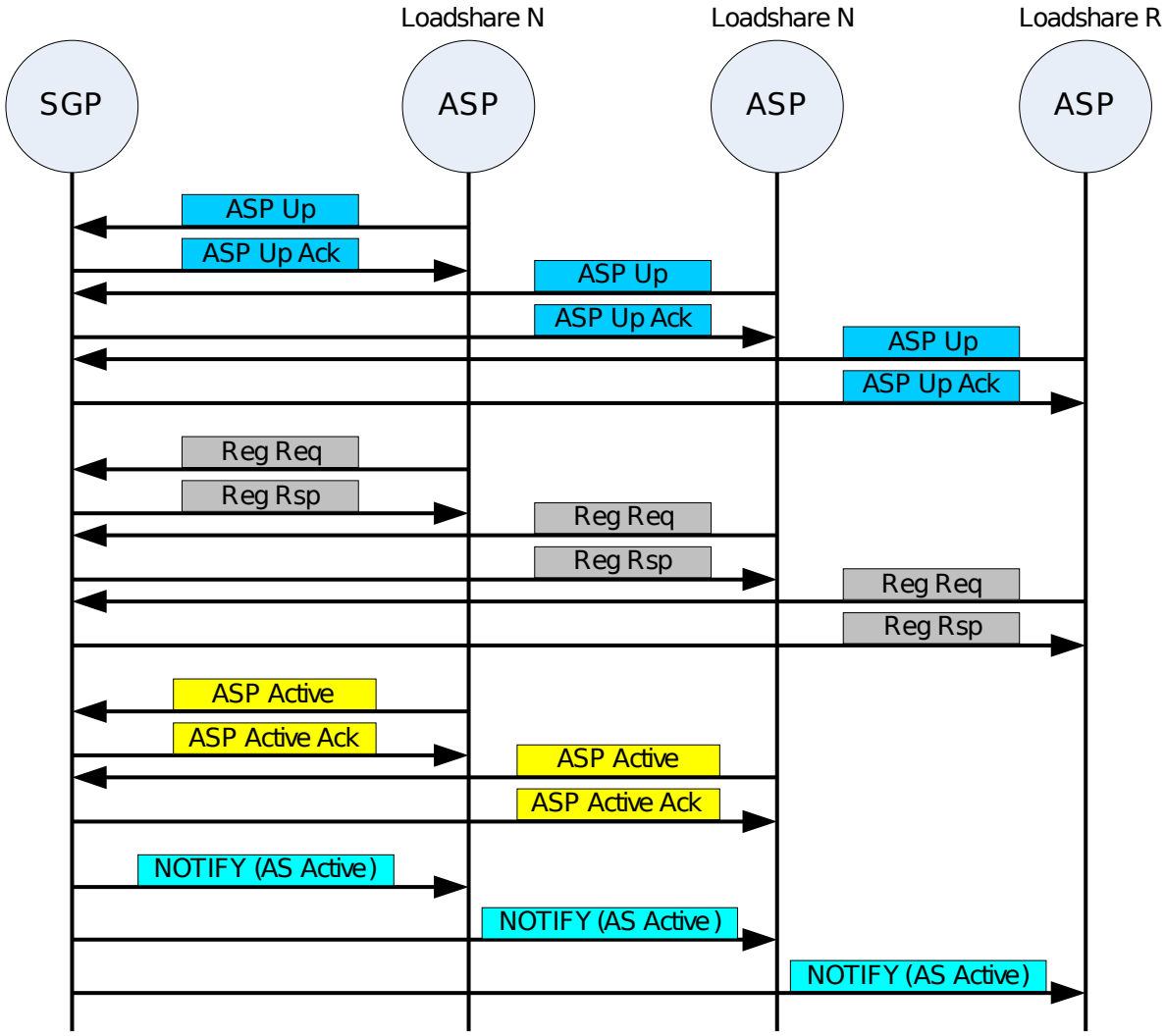
Slika 80: Prikaz izmenjave sporočil pri vzpostavitvi primarne in rezervne M3UA povezave

Delitev prometa (loadshare)

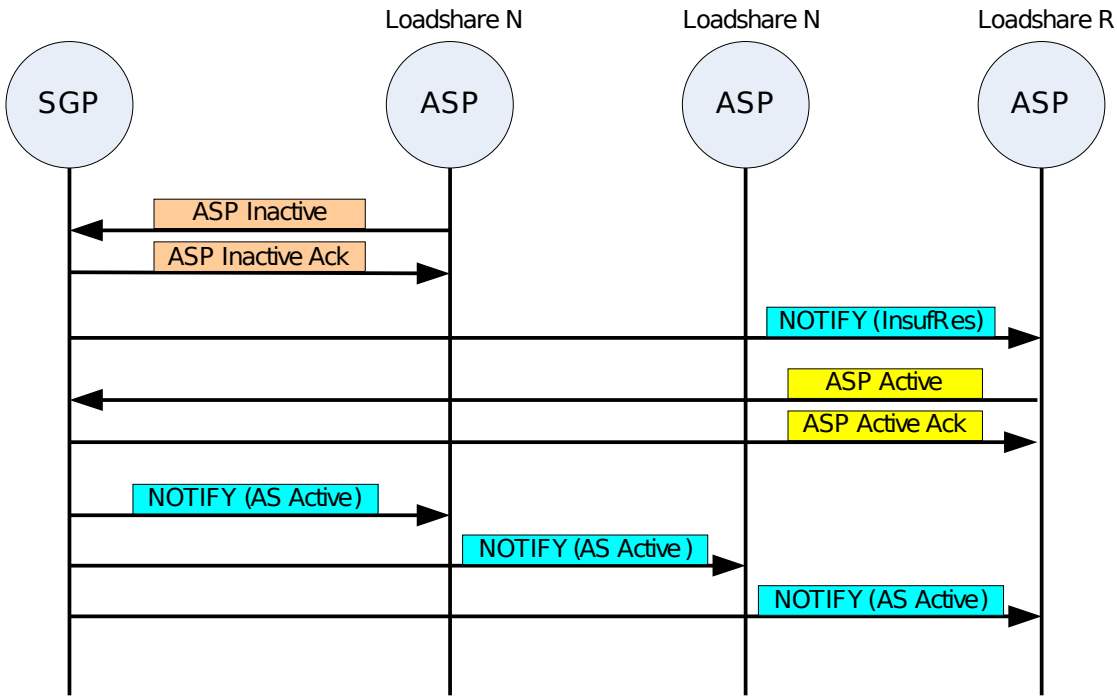
V MTP se delitev prometa izvaja med smermi in nato še med signalnimi povezavami v snopu. Podobna funkcionalnost je tudi na M3UA sloju, kjer so smeri v omrežju SS7 ekvivalentne aktivnim povezavam med SGP-ji in ASP-ji. Merilo za deljenje prometa je vrednost SLS polja v sporočilu SS7. Nadalje se promet razdeli po sporočilnih tokovih, pri katerih sicer razdeljevanje prometa nima redundančnih lastnosti, omogoča pa zmanjšanje števila krajših prekinitev dostave na posameznem sporočilnem toku.

V načinu delitve prometa se promet deli na N aktivnih SGP-jev ali ASP-jev, K registriranih pa čaka v pripravljenosti za morebitno prevzemanje prometa. Govorimo o N+K redundančnem modelu. Ko ima SGP manj kot N aktivnih povezav do ASP-ja, mu to sporoči s sporočilom NOTIFY(Insuficient resources). ASP pri pomanjkanju aktivnih povezav sam sproži ustrezno aktiviranje.

Na sliki 81 je prikazan primer postopka vzpostavljanja modela 2+1, ko imamo dva ASP procesa, ki si v normalni situaciji delita promet, en rezervni ASP pa čaka v pripravljenosti. Slika 82 prikazuje potek preklopa in aktiviranja rezervnega ASP-ja.



Slika 81: Prikaz izmenjave sporočil pri vzpostavitvi modela 2+1



Slika 82: Prikaz izmenjave sporočil pri preklopu in aktiviranju rezervnega ASP-ja

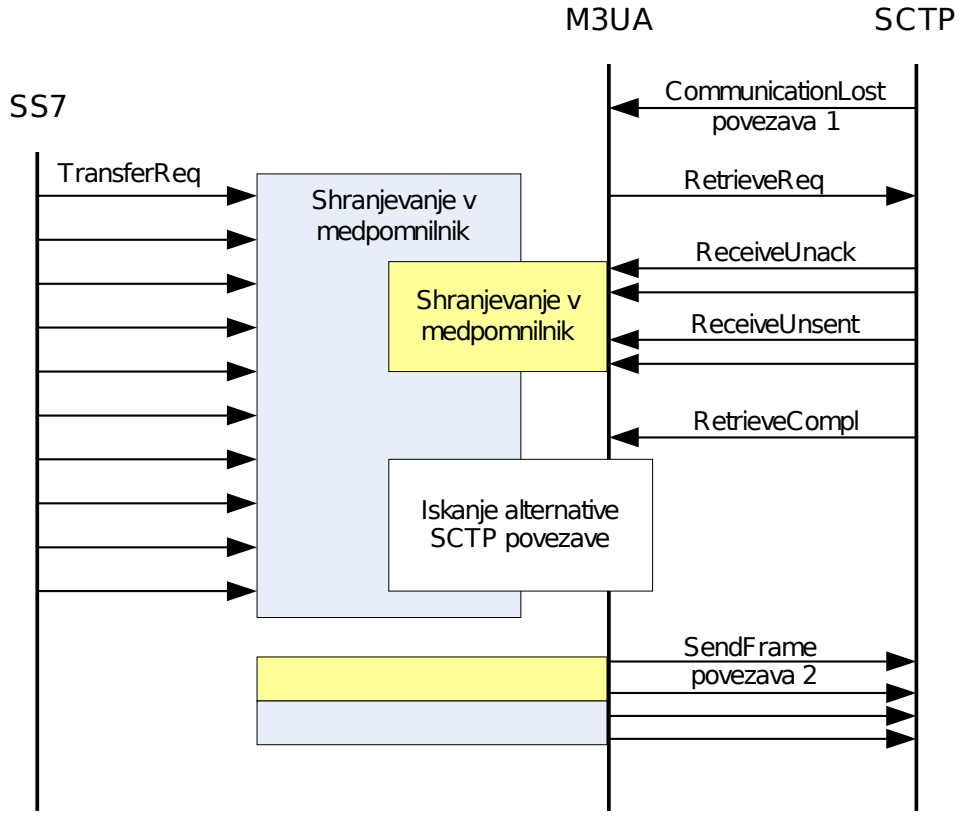
Razpršena oddaja (broadcast)

V načinu razpršene oddaje so hkrati aktivni vsi razpoložljivi procesi aplikacijskega strežnika. Vsi ASP-ji prejmejo ves signalni promet ter tako obdelajo identična signalna sporočila. Enako velja tudi v smeri AS->SG.

4.3.2.3.Preklop (failover)

V primeru, ko postaneta ASP ali SGP nedostopna, M3UA uporabnika SS7 o napaki ne obvesti takoj, temveč poizkuša preusmeriti promet na drugi ASP, oziroma drugi SGP. Slika 83 prikazuje celoten postopek prenosa iz povezave 1 na povezavo 2. Ves čas moramo ohranjati vrstni red oddanih sporočil za posamezno selekcijo signalne povezave (SLS – Signaling Link Selection). Medtem, čakamo na preklop, se sporočila, ki prihajajo iz uporabniškega nivoja, shranjujejo v začasni pomnilnik. Ko se iz sloja SCTP uspešno preberejo vsa nepotrjena in neposlana sporočila, se poišče nov aktiven ASP, oziroma SGP za isti AS, oziroma SG. Če se le ta najde, se vsa shranjena sporočila takoj pošljejo po novi poti. Če alternativne poti ni, SG ali AS vstopi v stanje PENDING, ter čaka neko časovno obdobje (3 sekunde), da se aktivira nov ASP oziroma

SGP. Ko časovnik za stanje PENDING poteče, se obvesti uporabniški nivo o nedostopnosti končne točke. Če se povezava obnovi, ali se izvede preklop na alternativno smer (proces), uporabnik sploh ne občuti izpada.

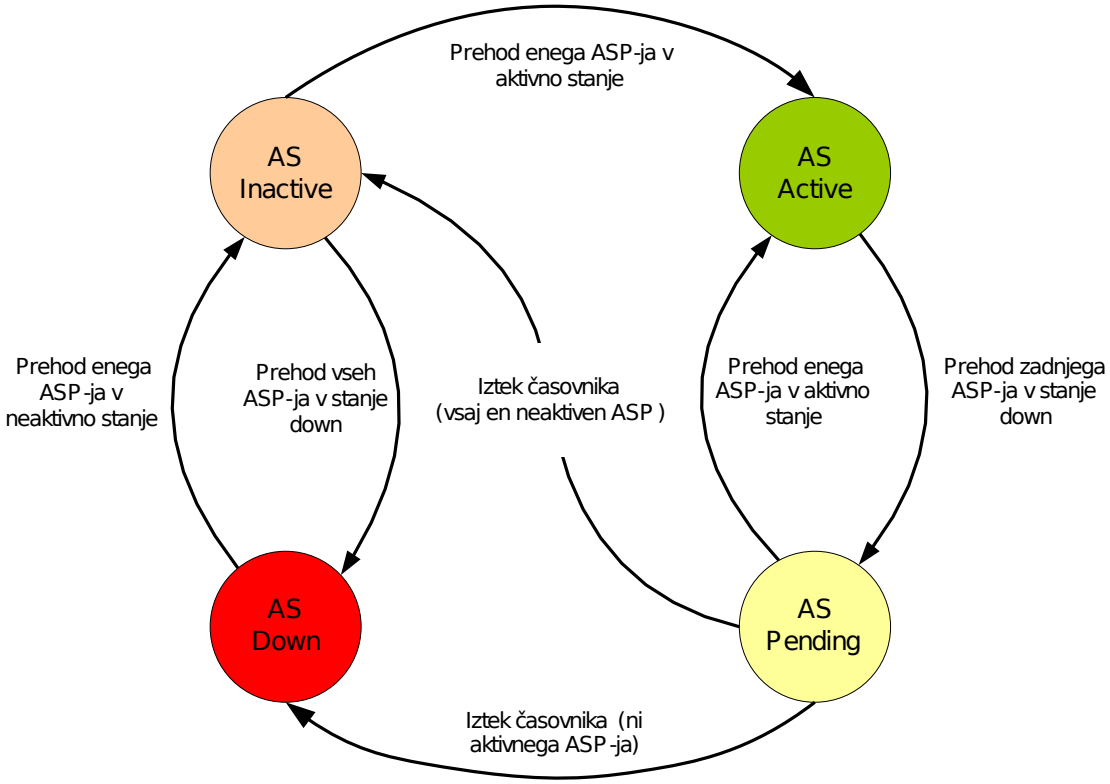


Slika 83: Prikaz izmenjave sporočil in shranjevanja podatkov pri preklopu

Stanje AS procesa - Pending

AS preide v začasno stanje *pending*, ko na gostitelju zadnji aktivni ASP preide v stanje *down* ali *registered*. V tem stanju je promet na AS-u začasno ustavljen, M3UA sloj pa ne obvešča uporabniški sloj, da je prišlo do napake. V primeru, da arhitektura omrežja omogoča redundantne povezave, ki čakajo v stanju pripravljenosti za aktiviranje, oziroma je protokol M3UA sposoben v zelo kratkem času ponovno vzpostaviti ravnokar prekinjeno povezavo, lahko preidemo nazaj v aktivno stanje. Časovno obdobje (pending), v katerem je lahko AS in poskuša vzpostaviti alternativno povezavo, je omejeno (približno 3 s). Uporabniški sloj kratkega izpada ne občuti, saj se vsa signalna sporočila shranjujejo in ponovno pošljejo po alternativni povezavi. V

drugem primeru, ko nimamo na razpolago alternativne povezave, AS preide v stanje *down*, ter obvesti uporabniški sloj o napaki.



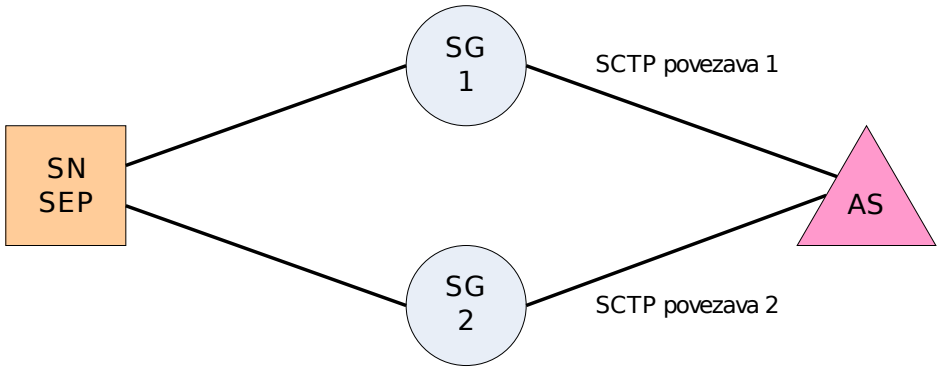
Slika 84: Stanje AS procesa – Pending

4.3.2.4.Redundančni arhitekture M3UA

V naslednjem poglavju so predstavljeni možni redundančni modeli in arhitekture. Arhitekture se med seboj razlikujejo po številu signalnih prehodov, številu aplikacijskih strežnikov, ter v prometnem načinu, ki je uporabljen na posamezni smeri. Drugačne so tudi redundančne možnosti pri preklopih in preusmeritvah. Več kot je v arhitekturnem modelu redundančnih možnosti, bolj je lahko celoten sistem zanesljiv. Pri načrtovanju sistema je potrebno najprej določiti, katere redundančne možnosti so glede na določeno storitev sploh tehnično možne in pomembno dvigujejo raven zanesljivosti.

Običajno se iz SG-ja proti AS-u uporablja enak način usmerjanja, ni pa nujno. V nadaljevanju so prikazane posamezne konfiguracije, kjer so na slikah z rdečo prikazani aktivni elementi, z modro pa neaktivni, ki v normalni situaciji, čakajo v pripravljenosti.

Arhitekturni model: 2 signalna prehoda, 1 aplikacijski strežnik



Slika 85: Arhitekturni model 2-SG, 1-AS

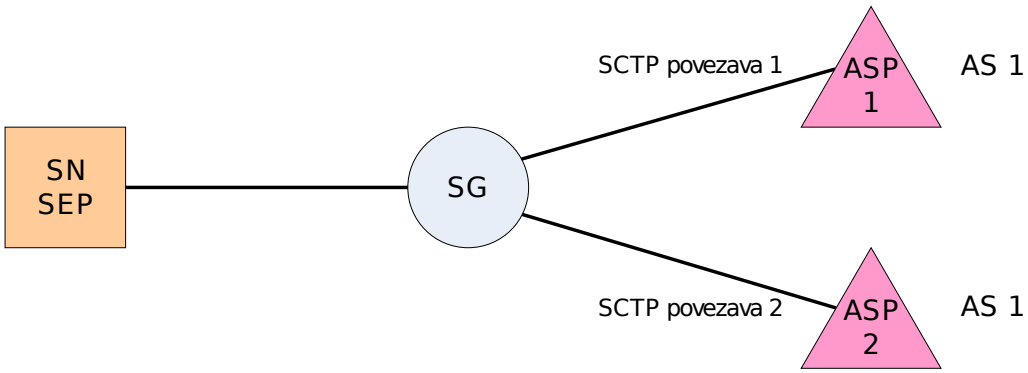
Zgornja arhitektura omogoča dva načina delovanja iz AS proti SG:

- z delitvijo prometa (loadshare) preko SG1 in SG2,
- prioritetno (priority) – z uporabo osnovne in alternativne smeri.

V prvem primeru sta oba procesa v signalnih prehodih ter v aplikacijskih strežnikih v aktivnem stanju in lahko prenašata uporabniški promet. Izvaja se delitev prometa (na osnovi SLS polja) kar omogoča polno izrabo omenjene arhitekture. Ob izpadu določene povezave, prevzame druga povezave celoten promet.

V drugem primeru je v aktivnem stanju samo en proces v signalnem prehodu in aplikacijskem strežniku. Drugi proces je v stanju registracije in v pripravljenosti. V primeru izpade aktivne povezave, pride do aktivacije drugega procesa, ki prevzame promet.

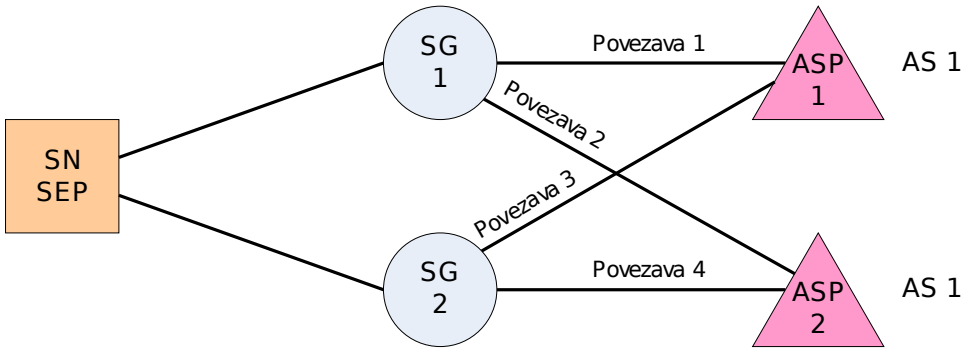
Arhitekturni model: 1 signalni prehod, 2 aplikacijska strežnika



Slika 86: Arhitekturni model SG, 2-AS

V zgornji arhitekturi je navadno en proces ASP na aplikacijskem strežniku aktiven, drugi pa v pripravljenosti. V primeru izpade aktivne povezave, signalni prehod obvesti (NOTIFY sporočilo) drugi neaktiven proces, ki aktivira povezavo in prevzame promet. Omenjena arhitektura se predvsem uporablja za preklop procesorja na AS-u.

Arhitekturni model: 2 signalna prehoda, 2 aplikacijska strežnika



Slika 87: Arhitekturni model 2-SG, 2-AS

Predstavljena arhitektura omogoča več načinov delovanja:

a) *Z uporabo osnovne in alternativne smeri med SG1 in SG2 ter prioritetno med ASP1 in ASP2*. Ob vzpostavitvi posameznih povezav je v aktivnem stanju samo povezava 1. Ob izpadu povezave 1, se najprej aktivira povezava 3. V primeru izpada aplikacijskega strežnika 1 (ASP1), prevzame promet ASP2, kjer velja enak postopek aktiviranja (najprej povezava 2).

b) *Z delitvijo prometa med SG1 in SG2 ter prioritetno med ASP1 in ASP2*. Ob vzpostavitvi sistema sta v aktivnem stanju povezava 1 in povezava 3. Aplikacijski strežnik 1 izvaja delitev prometa med obema povezavama. V primeru izpada aplikacijskega strežnika 1 (ASP1), prevzame promet ASP2, ki ravno tako izvaja delitev prometa med povezavama 2 in 4.

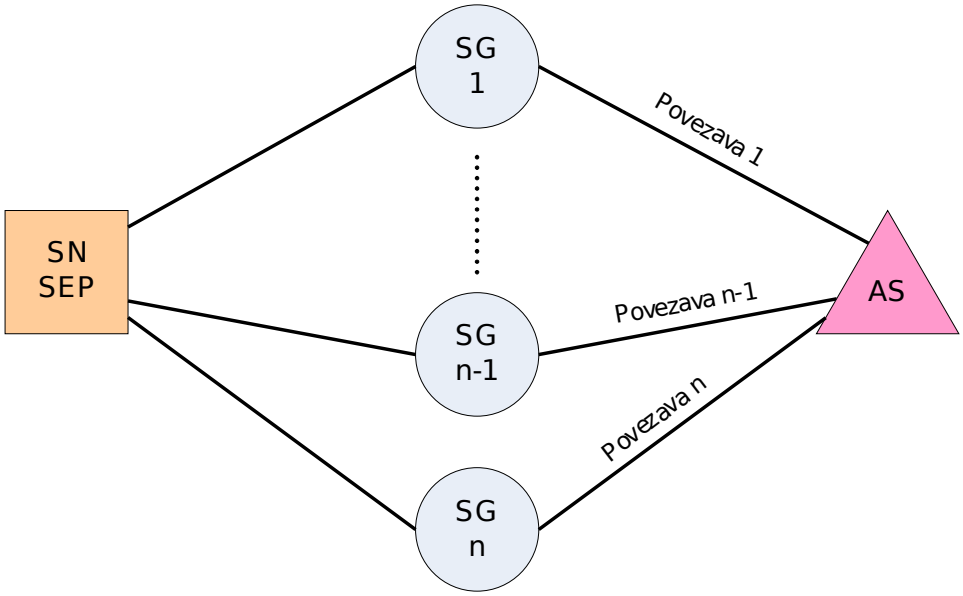
c) *z uporabo osnovne in alternativne smeri med SG1 in SG2 ter delitvijo prometa med ASP1 in ASP2*. Ob vzpostavitvi sistema sta v aktivnem stanju povezava 1 in povezava 2. Signalni prehod 1 (SG 1) izvaja delitev prometa med povezavama. V primeru izpada SG 1 se aktivirata povezavi 3 in 4.

d) z delitvijo prometa med SG1 in SG2 ter ASP1 in ASP2. V tem primeru so vse povezave aktivne in se v obeh smereh izvaja delitev prometa.

	Aktivnost povezave med normalnim delovanjem			
Arhitektura	Povezava 1	Povezava 2	Povezava 3	Povezava 4
a	aktivna	pasivna	pasivna	pasivna
b	aktivna	pasivna	aktivna	pasivna
c	aktivna	aktivna	pasivna	pasivna
d	aktivna	aktivna	aktivna	aktivna

Tabela 6: Aktivnost povezav v posameznih arhitekturah M3UA

Arhitekturni model: več signalnih prehodov, 1 aplikacijski strežnik

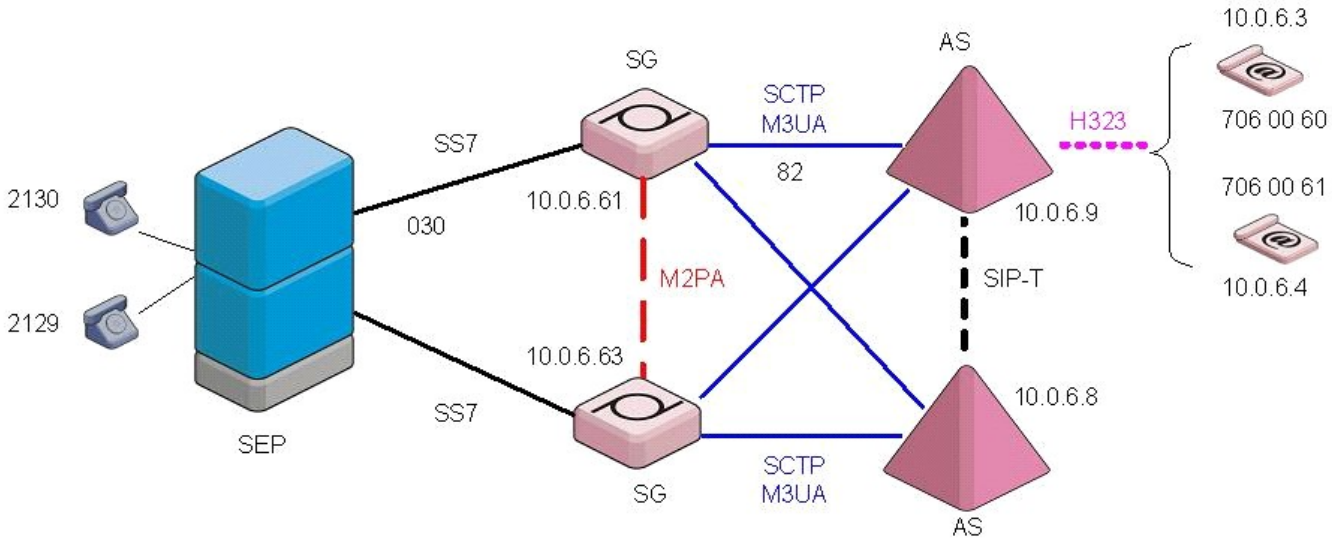


Slika 88: Arhitekturni model n x SG, 1 aplikacijski strežnik

Slika 88 prikazuje redundančni model z več signalnimi prehodi, od katerih sta navadno dva v aktivnem stanju. Aplikacijski strežnik vodi evidenco o aktivnih povezavah in v primeru izpada katere od povezav, aktivira naslednjo povezavo z najvišjo prioriteto.

5. PRAKTIČNO DELO IN REZULTATI TESTIRANJ

V Laboratoriju za telekomunikacije imamo postavljeno testno okolje, ki omogoča razvoj SIGTRAN protokolov. Do sedaj so bili uspešno implementirani in realizirani protokoli SCTP, M3UA in M2PA. Razvoj poteka tudi na protokolu M2UA, ki ima prednost v tem, da signalni prehod zaključen z M2UA ne potrebuje kode vozlišča (Point Code). Opisane modele in arhitekture sem lahko tako tudi praktično testiral. Rezultati testov so predstavljeni v nadaljevanju.



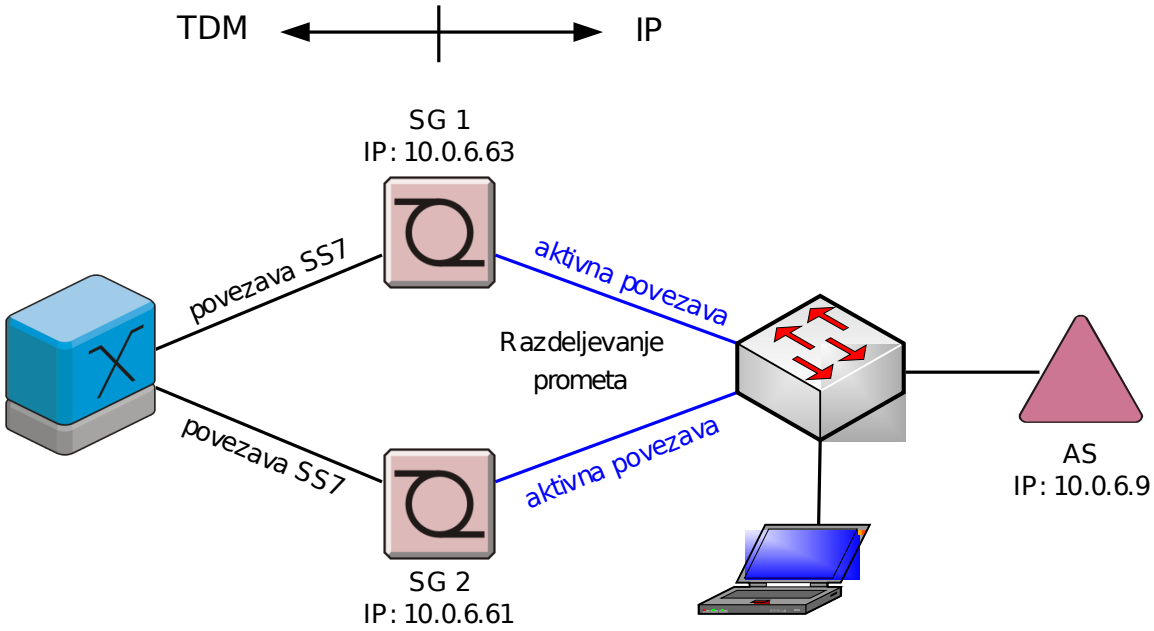
Slika 89: Testno okolje v Laboratoriju za telekomunikacije

Na zgornji sliki je predstavljeno testno omrežje IP telefonije v Laboratoriju za telekomunikacije. TDM centrala (SEP) je povezana z dvema SS7 signalnima povezavama s signalnima prehodoma, ki se naprej po omrežju IP povezujeta z dvema aplikacijskima strežnikoma.

5.1. REDUNDANČNA ARHITEKTURA 2SG-1AS (RAZDELJEVANJE PROMETA)

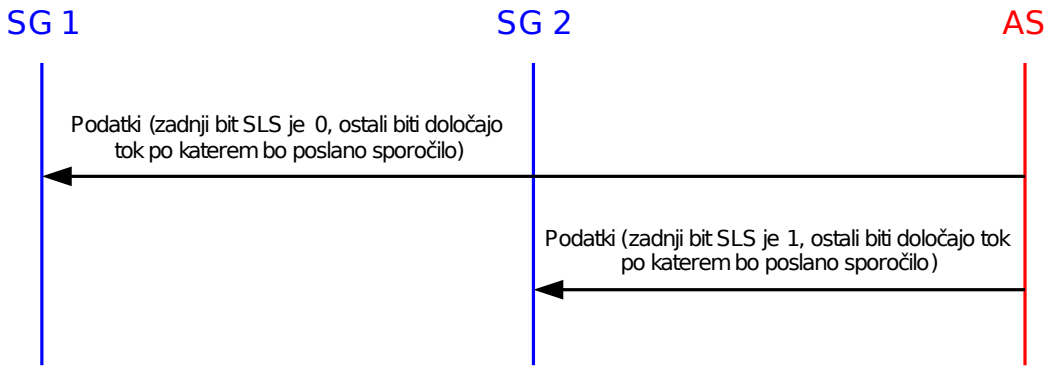
Spodnja arhitektura prikazuje primer razdeljevanja prometa med dvema signalnima prehodoma. Povezavi sta v aktivnem stanju,

aplikacijski strežnik pa razdeljuje promet med obema prehodoma. Pomembno je, da se promet deli tako, da ohranjamo nadzor posameznih klicev preko istih procesov. To pomeni, da vsa uporabniška sporočila za posamezen klic, prejme vedno isti proces.



Slika 90: Redundančna arhitektura 2SG-1AS (Razdeljevanje prometa)

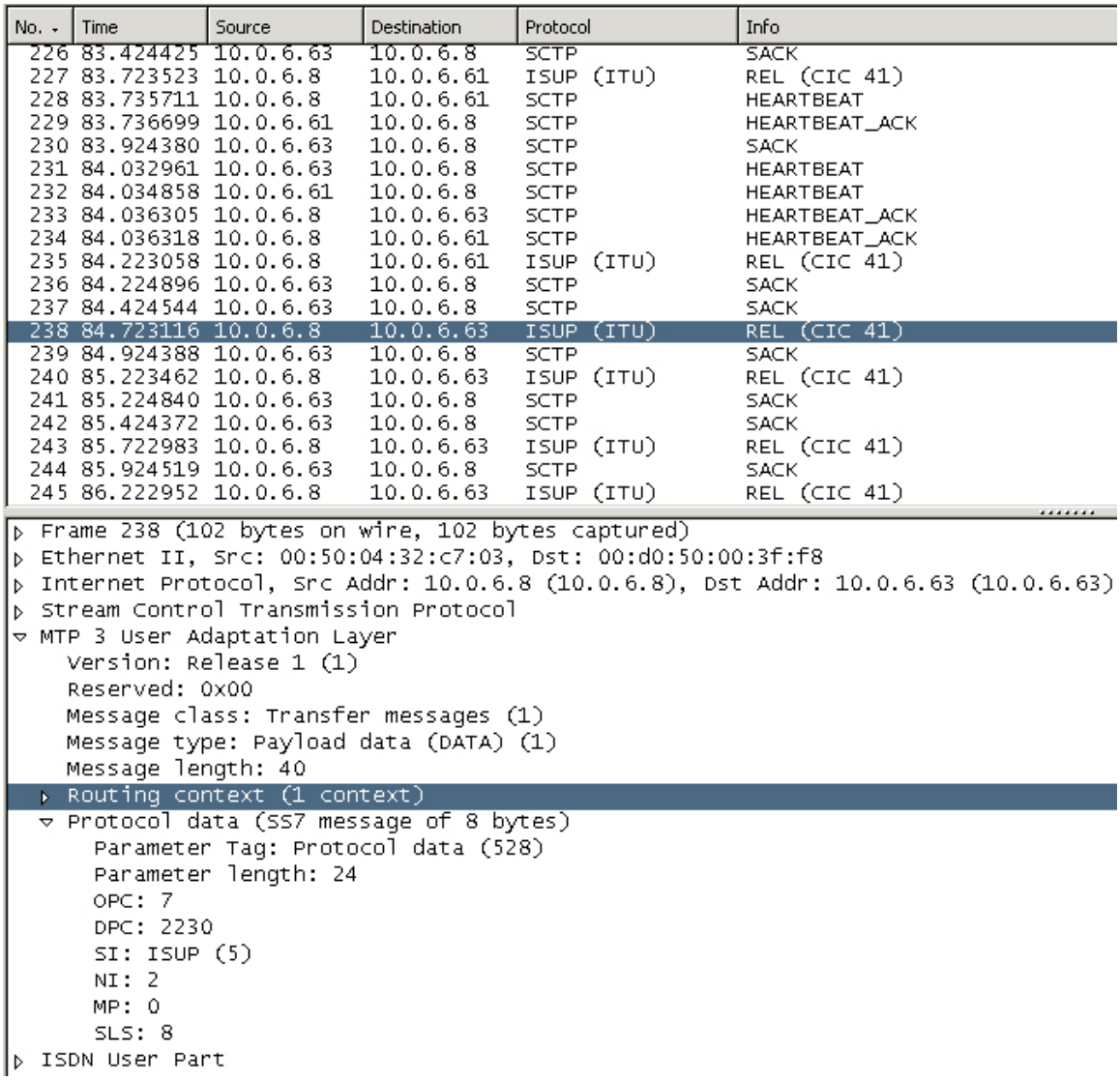
Razdeljevanje podatkov med aktivnimi procesi navadno poteka po vrednosti polja SLS (Signaling Link Selection). Najbolj pomemben bit določa po kateri povezavi se bo prenašal podatek, ostali trije biti pa določajo sporočilni tok znotraj povezave SCTP.



Slika 91: Razdeljevanje prometa po polju SLS

Za testiranje funkcionalnosti razdeljevanja prometa sem uporabil generator uporabniškega prometa. V testnih sporočilih (sporočilo

Release Complete – REL) sem povečeval polje SLS in tako dosegel razdeljevanje med aktivnima povezavama. Signalna sporočila z vrednostjo polja SLS med 0 in 7 se dodeljujejo signalnemu prehodu SG1, sporočila z vrednostjo polja SLS med 8 in 15 pa signalnemu prehodu SG2.

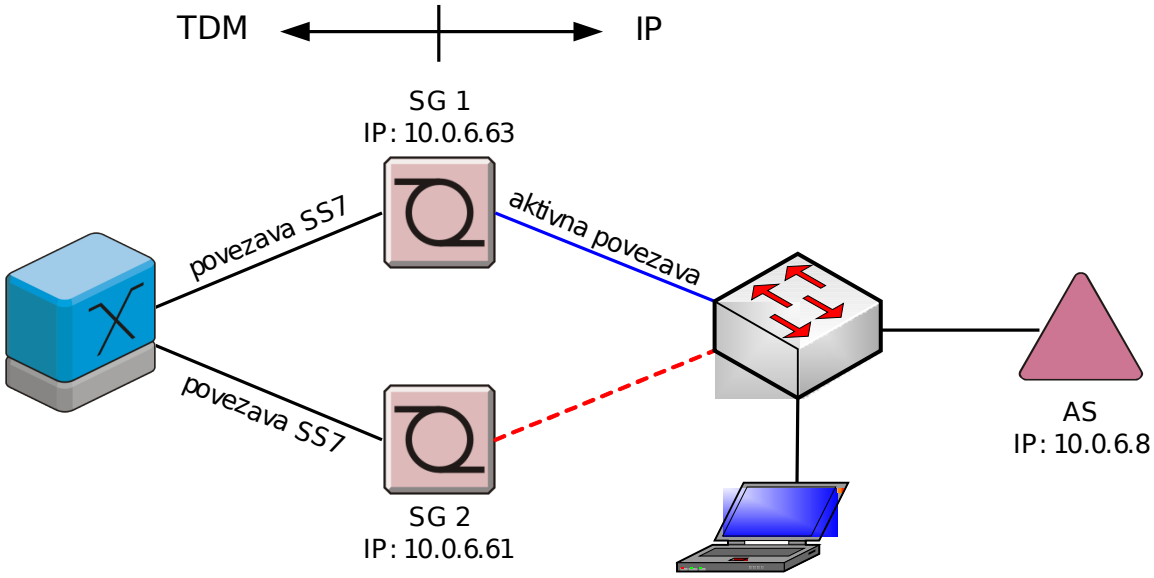


Slika 92: Redundančna arhitektura 2SG-1AS (Razdeljevanje prometa)

5.2.REDUNDANČNA ARHITEKTURA 2SG-1AS (PRIORITETNI NAČIN)

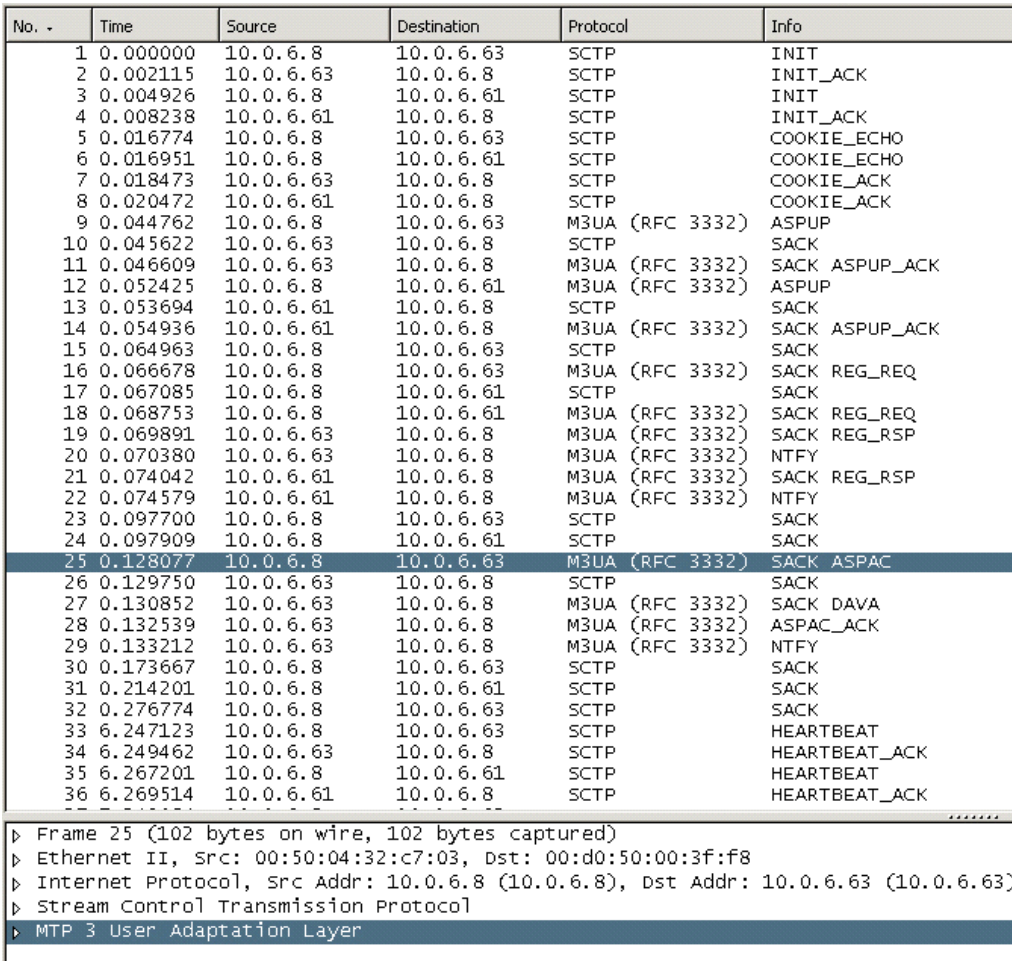
Na spodnji arhitekturi sem testiral preklop med dvema SCTP povezavama. Povezava med signalnim prehodom 1 (SG1) in aplikacijskim strežnikom (AS) je v aktivnem stanju. Druga povezava

(med SG2 in CS) je samo registrirana in v neaktivnem stanju. Stanja povezav nadzoruje AS. AS je usmerjal promet le po aktivni povezavi proti SG1. Ko sem izključil SG1, je AS zaznal prekinjeno povezavo in aktiviral registrirano povezavo proti SG2. S tem je SG2 prevzel ves promet, AS pa mu je poslal tudi prej poslani promet, katerega sprejem ni bil potrjen.

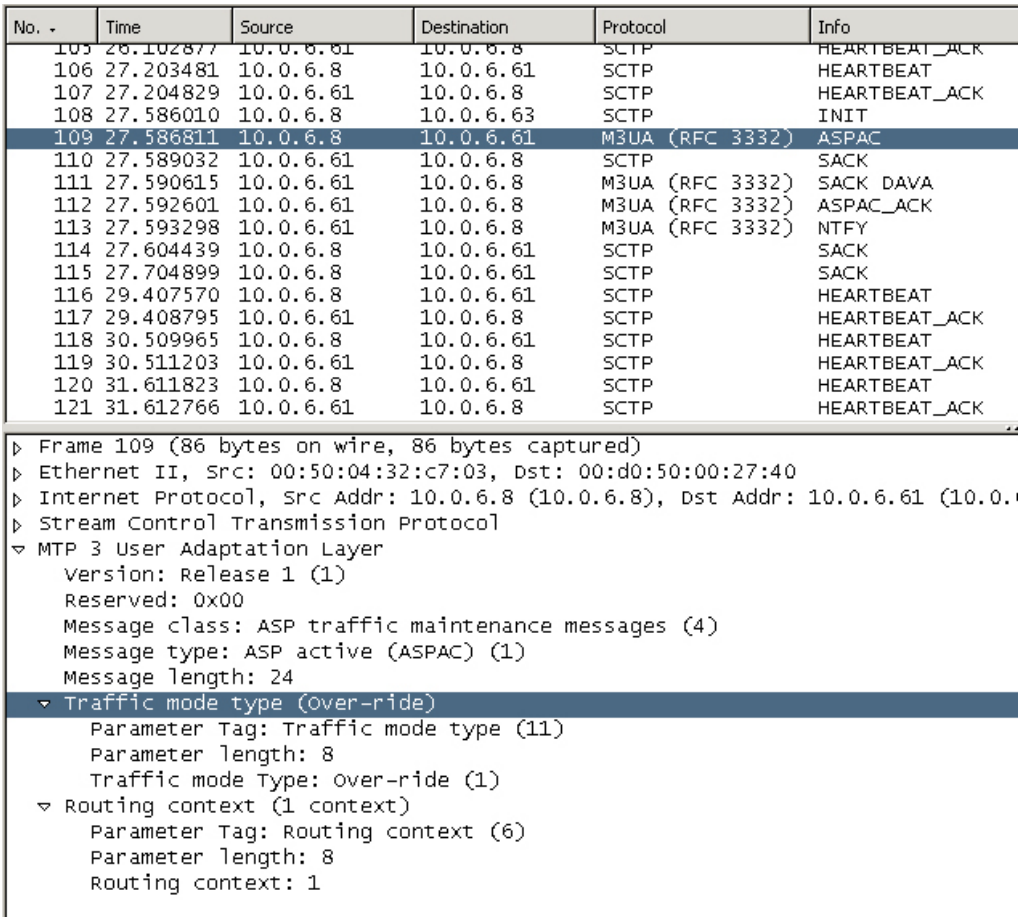


Slika 93: Redundančna arhitektura 2SG-1AS (Prioritetni način)

Promet sem zajemal s program Ethereal. Na spodnji sliki je prikazan zajem pomembnejših sporočil.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.6.8	10.0.6.63	SCTP	INIT
2	0.002115	10.0.6.63	10.0.6.8	SCTP	INIT_ACK
3	0.004926	10.0.6.8	10.0.6.61	SCTP	INIT
4	0.008238	10.0.6.61	10.0.6.8	SCTP	INIT_ACK
5	0.016774	10.0.6.8	10.0.6.63	SCTP	COOKIE_ECHO
6	0.016951	10.0.6.8	10.0.6.61	SCTP	COOKIE_ECHO
7	0.018473	10.0.6.63	10.0.6.8	SCTP	COOKIE_ACK
8	0.020472	10.0.6.61	10.0.6.8	SCTP	COOKIE_ACK
9	0.044762	10.0.6.8	10.0.6.63	M3UA (RFC 3332)	ASPUP
10	0.045622	10.0.6.63	10.0.6.8	SCTP	SACK
11	0.046609	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	SACK ASPUP_ACK
12	0.052425	10.0.6.8	10.0.6.61	M3UA (RFC 3332)	ASPUP
13	0.053694	10.0.6.61	10.0.6.8	SCTP	SACK
14	0.054936	10.0.6.61	10.0.6.8	M3UA (RFC 3332)	SACK ASPUP_ACK
15	0.064963	10.0.6.8	10.0.6.63	SCTP	SACK
16	0.066678	10.0.6.8	10.0.6.63	M3UA (RFC 3332)	SACK REG_REQ
17	0.067085	10.0.6.8	10.0.6.61	SCTP	SACK
18	0.068753	10.0.6.8	10.0.6.61	M3UA (RFC 3332)	SACK REG_REQ
19	0.069891	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	SACK REG_RSP
20	0.070380	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	NTFY
21	0.074042	10.0.6.61	10.0.6.8	M3UA (RFC 3332)	SACK REG_RSP
22	0.074579	10.0.6.61	10.0.6.8	M3UA (RFC 3332)	NTFY
23	0.097700	10.0.6.8	10.0.6.63	SCTP	SACK
24	0.097909	10.0.6.8	10.0.6.61	SCTP	SACK
25	0.128077	10.0.6.8	10.0.6.63	M3UA (RFC 3332)	SACK ASPAC
26	0.129750	10.0.6.63	10.0.6.8	SCTP	SACK
27	0.130852	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	SACK DAVA
28	0.132539	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	ASPAC_ACK
29	0.133212	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	NTFY
30	0.173667	10.0.6.8	10.0.6.63	SCTP	SACK
31	0.214201	10.0.6.8	10.0.6.61	SCTP	SACK
32	0.276774	10.0.6.8	10.0.6.63	SCTP	SACK
33	6.247123	10.0.6.8	10.0.6.63	SCTP	HEARTBEAT
34	6.249462	10.0.6.63	10.0.6.8	SCTP	HEARTBEAT_ACK
35	6.267201	10.0.6.8	10.0.6.61	SCTP	HEARTBEAT
36	6.269514	10.0.6.61	10.0.6.8	SCTP	HEARTBEAT_ACK



Slika 94: Prikaz sporočil zajetih s program Ethereal v primeru 2SG-1AS (Prioritetni način)

Razvidno je, da aplikacijski strežnik potrebuje določen čas, da zazna okvarjeno povezavo. V priporočilih za SS7 [21] je predviden največji čas preklopa za okvarjeno povezavo 500ms. V omrežju SS7 je to zagotovljeno tako, da v primeru ko ni signalnega prometa, se po signalni povezavi pošiljajo FISU sporočila. Za ugotavljanje stanja povezave v omrežju IP, pa uporablja SCTP protokol heartbeat sporočila. V odvisnosti od nastavljenih parametrov je odvisen tudi čas preklopa iz neaktivne na aktivno povezavo. Izbira parametrov ima v realnem omrežju kritičen pomen, saj je omrežje IP mnogo bolj nepredvidljivo kot omrežje SS7. V določenih situacijah lahko tako pride do nepotrebnih preklopov ali pa ob izpadu povezave do velikih zakasnitev signalnih sporočil. V spodnji tabeli je v odvisnosti od izbranih parametrov izmerjen čas preklopa po izpadu aktivne povezave.

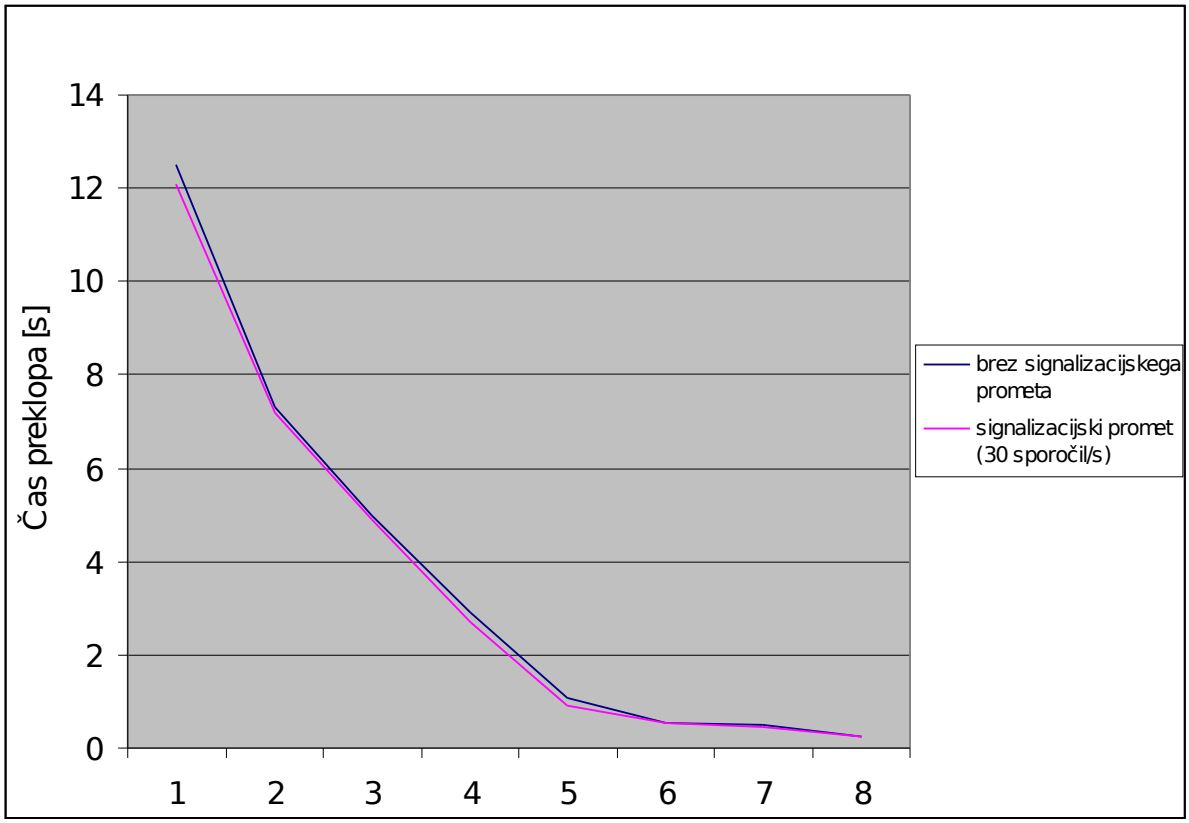
Parametri SCTP povezave			
rto_min [ms]	rto_max [ms]	max_path_retrans	Čas preklopa [s]
1000	3000	5	12,5
1000	3000	3	7,3
500	1000	5	5,0
500	1000	3	2,9
100	200	5	1,1
100	200	3	0,55
50	100	5	0,49
50	100	3	0,27

Tabela 7: Čas preklopa brez signalnega prometa

Parametri SCTP povezave			
rto_min [ms]	rto_max [ms]	max_path_retrans	Čas preklopa [s]
1000	3000	5	12,1
1000	3000	3	7,2
500	1000	5	4,9
500	1000	3	2,7
100	200	5	0,9
100	200	3	0,53
50	100	5	0,47
50	100	3	0,26

Tabela 8: Čas preklopa pri signalnem prometu (30 sporočil/sek)

Iz tabel in spodnjega grafa je razvidno, da ob ustreznem izboru parametrov lahko dosežemo preklope, ki so primerljivi s preklopi v omrežju SS7. Pri tem ne smemo pozabiti, da so omenjeni testi potekali v laboratorijskem omrežju, ki je z vidika uporabnika idealno okolje (minimalne zakasnitve, minimalne variacije zakasnitev, brez izgube paketov, "neomejena pasovna širina",...).



Slika 95: Čas preklopa po izpadu aktivne povezave

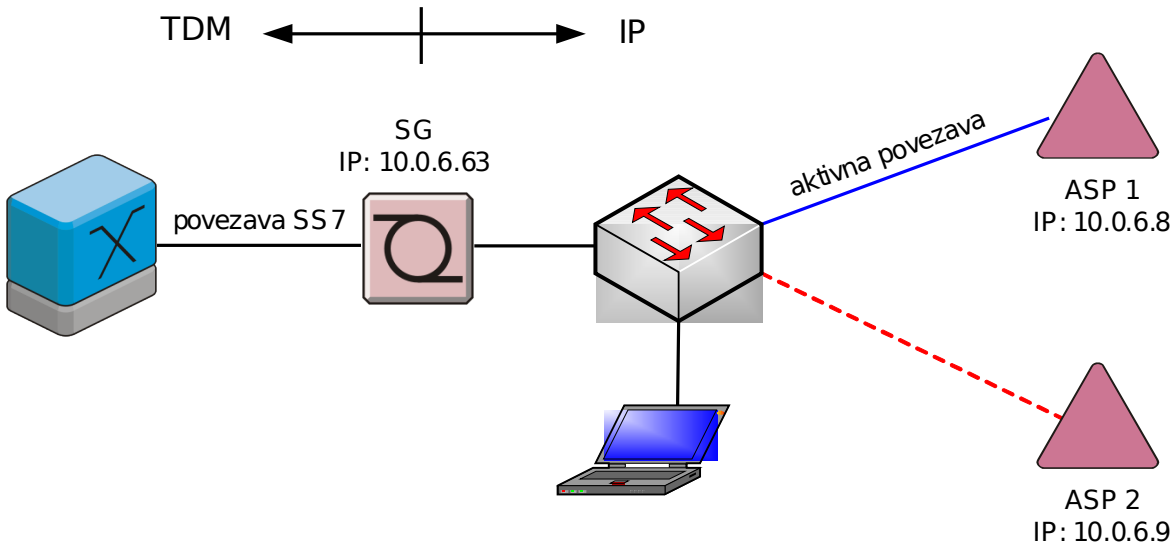
V spodnji tabeli so podani parametri, ki jih priporoča ETSI. Podana je primerjava z vrednostmi parametrov, ki so določeni v standardu za SCTP (RFC 2960).

Parameter	ETSI Največja vrednost	ETSI Najmanjša vrednost	ETSI Korak	Privzeto v RFC 2960 [2]
RTO Min	10ms	5s	10ms	1s
RTO Max	1s	120s	10ms	60s
RTO Initial	RTO Min	RTO Max	10ms	3s
RTO Alpha	1\8	1\8		1\8
RTO Beta	1\4	1\4		1\4
Valid Cookie Life	5s	120s	1s	60s
HB Interval	1s	300s	1s	30s
SACK period	0ms	500ms	10ms	200ms
SACK frequency	1	5	1	2
MTU size	508bytes	65535bytes	1byte	1500bytes

Tabela 9: Primerjava parametrov v ETSI priporočilih v primerjavi z IETF

5.3.REDUNDANČNA ARHITEKTURA 1SG-2AS (PRIORITETNI NAČIN)

Spodnja arhitektura prikazuje primer, ko imamo dva aplikacijska strežnika, ki navadno strežeta istim uporabnikom. Aplikacijska strežnika sta lahko fizično ločena in locirana na različnih mestih, ali pa sta to dva različna procesa v sklopu ene centrale (preklop med aktivnim procesorjem in procesorjem v pripravljenosti). Ob izpadu aktivnega povezave, se aktivira proces drugega aplikacijskega strežnika (ASP2), ki prevzame ves signalni promet.

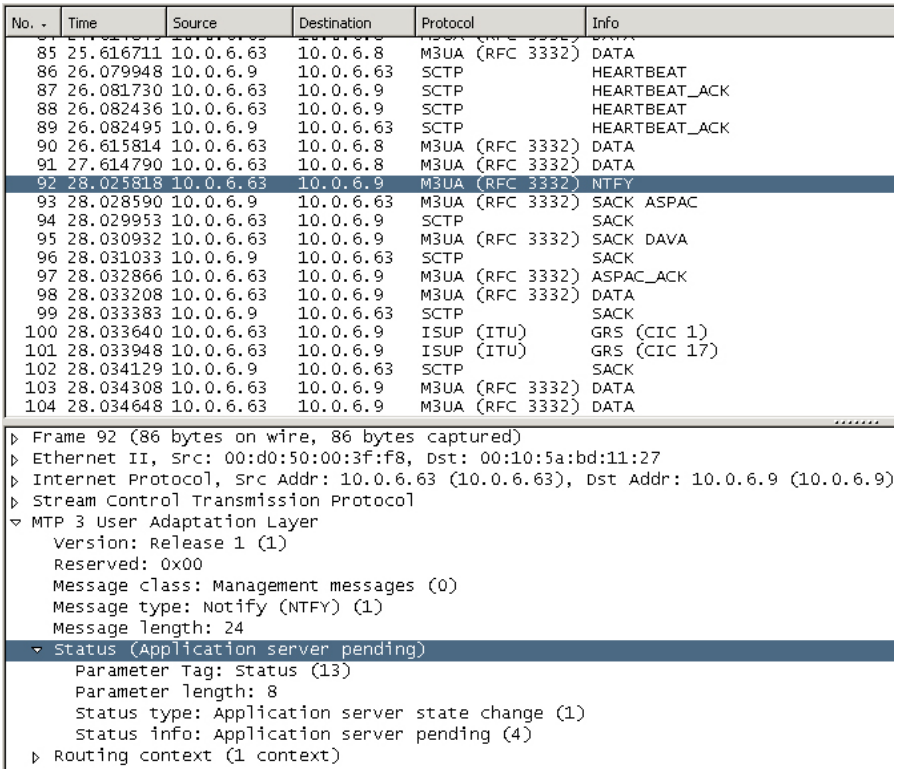


Slika 96: Redundančna arhitektura 1SG-2AS (Prioritetni način)

Na spodnjih dveh slikah je prikazana izmenjava signalnih sporočil pri vzpostavitvi redundančnega modela 1SG-2AS. Razvidno je, da pride do vzpostavitve in aktivacije SCTP povezave med signalnim prehodom in aplikacijskim strežnikom 1. Druga SCTP povezava med signalnim prehodom in aplikacijskim strežnikom 2 je vzpostavljena, vendar v na nivoju M3UA v stanju registracije. Izpad aktivne povezave signalni prehod po določenem času zazna in o tem obvesti ASP2 s signalnim sporočilom NOTIFY (Pending). To je stanje, v katerem signalni prehod

ne obvešča sosednjih točk o spremembi (nedostopnost signalne točke) stanja v omrežju, ampak določen časa počaka, da se aktivira alternativna signalna povezava. Po sprejetju sporočila NOTIFY aplikacijski strežnik takoj aktivira rezervno povezavo, ki prevzame ves signali promet (najprej se pošljejo nepotrjena in neposlana sporočila).

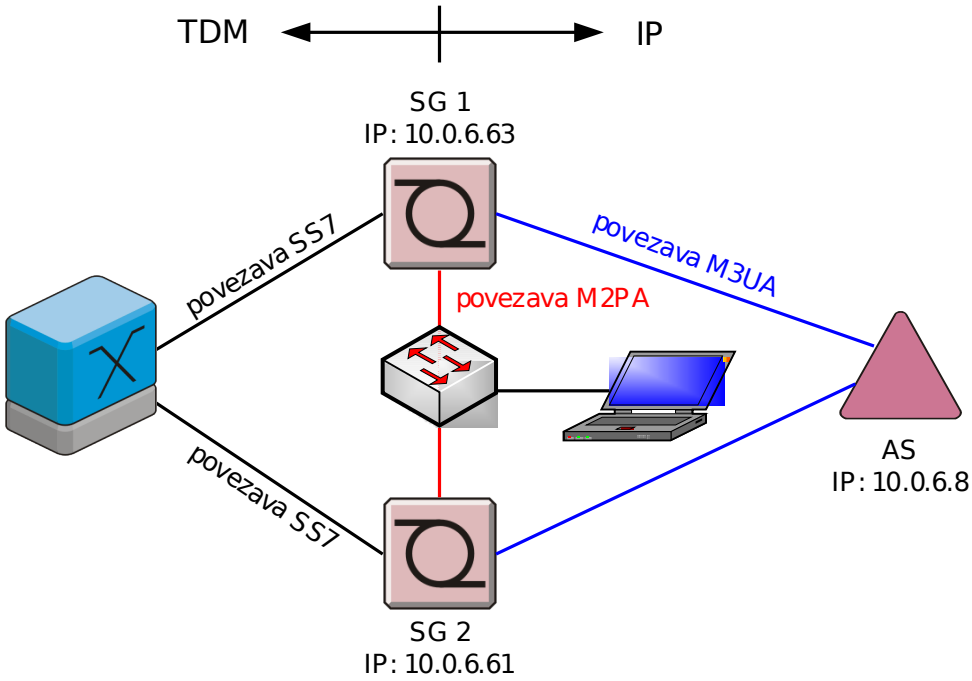
No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.6.8	10.0.6.63	SCTP	INIT
2	0.002683	10.0.6.63	10.0.6.8	SCTP	INIT_ACK
3	0.003109	10.0.6.8	10.0.6.63	SCTP	COOKIE_ECHO
4	0.005607	10.0.6.63	10.0.6.8	SCTP	COOKIE_ACK
5	0.009891	10.0.6.8	10.0.6.63	M3UA (RFC 3332)	ASPUP
6	0.012173	10.0.6.63	10.0.6.8	SCTP	SACK
7	0.012991	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	SACK ASPUP_ACK
8	0.013874	10.0.6.8	10.0.6.63	SCTP	SACK
9	0.017288	10.0.6.8	10.0.6.63	M3UA (RFC 3332)	REG_REQ
10	0.019705	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	SACK REG_RSP
11	0.020208	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	NTFY
12	0.020843	10.0.6.8	10.0.6.63	M3UA (RFC 3332)	SACK ASPAC
13	0.020902	10.0.6.8	10.0.6.63	SCTP	SACK
14	0.022215	10.0.6.63	10.0.6.8	SCTP	SACK
15	0.023201	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	SACK DAVA
16	0.024997	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	ASPAC_ACK
17	0.025655	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	NTFY
18	0.026705	10.0.6.8	10.0.6.63	SCTP	SACK
19	0.227192	10.0.6.8	10.0.6.63	SCTP	SACK
20	6.017518	10.0.6.8	10.0.6.63	SCTP	HEARTBEAT
21	6.017865	10.0.6.63	10.0.6.8	SCTP	HEARTBEAT_ACK
22	8.017312	10.0.6.8	10.0.6.63	SCTP	HEARTBEAT
23	8.017879	10.0.6.63	10.0.6.8	SCTP	HEARTBEAT_ACK
24	8.065928	10.0.6.9	10.0.6.63	SCTP	INIT
25	8.069601	10.0.6.63	10.0.6.9	SCTP	INIT_ACK
26	8.069995	10.0.6.9	10.0.6.63	SCTP	COOKIE_ECHO
27	8.072913	10.0.6.63	10.0.6.9	SCTP	COOKIE_ACK
28	8.078141	10.0.6.9	10.0.6.63	M3UA (RFC 3332)	ASPUP
29	8.080581	10.0.6.63	10.0.6.9	SCTP	SACK
30	8.080823	10.0.6.63	10.0.6.9	M3UA (RFC 3332)	SACK ASPUP_ACK
31	8.081389	10.0.6.9	10.0.6.63	SCTP	SACK
32	8.084627	10.0.6.9	10.0.6.63	M3UA (RFC 3332)	REG_REQ
33	8.087230	10.0.6.63	10.0.6.9	M3UA (RFC 3332)	SACK REG_RSP
34	8.087771	10.0.6.63	10.0.6.9	M3UA (RFC 3332)	NTFY
35	8.088068	10.0.6.9	10.0.6.63	SCTP	SACK
36	10.012279	10.0.6.63	10.0.6.8	SCTP	HEARTBEAT
37	10.012375	10.0.6.8	10.0.6.63	SCTP	HEARTBEAT_ACK
38	10.017332	10.0.6.8	10.0.6.63	SCTP	HEARTBEAT
39	10.017830	10.0.6.63	10.0.6.8	SCTP	HEARTBEAT_ACK
40	11.618319	10.0.6.63	10.0.6.8	M3UA (RFC 3332)	DATA
41	11.618335	10.0.6.8	10.0.6.63	SCTP	SACK
42	11.618580	10.0.6.8	10.0.6.63	ISUP (ITU)	SACK REL (CIC 0)
43	11.823650	10.0.6.63	10.0.6.8	SCTP	SACK



Slika 97: Prikaz sporočil zajetih s program Ethereal v primeru 1SG-2AS (Prioritetni način)

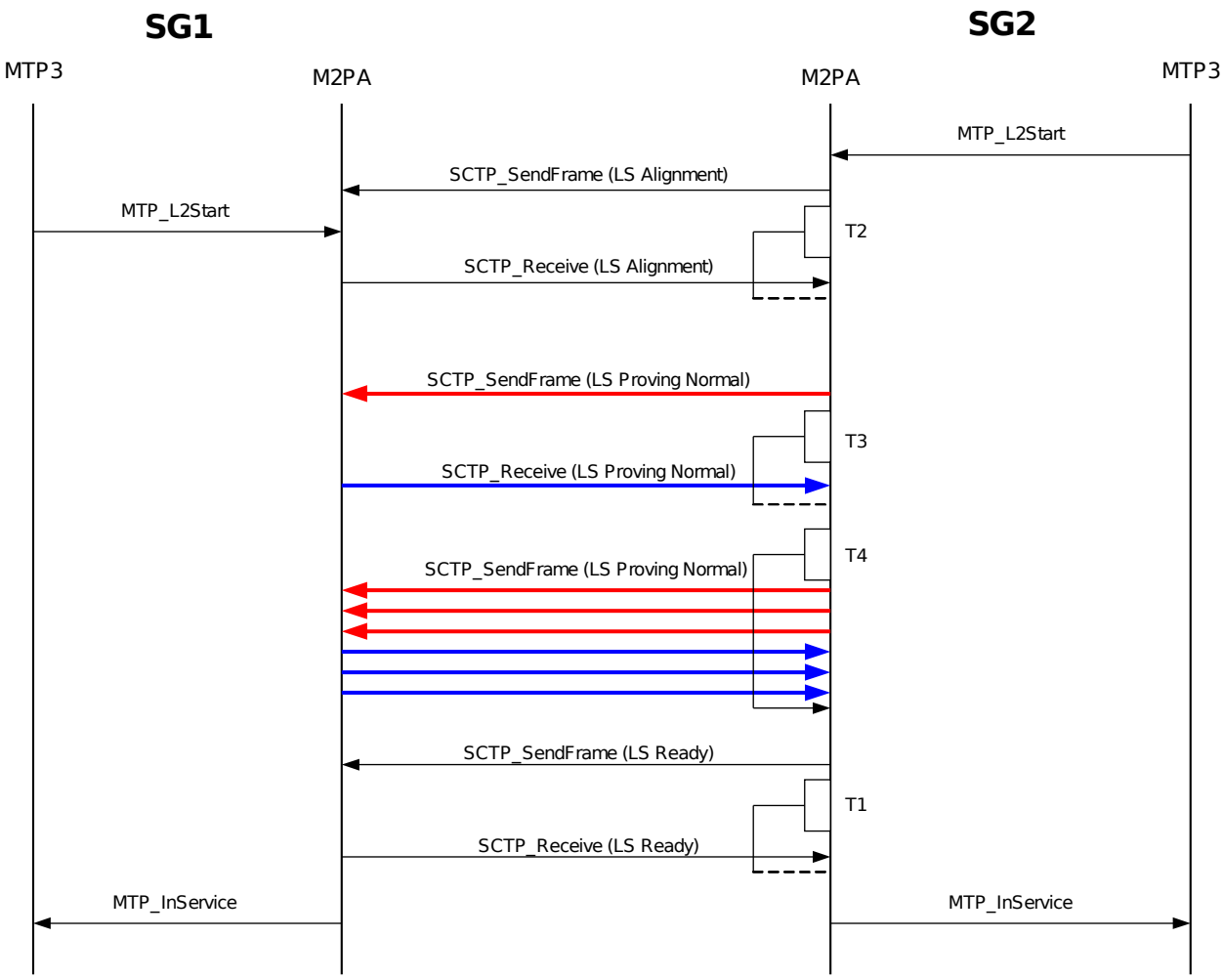
5.4.REDUNDANČNA ARHITEKTURA 2SG-1AS (VZPOSTAVITEV POVEZAVE M2PA)

Na spodnjem primeru je prikazana uporaba protokola M2PA za povezovanje dveh signalnih prehodov. Povezava M2PA nadomešča klasično povezavo SS7. Z vpeljavo nove povezave je arhitektura signalnega omrežja postala bolj kompleksna, ponuja pa zato nove redundančne možnosti. Vzpostavitev povezave M2PA je podobno vzpostavitvi povezave na sloju MTP2.



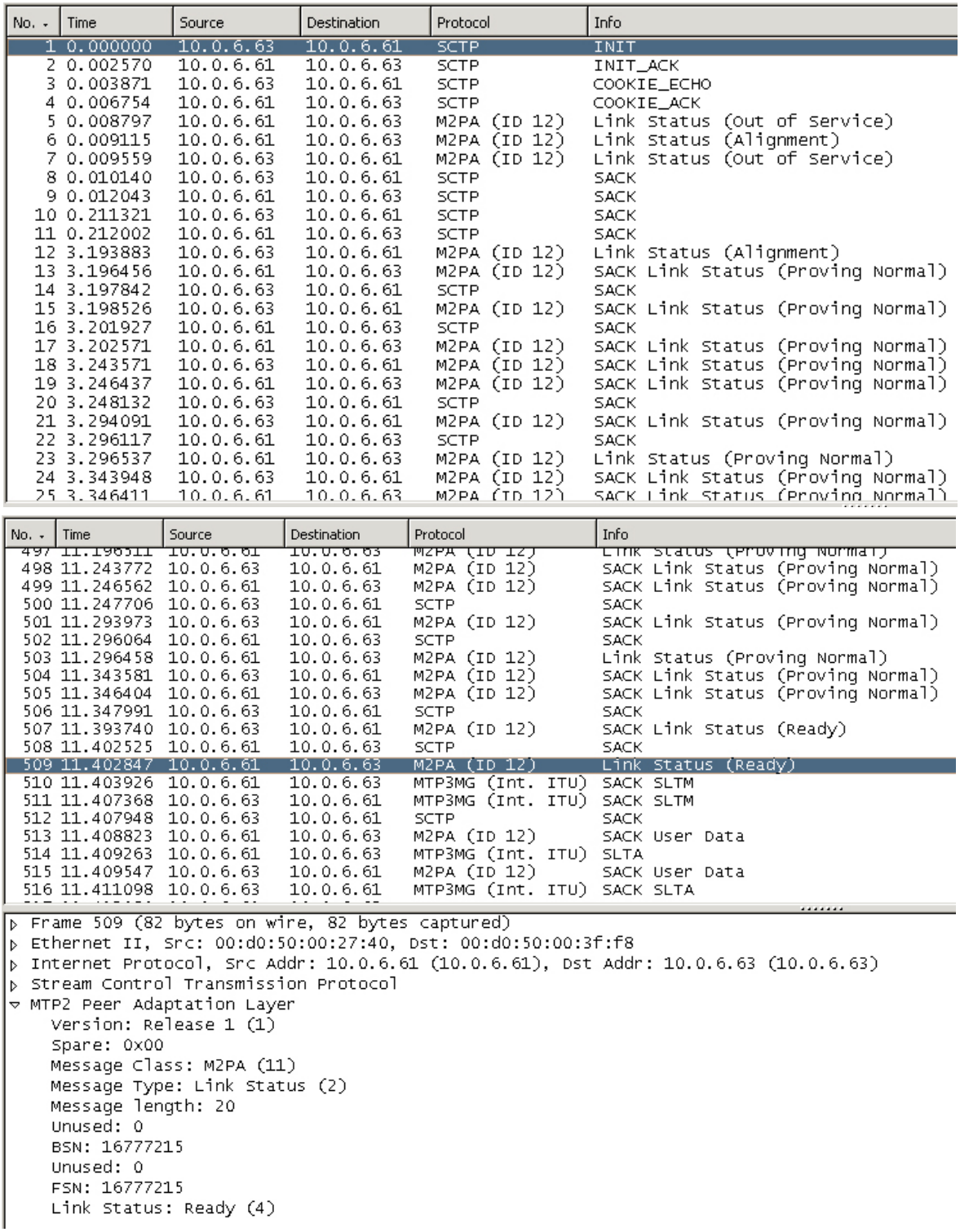
Slika 98: Primer 3 – Uporaba protokola M2PA za povezavo signalnih prehodov

Diagram poteka tipične vzpostavitve povezave M2PA povezave je prikazan na spodnji sliki. Po vzpostavitvi SCTP povezave poteka vzpostavljanje signalne povezave M2PA ekvivalentno kot pri MTP2 [22], s tem da se statusna sporočila pošiljajo samo enkrat, razen nekaj izjem.



Slika 99: Potek vzpostavitve povezave M2PA

Na spodnji sliki je prikazana izmenjava signalnih sporočil zajetih s programom Ethereal med dvema signalnima prehodoma. Velikost časovnikov pri vzpostavitvi povezave M2PA je podobna velikosti časovnikov, ki se uporabljajo ob vzpostavitvenim uvrščanjem na sloju MTP2. Po končanem proceduri vzpostavitvenega uvrščanja obvestimo zgornji sloj (MTP3) o sposobnosti povezave. Na sliki je razvidno, da se po sprejemu statusnega sporočila *READY*, že začne izmenjava sporočil na tretjem sloju.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.6.63	10.0.6.61	SCTP	INIT
2	0.002570	10.0.6.61	10.0.6.63	SCTP	INIT_ACK
3	0.003871	10.0.6.63	10.0.6.61	SCTP	COOKIE_ECHO
4	0.006754	10.0.6.61	10.0.6.63	SCTP	COOKIE_ACK
5	0.008797	10.0.6.61	10.0.6.63	M2PA (ID 12)	Link Status (Out of Service)
6	0.009115	10.0.6.61	10.0.6.63	M2PA (ID 12)	Link Status (Alignment)
7	0.009559	10.0.6.63	10.0.6.61	M2PA (ID 12)	Link Status (Out of Service)
8	0.010140	10.0.6.63	10.0.6.61	SCTP	SACK
9	0.012043	10.0.6.61	10.0.6.63	SCTP	SACK
10	0.211321	10.0.6.63	10.0.6.61	SCTP	SACK
11	0.212002	10.0.6.61	10.0.6.63	SCTP	SACK
12	3.193883	10.0.6.63	10.0.6.61	M2PA (ID 12)	Link Status (Alignment)
13	3.196456	10.0.6.61	10.0.6.63	M2PA (ID 12)	SACK Link Status (Proving Normal)
14	3.197842	10.0.6.63	10.0.6.61	SCTP	SACK
15	3.198526	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Proving Normal)
16	3.201927	10.0.6.61	10.0.6.63	SCTP	SACK
17	3.202571	10.0.6.61	10.0.6.63	M2PA (ID 12)	SACK Link Status (Proving Normal)
18	3.243571	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Proving Normal)
19	3.246437	10.0.6.61	10.0.6.63	M2PA (ID 12)	SACK Link Status (Proving Normal)
20	3.248132	10.0.6.63	10.0.6.61	SCTP	SACK
21	3.294091	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Proving Normal)
22	3.296117	10.0.6.61	10.0.6.63	SCTP	SACK
23	3.296537	10.0.6.61	10.0.6.63	M2PA (ID 12)	Link Status (Proving Normal)
24	3.343948	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Proving Normal)
25	3.346411	10.0.6.61	10.0.6.63	M2PA (ID 12)	SACK Link Status (Proving Normal)

No.	Time	Source	Destination	Protocol	Info
497	11.196511	10.0.6.61	10.0.6.63	M2PA (ID 12)	Link Status (Proving Normal)
498	11.243772	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Proving Normal)
499	11.246562	10.0.6.61	10.0.6.63	M2PA (ID 12)	SACK Link Status (Proving Normal)
500	11.247706	10.0.6.63	10.0.6.61	SCTP	SACK
501	11.293973	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Proving Normal)
502	11.296064	10.0.6.61	10.0.6.63	SCTP	SACK
503	11.296458	10.0.6.61	10.0.6.63	M2PA (ID 12)	Link Status (Proving Normal)
504	11.343581	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Proving Normal)
505	11.346404	10.0.6.61	10.0.6.63	M2PA (ID 12)	SACK Link Status (Proving Normal)
506	11.347991	10.0.6.63	10.0.6.61	SCTP	SACK
507	11.393740	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK Link Status (Ready)
508	11.402525	10.0.6.61	10.0.6.63	SCTP	SACK
509	11.402847	10.0.6.61	10.0.6.63	M2PA (ID 12)	Link Status (Ready)
510	11.403926	10.0.6.61	10.0.6.63	MTP3MG (Int. ITU)	SACK SLTM
511	11.407368	10.0.6.63	10.0.6.61	MTP3MG (Int. ITU)	SACK SLTM
512	11.407948	10.0.6.63	10.0.6.61	SCTP	SACK
513	11.408823	10.0.6.61	10.0.6.63	M2PA (ID 12)	SACK User Data
514	11.409263	10.0.6.61	10.0.6.63	MTP3MG (Int. ITU)	SLTA
515	11.409547	10.0.6.63	10.0.6.61	M2PA (ID 12)	SACK User Data
516	11.411098	10.0.6.63	10.0.6.61	MTP3MG (Int. ITU)	SACK SLTA

```
▷ Frame 509 (82 bytes on wire, 82 bytes captured)
▷ Ethernet II, Src: 00:d0:50:00:27:40, Dst: 00:d0:50:00:3f:f8
▷ Internet Protocol, Src Addr: 10.0.6.61 (10.0.6.61), Dst Addr: 10.0.6.63 (10.0.6.63)
▷ Stream Control Transmission Protocol
▽ MTP2 Peer Adaptation Layer
    Version: Release 1 (1)
    Spare: 0x00
    Message Class: M2PA (11)
    Message Type: Link Status (2)
    Message length: 20
    Unused: 0
    BSN: 16777215
    Unused: 0
    FSN: 16777215
    Link Status: Ready (4)
```

Slika 100: Prikaz signalnih sporočil pri vzpostavitvi povezave M2PA

SKLEP

Razvoj bodočih telekomunikacijskih omrežij je prišel do faze, ko lahko trdimo, da prehod vodovno komutiranih sistemov na paketne tehnologije ni več vprašljiv. Ponudniki klasičnih telekomunikacijskih storitev v zadnjih letih pospešeno uvajajo celične ali paketne prenosne tehnologije, ki dopolnjujejo njihova hrbtenična omrežja digitalne sinhrone hierarhije SDH. Trend združevanja oziroma preseljevanja govornega prometa na enotno prenosno in komutacijsko infrastrukturo bo, ali je že, posledica zmanjšanja stroškov obratovanja in vzdrževanja omrežja. Pomembno vlogo pri tem bodo imeli mehanizmi za zagotavljanja kakovosti storitev, med katere spada tudi zanesljiva signalizacija.

Signalizacija potrebuje visoko zanesljiv prenos signalnih sporočil s hitrimi odzivi na napake. V klasičnem telefonskem omrežju je bil razvit protokolni sklad SS7, ki se je s svojimi postopki izkazal kot zanesljiv sistem za prenos signalnih sporočil. Če želimo prenos signalizacije prestaviti v univerzalno omrežje IP, moramo poskrbeti za enak nivo zanesljivosti.

Redundančni in potrjevalni postopki sami po sebi niso dovolj za zanesljiv prenosni sistem. Pri načrtovanju sistema je pomembna tudi redundančna arhitektura omrežja. Postopki lahko le uporabijo nabor možnosti, ki jih arhitektura omrežja ponuja. Bistvena razlika med protokolnim skladom SS7 in protokolnim skladom SIGTRAN je predvsem v organiziranosti in načinu prenosa na podatkovnem nivoju. Povprečna zasedenost signalnih povezav v TDM je 0,2 Erlanga. S tem imamo zagotovljeno rezervo ob izpadu katere od signalnih povezav. Podatkovni nivo omrežja IP pa deluje na principu statističnega multipleksa. Preko omrežja IP signalizacija nima zagotovljene kapacitete prenosa, temveč si jo deli z drugimi trenutnimi uporabniki. Iz tega sledi, da mora biti omrežje IP univerzalno, ter tako podpirati veliko število različnih protokolov. Odzivni čas na spremembe omrežja IP in zakasnitve na posamezni omrežni napravi so zato večje kot v namenskem telefonskem omrežju. Omenjene pomanjkljivosti lahko izboljšamo z uporabo redundančne arhitekture, uporabljeno omrežje

lahko ločimo od ostalih uporabnikov ali pa signalizaciji na posameznih usmerjevalnikih določimo ustrezno prioriteto ali QoS.

Za prenos signalizacije SS7 prek omrežja IP se uporablja skupino SIGTRAN protokolov. Transportni protokol SCTP uporablja selektivno potrjevanje, večdomnost, večtokovnost, preverjanje dostopnosti poti s heartbeati in prekolop med aktivnimi potmi. Primerjava protokola SCTP in istoležnega sloja MTP2 nam pokaže, da protokol SCTP omogoča tudi redundančne in preklopne postopke, medtem ko MTP2 skrbi le za potrjevanje in hitro zaznavanje izpadov dostopnosti ene same signalne povezave. Lahko bi povzeli, da SCTP omogoča povezavo z več potmi med dvema signalnima točkama. SCTP uporabi redundančno arhitekturo omrežja IP ter svoje postopke z namenom, da ustvari dovolj veliko zanesljivost, ki mora biti ekvivalentna namenskemu telefonskemu omrežju.

V protokolnem skladu SS7 imamo na tretjem nivoju sloj MTP3, ki skrbi za pravilno dostavo signalnih sporočil in vzdrževanje omrežja. V protokolnem skladu SIGTRAN imamo na tretjem nivoju več prilagodilnih slojev. Podobno funkcionalnost in enak nabor postopkov kot sloj MTP3 nam omogoča protokol M3UA.

Prednost signalizacije preko omrežja IP je predvsem v tem, da so smernice razvoja telekomunikacij uprte v univerzalno prenosno omrežje IP. Izboljšujejo se hitrosti omrežnih naprav, kapacitete fizičnih povezav, prenosni protokoli (IPv6) in varnost. Uporablja se tudi omejitev prometa, multicasting ter zagotavljanje QoS določenim storitvam. Nadaljnji razvoj namenskega prenosnega sistema in omrežja za telefonijo, bi bil predrag in nesmiseln, saj lahko tudi omrežje IP ločimo od drugih uporabnikov ter tako izkoristimo vso kapaciteto omrežja za eno samo storitev.

V resnici je na prvi pogled omrežje IP po svoji naravi še vedno manj predvidljivo in zanesljivo kot omrežje SS7. Ima večje zakasnitve, kasnejše odkrivanje napak, pri preklopu pa se sporočila lahko izgubijo ali podvajajo. Te lastnosti izboljšujemo z velikim naborom redundančnih in drugih postopkov. Bistvenega pomena je torej ustrezno načrtovati arhitekturo omrežja, v katero moramo vnesti dovolj redundance glede

na raven zanesljivosti, ki jo želimo doseči. Če uporabimo omrežje, ki ga hkrati uporablja več različnih uporabnikov, je potrebno pripraviti tudi posamezne omrežne elemente, da signalizacijo obravnavajo prioritetno. Zato je še vedno najlažje imeti ločeno ter namensko omrežje IP. Z opisanimi postopki je lahko zanesljivost signalizacije preko omrežja IP primerljiva prenosnemu sistemu MTP. Vsebuje namreč vse potrebne postopke za zagotavljanje zanesljivosti, ki jo je v omrežju SS7 navajen uporabnik.

Prenos signalizacije SS7 preko omrežja IP je smiseln tudi zaradi visokih cen signalizacijskih vmesnikov, vzdrževanja in postavitve samega omrežja. Končne točke v omrežju SS7 morajo namreč biti povezane z 2MB E1 povezavami, ki navadno niso popolnoma izkoriščene. V omrežju IP lahko vedno bolj zmogljive povezave izkoristimo tako za signalizacijo kot za prenos drugih podatkov. Poleg tega je omrežje IP marsikje že postavljeno, zaradi IP usmerjanja pa je enostavnejša redundanca prenosnih poti. Moje mnenje je, da prenos signalizacije SS7 preko omrežja IP ni alternativa ali zamenjava za obstoječe omrežje SS7. Kvečjemu bo ta korak prispeval k razširitvi signalnega omrežja in zagotavljanju večje zanesljivosti in redundance.

SEZNAM UPORABLJENIH VIROV

[1] RFC 2719, Framework Architecture for Signaling Transport, IETF, Oktober 1999,
http://www.ietf.org/rfc/rfc2719.txt

[2] RFC 2960, Stream Control Transmission Protocol, IETF, Oktober 2000,
http://www.ietf.org/rfc/rfc2960.txt

[3] RFC 3332, Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA), IETF, September 2002,
http://www.ietf.org/rfc/rfc3332.txt

[4] RFC 3332, Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Adaptation Layer (M2UA), IETF, September 2002,
http://www.ietf.org/rfc/rfc3331.txt

[5] RFC 3332, Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Peer-to-Peer Adaptation Layer (M2PA), IETF, September 2005,
http://www.ietf.org/rfc/rfc4165.txt

[6] draft-ietf-tsvwg-sctpimpguide-16.txt, Stream Control Transmission Protocol (SCTP) Specification Errata and Issues, IETF, 24.Oktober 2005,
http://www.ietf.org/internet-drafts/draft-ietf-tsvwg-sctpimpguide-16.txt

[7] draft-asveren-sigtran-m3uacons-00.txt, M3UA Deployment Considerations, IETF, 22. November 2005,
http://www.ietf.org/internet-drafts/draft-asveren-sigtran-m3uacons-00.txt

[8] Tine Stegel, Zanesljivost in redundanca v SIGTRAN protokolih, diplomsko delo, 2005

[9] Jaka Javornik, Protokol SCTP z dodatkom delne zanesljivosti in uporaba pri strujanju večpredstavnostnih vsebin, diplomsko delo, 2005

[10] Rok Žurbi, Signalizacijski in krmilni protokoli v omrežjih naslednje generacije, magistrsko delo, 2001

[11] Roman Osredkar, Zlivanje telekomunikacijskih omrežij, magistrsko delo, 2002

[12] Travis Russel, Signaling System #7, second edition, McGraw-Hill, 1998

[13]Guy Redmill , An Introduction to SS7, white paper, julij 2001
[14]SS7 Tutorial, Preformance Technologies, www.pt.com
[15]CiscoSS7Fundamentals, http://www.cisco.com/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/
[16]Signaling Transport over IP (SIGTRAN), http://www.sctp.de/sigtran.html
[17]OpenSS7, http://www.openss7.org/
[18]Andreas Jungmaier, University of Essen, Institute of Computer Networking Technology, Germany Michael Schopp, Michael T¨uxen, Siemens AG, Information and Communication Networks, Munich, Germany, Performance Evaluation of the Stream Control Transmission Protocol, 3rd International Conference on ATM, 2000
[19]ITU-T Recommendation Q.700: Introduction to CCITT Signalling System No. 7, International Telecommunication Union
[20]ITU-T Recommendation Q.701: Functional description of the message transfer part (MTP) of Signalling System No. 7, International Telecommunication Union
[21]ITU-T Recommendation Q.702: Signalling data link, International Telecommunication Union
[22]ITU-T Recommendation Q.703: Signalling link, International Telecommunication Union
[23]ITU-T Recommendation Q.704: Signalling network functions and messages, International Telecommunication Union
[24]ITU-T Recommendation Q.706: Signalling System No. 7 – Message Transfer Part Signalling Performance

IZJAVA

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

Ljubljana, april 2006

Primož Brajnik

SEZNAM UPORABLJENIH KRATIC IN DOLOČENIH IZRAZOV

AS	Application Server	Aplikacijski strežnik
DPC	Destination Point Code	Koda ponorne točke
FISU	Fill-In Signal Unit	Signalno sporočilo za zapolnjevanje
GT	Global Title	Globalni naslov
IETF	Internet Engineering Task Force	Delovna skupina za internetsko inženirstvo
IN	Intelligent Network	Inteligentno omrežje
INAP	Intelligent Network Application Part	Aplikacijski protokol inteligentnega omrežja
IP	Internet Protocol	Internetni protokol
ISDN	Integrated Services Digital Network	Digitalno omrežje z integriranimi storitvami
IUA	ISDN Q.921 User Adaptation Layer	ISDN uporabniški prilagodilni sloj Q.921
LSSU	Link Status Signal Unit	Signalno sporočilo o stanju povezave
MAP	Mobile Application Part	Mobilni aplikacijski del
M2PA	MTP2 Peer to Peer Adaptation Layer	MTP2 soležni prilagodilni sloj
M2UA	MTP2- User Adaptation Layer	Uporabniški prilagodilni sloj MTP 2. sloja
M3UA	MTP3-User Adaptation Layer	Uporabniški prilagodilni sloj MTP 3. sloja
MSU	Message Signal Unit	Signalno sporočilo z vsebino višjih slojev
MTP	Message Transfer Part	Sporočilno-prenosni del
MTU	Maximum Transmission Unit	Največja prenosna enota
NIF	Nodal Inter-working Function	Prilagodilni sloj
OPC	Origination Point Code	Koda izvorne točke
PSTN	Public Switched Telephone Network	Javno komutirano telefonsko omrežje
OMAP	Operation, Maintenance and Administration Part	Obratovalno vzdrževalni administrativni del
QoS	Quality of Service	Kakovost storitve
OSI	Open System Interconnection	Medsebojno povezovanje odprtih sistemov
RTO	Retransmission Time-out	Časovni iztek za ponovno pošiljanje

RTT	Round-trip Time	Čas obhoda
R WND	Receiver Window	Sprejemno okno
SCCP	Signaling Connection Control Part	Krmilni del signalne zveze
SCP	Signalling Control Point	Storitvena krmilna točka
SCTP	Stream Control Transmission Protocol	Prenosni protokol s krmiljenjem pretoka
SEP	Signaling End Point	Končna signalna točka
SG	Signaling Gateway	Signalni prehod
SGP	Signaling Gateway Process	Proces signalnega prehoda
SI	Stream Identificator	Identifikator sporočilnega toka
SIO	Service Indicator Octet	Indikator storitev (oktet)
SLS	Signaling Link Selection	Selekcija signalne povezave
SN	Switch Node	Komutacijsko vozlišče
SSP	Service Switching Point	Točka preklapljanja storitev
STP	Signaling Transfer Point	Signalna prenosna točka
SS7	Signalling System no.7	Signalizacija številka 7
SSN	Subsistem Number	Številka podsistema
SSN	Stream Sequence Number	Zaporedna številka sekvence v toku
SUA	SCCP User Adaptation Layer	Uporabniški prilagodilni sloj SCCP-ja
TCAP	Transaction Capabilities Application Part	Aplikacijski del za transakcijske zmožnosti
TCP	Transmission Control Protocol	Protokol za krmiljenje prenosa
TDM	Time division multiplex	Časovni multipleks
TSN	Transmission Sequence Number	Zaporedna številka oddaje
TUP	Telephone User Part	Telefonski uporabniški del
UDP	User Datagram Protocol	Uporabniški datagramski protokol
ULP	Upper-layer Protocol,	Protokol višje ležečega sloja