Univerza v Ljubljani

Fakulteta za elektrotehniko

Roman Kotnik

NADZOR SIGNALIZACIJ V TELEKOMUNIKACIJSKIH OMREŽJIH

MAGISTRSKO DELO

Mentor: prof. dr. Janez Bešter

V Ljubljana, 2005

Zahvala

Želim se zahvaliti vsem, ki so mi stali ob strani, me vzpodbujali in mi nudili pomoč skozi vsa študijska leta. Posebna zahvala gre mentorju prof. dr. Janeza Beštru in mag. Franciju Katrašniku, ki sta me z nasveti, razmišljanji in strokovnim znanjem vodila in usmerjala pri izdelavi magistrskega dela. Zahvala tudi vsem sodelavcem Laboratorija za telekomunikacije za vzpodbude in pomoč. Na tem mestu se zahvaljujem tudi svojim staršem, ki so mi študij omogočili.

Vsem iskrena hvala !

Staršema Viktorju in Vidi, ter bodoči ženi Nataši

Povzetek

Magistrska naloga obravnava nadzor in spremljanje signalizacij v telekomunikacijskih sistemih. Predstavljena je problematika in koncept sistemov za nadzor signalizacij.

Signalizacija je v telekomunikacijskih sistemih ključnega pomena. V klasičnih javnih telefonskih omrežjih se tipično uporablja signalizacija številka sedem. V omrežjih nove generacije se uporablja več tipov signalizacij.

V današnjih omrežjih je nadzor omrežja in spremljanje karakteristik postal pomembnejši kot kadarkoli prej. Nadzor signalizacijskega prometa je najenostavnejša metoda za odkrivanje nenamernih in namernih zlorab v signalizacijskih omrežjih. Ne uporablja se samo za določitev stanja v katerem je omrežje in kaj se v omrežju dogaja, ampak lahko z nadzorom opravljamo kompleksno zaračunavanje storitev, zajemanje podatkov, odkrivanje in preprečevanje vdorov v omrežje, upravljamo s podatki, delamo statistike ter razvijamo uporabniške aplikacije.

V Laboratoriju za telekomunikacije smo v sodelovanju s slovenskim podjetjem razvili produkt za nadzor signalizacije imenovan Symonet. Za zajem signalizacijskih podatkov se uporablja sonda. Sonda v sprotnem času zajema podatke s signalne povezave. Sistem trenutno omogoča nadzor signalizacije številka sedem.

V zadnjem času se telefonski operaterji odločajo za integracijo tradicionalnih omrežij s paketno orientiranimi omrežji. Zaradi tega se je pojavila potreba po razširitvi sistema Symonet na nadzor v omrežjih nove generacije.

Poudarek razširitve sistema je v uporabi novih zapisov klicev in zajemu signal-

izacije. Potrebno je razširiti funkcionalnost sonde. Trenutno uporabljena strojna oprema se ni izkazala za dovolj zmogljivo. Nova strojna oprema bi omogočala razširitev na zajem novih signalizacij in izboljšanje zmogljivosti zajema signalizacije številka sedem.

Ključne besede: Signalizacija številka sedem (SS7), Nadzor siganlizacije, Omrežja nove generacije (NGN)

Abstract

This paper discusses surveillance and monitoring methods of signalling systems in telecommunications networks. It presents several issues and a concept of signalling monitoring systems.

Signalling in telecommunications systems is of great importance. Typical signalling, found in classical public telephony systems, is Signalling System Number 7. In new generation networks several different signalling types are used.

Until present time network monitoring and surveillance of network characteristics have gained greater importance than ever before. Monitoring of signalling traffic is the simplest method used for detecting intentional and unintentional abuses in signalling systems. Apart form defining the condition and operation of the network, the method serves as a strong tool to perform complex service accounting, data collection, detection and prevention of network intrusions, data management, statistics and user application development. Performance monitoring, security, fraud detection, alarm monitoring, billing verification, remote protocol analysis, failure prediction and traffic engineering are some aspects that need to be monitored continuously.

As a result of close cooperation with a Slovenian telecommunications company Laboratory for telecommunications has developed a product for signalling monitoring, called Symonet. A probe is used that collects signalling data from a signalling connection in real time. For the moment, the product provides for monitoring of Signalling System Number 7.

New generation networks concept has been driving telecommunications op-

erators into integration of traditional and packet oriented networks. Therefore, there is a need to upgrade current version of Symonet to provide new generation networks monitoring.

Two key aspects of the product upgrade are the use of call detail records and extended signalling monitoring. The functionalities of the probe have been further extended. Current hardware of the probe has not been proved enough efficient. Therefore, new hardware version has been designed that could provide extensions for monitoring new signalling systems and enhanced capabilities of monitoring existent Signalling System Number 7.

Keywords: Signalling System Number 7 (SS7), Surveillance and Monitoring, New Generation Networks (NGN)

Vsebina

Seznam slik

1. Uvod

Na nivoju signalizacije med centralami se sedaj praktično v vseh omrežjih uporablja signalizacija številka sedem (Signalling System no. 7 - SS7), ki se uporablja tudi za dostop do specializiranih centrov in v zadnjem času vse več tudi za povezavo z internetnim protokolom (Internet protokol - IP)baziranimi aplikacijami.

SS7 predstavlja živčni sistem sodobnih telekomunikacijskih sistemov saj poleg signalizacije za vzpostavljanje zvez omogoča tudi dodatne in inteligentne storitve, prehode med omrežji, nadzor in upravljanje omrežij ter vrsto novih aplikacij. Omrežje SS7 je za operaterje in upravljavce dragocen vir informacij o stanju ne samo signalnega temveč tudi uporabniških omrežij. Zato se že nekaj časa pojavlja potreba po čim učinkovitejšem nadzoru signalizacijskega omrežja in posredno tudi uporabniškega. Z ustreznim nadzorom, shranjevanjem in ustrezno analizo podatkov zajetih na signalnih povezavah lahko kvalitetno nadzorujejo, upravljajo in načrtujejo telekomunikacijski sistem. Glavna prednost omrežja SS7 je njegova zanesljivost, robustnost in razpoložljivost. Da to dosežemo in ohranimo v pogojih vse večjega prometa in novih povezav je potrebno pazljivo načrtovanje in vzdrževanje signalizacijskega omrežja. V omrežju mora biti zadosti redundance, da sistem SS7 brez problemov preživi posamezne okvare v signalnem omrežju.

Razvoj sistemov za nadzor signalizacije postal nuja, saj vedno več operaterjev zahteva nadzor v svojih omrežjih. Z nadzorom signalizacije operaterji dobijo povratne informacije o dogajanju v njihovih omrežjih. Na podlagi pridobljenih informacij, kot so klicne navade uporabnikov, lokacija od kje in kam uporabniki

kličejo, trajanje in pogostost klica, lahko operaterji izboljšajo kvaliteto storitev, varnost in preprečevanje zlorab ter razvoj in zaračunavanje novih izboljšanih storitev.

V začetku je sledenje in nadzor signalizacije SS7 služilo za ugotavljanje stanja in diagnosticiranja omrežja SS7. Na omrežju so postavili naprave s katerimi so zajemali in obdelali podatke v sprotnem času. Obdelane podatke so zatem zbrali v centru, kjer so analizirali delovanje celotnega omrežja. Tako so lahko neprestano spremljali vsak link, sporočilo in klic v omrežju SS7.

Nadzor signalizacije se ne uporablja samo za spremljanje stanja omrežja. Z nadzorom lahko opravljamo kompleksno zaračunavanje storitev, zajemanje podatkov, odkrivanje in preprečevanje vdorov v omrežje, upravljamo s podatki, delamo statistike ter razvijamo uporabniške aplikacije.

2. Signalizacije v telekomunikacijskih sistemih

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.

2.1 Signalizacija številka sedem

Sodobna vodovno komutirana omrežja uporabljajo signalizacijo številka 7 (SS7). Protokoli SS7 so namenjeni izmenjavi krmilnih sporočil med elementi omrežja. Krmilne funkcije v omrežnih elementih uporabljajo vsebino signalizacijskih sporočil za usmerjanje, rezervacijo virov, prevedbo naslovov, vzpostavitev in upravljanje klica ter zaračunavanje. SS7 predstavlja živčni sistem sodobnih telekomunikacijskih sistemov, saj poleg signalizacije za vzpostavljanje zvez omogoča tudi dodatne in inteligentne storitve, prehode med omrežji, nadzor in upravljanje omrežij ter vrsto novih aplikacij. Signalizacijski sistem številka sedem je osnovan na podatkovnem prenosnem omrežju, ki na fizičnem sloju uporablja TDM-prenosne kanale, na omrežnem sloju pa komutacijo sporočil; govorimo lahko o paketni komutaciji. Glavna prednost omrežja SS7 je njegova zanesljivost, robustnost in razpoložljivost.

2.1.1 Arhitektura

Omrežje SS7 sestavljajo signalizacijske točke in podatkovne sigalizacijske povezave med temi točkami. Signalizacijska sporočila se prenašajo prek signalnih povezav v sporočilih različne dolžine, ki jih imenujemo signalni stavki (signal unit). Imamo tri vrste signalnih stavkov, ki se ločijo po indikatorju dolžine. To so polnilni stavek (Fill In Signal Unit - FISU), ki se prenaša kadar ni drugih stavkov, statusni stavek (Link Status Signal Unit - LSSU) za prenos kontrolnih informacij in sporočila, ki se prenašajo v sporočilnih signalnih stavkih (Message Signal Unit - MSU). Signalizacijska sporočila se med vozlišči prenašajo v paketih s postopkom paketne komutacije, kar zagotavlja boljšo izrabo signalnih povezav.

Ločimo tri vrste signalizacijskih točk:

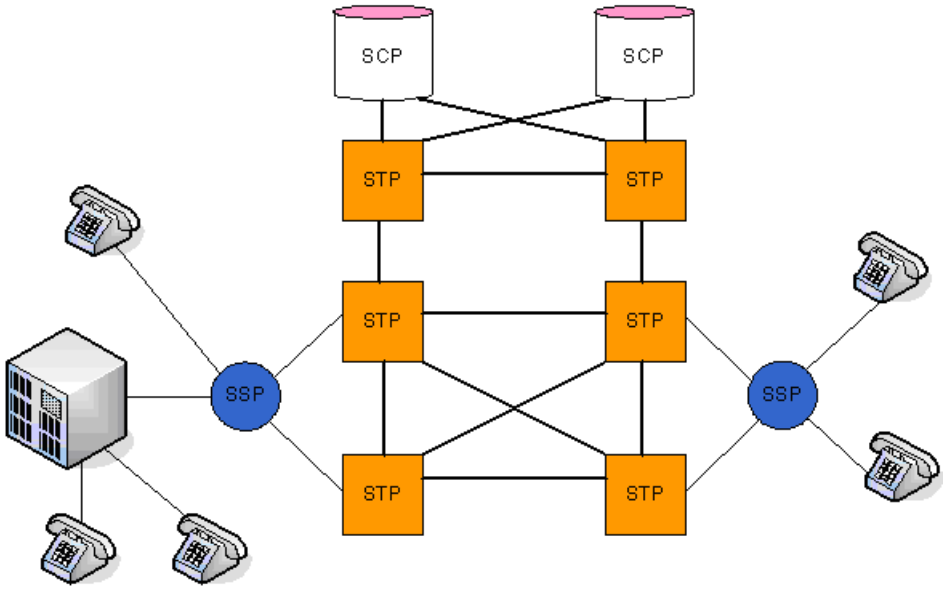
- storitvene komutacijske točke (Service Switching Point - SSP),
- signalizacijske prenosne točke (Signalling Transfer Point - STP),
- storitvene kontrolne točke (Signalling Control Point - SCP).

Signalizacijske točke zagotavljajo dostop do signalizacijskega SS7 omrežja, dostop do podatkovnih baz, ter usmerjajo sporočila do ostalih točk znotraj omrežja. Svetovno signalizacijsko omrežje je razdeljeno na dve ravni, ki sta 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 (Point Code).

Storitvena komutacijska točka (Signalling Switching Point - 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



Slika 2.1: Arhitektura SS7 omrežja

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 (Signalling Control Point - SCP). V primeru uspešne poizvedbe lahko usmeri določen klic na ustrezno vozlišče.

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

Storitvena krmilna točka (SCP) služi kot vmesnik za dostop do podatkovnih baz operaterjev. Podatkovne baze shranjujejo informacije o naročnikih, parametre za usmerjanje posebnih telefonskih številk, varujejo pred zlorabami in nepooblaščenimi uporabniki. Vsak ponudnik storitev ima različne zahteve, zato se njihove baze ponavadi med seboj razlikujejo.

Poznamo tri nivoje prenosnih signalih točk:

- nacionalne prenosne signalizacijske toče,

- internacionalne prenosne signalizacijske točke,
- prehodne prenosne signalizacijske točke.

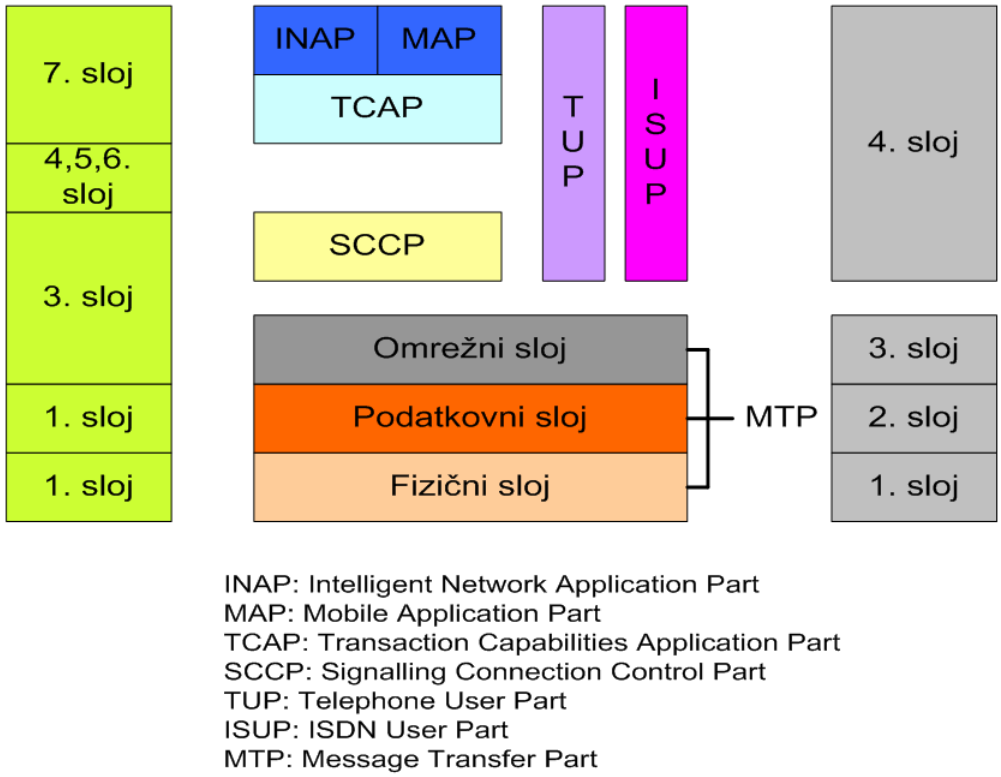
2.1.2 Protokolni sklad signalizacije številka sedem

Arhitektura protokolnega sklada SS7 je prikazana na sliki 2.2. Z nje je razvidna tudi umestitev posameznih protokolnih slojev v OSI modelu. Protokolno arhitekturo sestavljajo omrežni storitveni del (Network Service Part - NSP) in uporabniški del (User Part) ki predstavlja višje protokolne sloje in se nanaša na uporabnike signalizacijskega omrežja (uporabniška signalizacija).

NSP sestavljata podsistem za prenos sporočil (Message Transfer Part - MTP) in krmilni del signalizacijske zveze (Signalling Connection Control Part - SCCP). Del za prenos sporočil sestavljajo trije sloji, ki opravljajo funkcije signalizacijskega podatkovnega voda, signalizacijskega voda in signalizacijskega omrežja. MTP omogoča nepovezavno usmerjen prenos signalnih sporočil preko omrežja do določenega ponora (uporabnika). Funkcije vgrajene v MTP omogočajo, da se v primeru posameznih okvar v signalizacijskem omrežju nadaljuje prenos sporočil brez večjih poslabšanj. SCCP zagotavlja dodatne funkcije k MTP za povezavne in nepovezavne omrežne storitve. MTP je bil definiran pred SCCP in je ukrojen po meri časovnih 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, recimo storitve preko transakcijskega sloja.

2.1.3 Podsistem za prenos sporočil

Podsistem za prenos sporočil (MTP), uporabljajo vsi uporabniški podsistemi v signalizaciji SS7 kot nepovezavno orientiran transportni sistem za izmenjavo

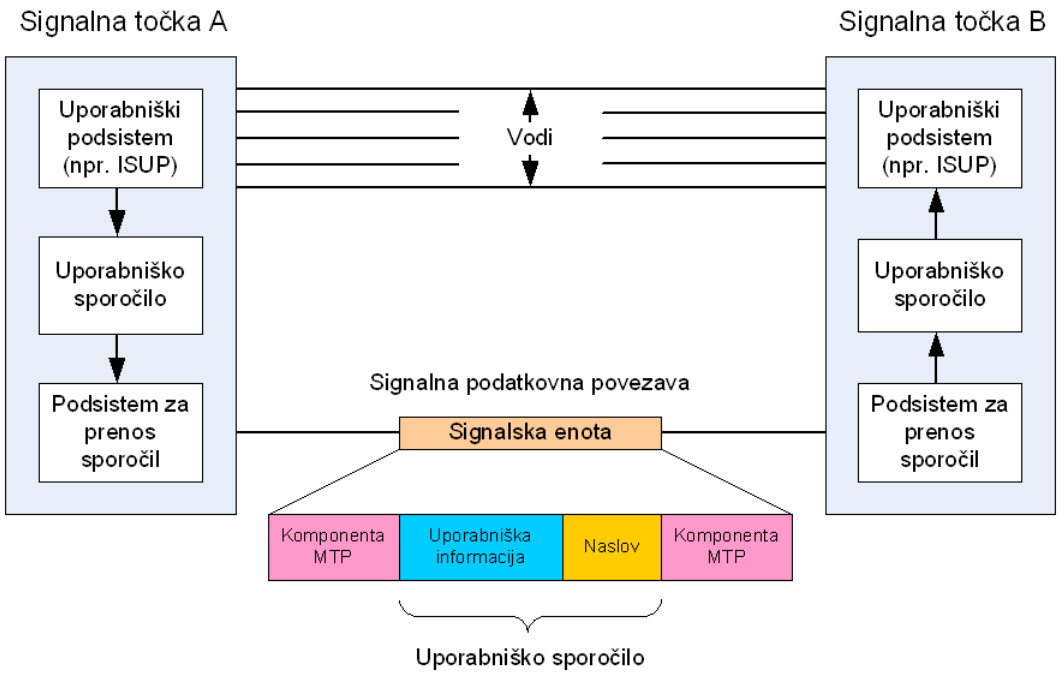


Slika 2.2: Protokolni sklad SS7

sporočil. Sporočila, ki se morajo prenesti od ene končne signalizacijske točke k drugi, se predajo podsistemu za prenos sporočil. Ta zagotavlja, da bodo sporočila dosegla naslovljeni uporabniški podsistem v pravilnem zaporedju, brez podvajanja in brez bitnih napak.

Vsaka signalna točka ima svoj unikaten naslov (PC - Point Code), na podlagi katerega se izvaja usmerjanje po celotnem omrežju. Vzporednice bi lahko vlekli z IP protokolom, v katerem je prenos sporočil prav tako nepovezavno orientiran, usmerjanje pa temelji na IP naslovih. Kljub navidezni podobnosti pa so razlike vendarle velike.

SS7 je namensko omrežje, torej ločeno od drugih storitev oziroma uporabnikov, medtem ko si lahko omrežje IP deli več različnih uporabnikov. Prenos na fizičnem sloju SS7 deluje na principu časovnega dodeljevanja prenosnih zmogljivosti TDM (Time Division Multiplex). Vsak logičen kanal, signalna



Slika 2.3: Signalni podatkovni vod (MTP1)

povezava ima zagotovljeno stalno hitrost, s katero lahko pošilja podatke, do druge signalno transportne točke. V omrežju IP večinoma ni zagotovljene hitrosti in zanesljivosti prenosa, ampak si njegove kapacitete, kot so fizične povezave, hitrost stikal in usmerjevalnikov, dinamično razdelijo vsi uporabniki (statistični multipleks). Kadar med signalnima točkama ni prometa, v SS7 je ves čas zaseden celotni logični kanal (prenašajo se prazne signalizacijske enote FISU), medtem ko so v omrežju IP kapacitete povezave zasedene le kadar je potrebno.

Potrjevanje sprejetih sporočil se v MTP izvaja že na neposredni povezavi med dvema točkama na MTP2 sloju. V TCP/IP protokolnem skladu potrjevanje izvaja šele TCP/SCTP ali kakšen drug višjeležeči sloj, potrjuje pa se le na relaciji končnih točk, torej čez celotno pot, na kateri ni možno hitro določiti točnega položaja in vzroka napake. Zagotavljanje zanesljivosti dostave se v MTP izvaja na precej nižjem nivoju kot v TCP/IP, kar nakazuje, da je v SS7 poudarek predvsem na zanesljivosti in hitrem zaznavanju napak.

Povezavno funkcionalnost v SS7 po potrebi zagotovi šele SCCP sloj, ki leži nad MTP3 nivojem. SCCP je torej del transportnega sistema SS7, ni pa za vse višje uporabniške protokole nujno potreben, zato ga ponavadi opisujemo ločeno.

Prvi sloj - MTP1

Signalni podatkovni vod 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 slotov (time slot access), ki ima priključek na signalni terminal. 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. Analogni signalni data link je sestavljen iz govornega analognega kanala in modemov. Prenosni kanali so lahko zemeljski ali linijsko/radijski.

Za digitalne signalizacijske podatkovne linke 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).

Drugi sloj - MTP2

Skupaj s signalnim podatkovnim linkom omogočajo funkcije signalizacijskega linka zanesljiv prenos signalnih sporočil med dvema direktno povezanima signalnima vozliščema. Signalna sporočila se prenašajo preka signalizacijskega linka v sporočilih različne dolžine, ki jih imenujemo signalizacijske stavke (signal unit). Imamo tri vrste signalnih stavkov, ki se ločijo po indikatorju dolžine (LI - length indicator). To je 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).

MTP2 sloj skrbi za vzpostavljanje in rušenje logične signalizacijske povezave med neposredno povezanima signalnima točkama in nadzira stanje in zasičenost le te, o spremembah pa obvešča MTP3 sloj. Zagotavlja tudi zaporedno pošiljanje in dostavljanje SS7 signalnih enot ter izvaja njihove potrditve sprejema. Z algoritmom za ugotavljanje napak zazna napačno sprejete signalizacijske enote, ki jih ne potrjuje. Oddajna točka poskrbi, da se po izteku časovnika izgubljene oziroma napačno sprejete signalizacijske enote ponovno pošljejo.

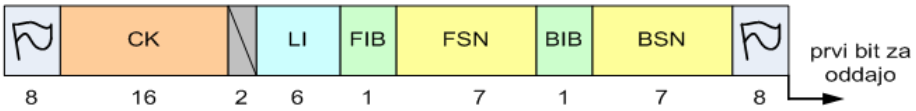
MTP2 sloj skrbi za povezavo in prenos signalnih enot le do naslednje signalizacijske točke po eni sami povezavi in nima nobene redundance. Dosegljivost vsake vzpostavljene logične povezave se spremlja tudi v času, ko se po povezavi ne pošilja nobenih sporočilnih signalnih enot. Namesto sporočilnih signalnih enot se takrat pošilja prazne signalizacijske enote FISU, ki zagotavljajo neprekinjeno sinhronizacijo in nadzor dosegljivosti in merjenje stopnje napak.

Ena fizična povezava se navadno deli na več logičnih kanalov/povezav. Za primer ima E1 povezava 32 kanalov s hitrostjo 64kbit/s, skupaj torej 2048 kbit/s. MTP2 nadzoruje eno samo logično povezavo. Če je na povezavi več logičnih povezav namenjenih signalizaciji, je potrebno prav toliko MTP2 procesov, med njimi pa MTP3 sloj avtomatično razdeljuje promet.

Signalizacijske in druge informacije se prenašajo preko signalizacijske povezave v okvirjih imenovanih signalizacijske enote (SU - signal units). Signalna enota je sestavljena iz različno dolgega informacijskega, oziroma sporočilnega polja. Lahko prenaša informacijo uporabnika ali informacijo signalizacijske povezave, v tako imenovanem statusnem polju. Poleg tega vsebuje določeno število parametrov različnih dolžin, ki vsebujejo podatke za nadzor prenosa sporočil.

FISU (Fill-In Signal Unit)

Signalizacijske enote FISU so najenostavnejše enote na MTP2 nivoju. Prenašajo se med delovanjem, ko ni drugih signalnih enot. S tem zagotavljamo stalen bitni pretok in zasedenost povezave. V vsaki sprejeti FISU signalni enoti preverimo CK (ki je izračunan s Cyclic Redundancy Check - CRC) zaščitno kodo za odkrivanje napak, tako lahko hitro odkrijemo okvarjeno povezavo in jo odstranimo iz uporabe.



Slika 2.4: Vsebina FISU

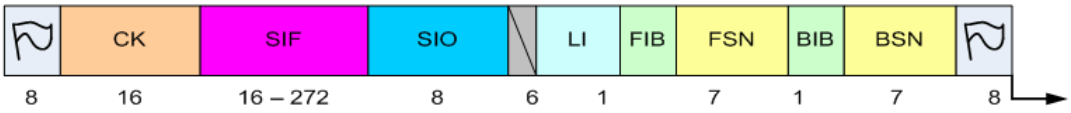
LSSU (Link Status Signal Unit)

Signalizacijske enote LSSU se uporabljajo za izmenjavo informacije o statusu sigalizacijske povezave med dvema sigalizacijskima točkama. Pošiljajo se med vzpostavitvenim uvrščanjem za kontrolo sigalizacijske povezave.

Slika 2.5: Vsebina LSSU

MSU (Message Signal Unit) sigalizacijske enote.

MSU so namenjene za prenašanje informacij iz višjih nivojev. Sporočilo lahko vsebuje sigalizacijske informacije iz tretjega nivoja MTP (MTP3) ali sigalizacijske informacije od uporabnikov na višjih slojih (TUP, ISUP, SCCP). Tip uporabnika 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 2.6: Vsebina MSU

Tretji sloj - MTP3

MTP3 sloj skrbi za pravilno dostavo in usmerjanje SS7 signalnih enot uporabniških slojev, za pravočasno zaznavo napak na omrežju ter temu ustrezno reakcijo. Za pravilno delovanje mora imeti MTP3 pregled nad vsemi logičnimi signalnimi povezavami ter na podlagi njihovega statusa, ki mu ga sporoča MTP2 sloj, odločati po kateri logični signalni povezavi sporočilo poslati.

Dve signalni točki sta lahko neposredno povezani z več logičnimi signalnimi povezavami. Če sta povezavi tudi fizično ločeni, govorimo o redundanci oziroma povečani zanesljivosti, saj v primeru, da se ena od fizičnih povezav prekine, signalni promet prevzame druga povezava.

MTP3 krmili preusmerjanje sigalizacijskega prometa z okvarjenih signalnih povezav ali smeri na sigalizacijske povezave ali smeri brez okvar. Krmili tudi porazdelitev obremenitve na signalnih povezavah in smereh.

2.1.4 Uporabniški del za digitalno omrežje integriranih storitev

Uporabniški del za digitalno omrežje integriranih storitev (Integrated Services Digital Network User Part - ISDN User Part) predstavlja postopke in protokole , ki se uporabljajo za vzpostavitev, upravljanje in rušenje zvez. Zveze med uporabniki ISDN omrežja omogočajo prenos podatkov ali govorno komunikacijo. Pred ISUP 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 signalizacijskih 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 nivoja. 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 se glede na funkcije delijo v skupine).

Vzpostavitev zveze med dvema končnima točkama omrežja, vzemimo na primer med centralama ISDN, v grobem poteka na sledeč način:

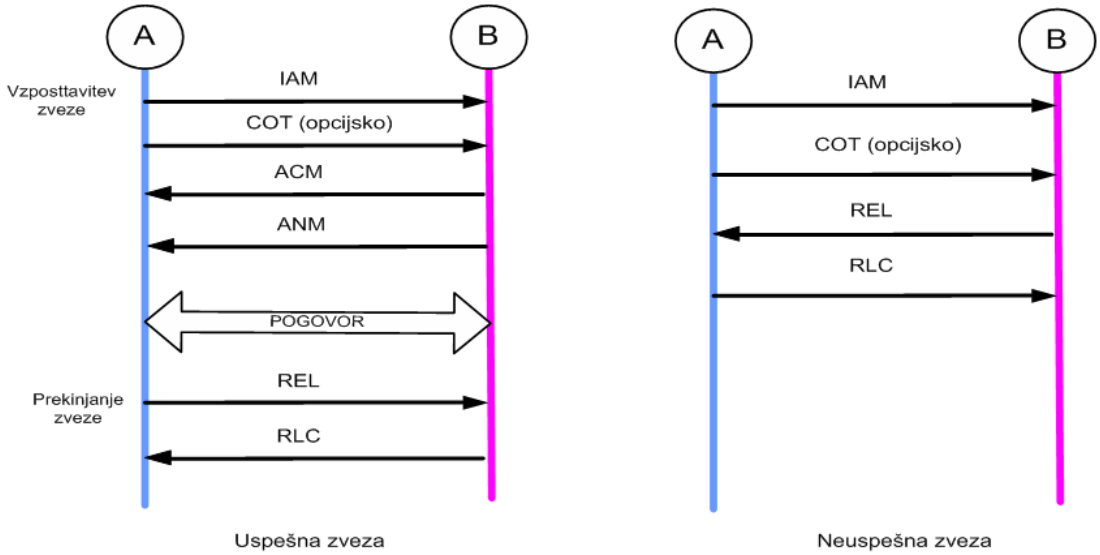
1. Klicoča stran (izvorna signalizacijska točka) pošlje začetno naslovno sporočilo (Initial Address Message, IAM) sosednji centrali na poti k centrali, na katero je priključen pozvani naročnik. Vsaka vmesna centrala pošlje IAM sporočilo do naslednje centrale v zvezi, glede na klicano naročniško številko v ISUP sporočilu in 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 ob oddaji IAM sporočila. 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 cen-

trala 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 - REL). Prekinitveno sporočilo se pošilja tudi v primeru zasedenega naročnika. Vsaka centrala po prejemu RCM sprosti zasedene kanale, izvorna centrala pa preneha s tarifiranjem.



Slika 2.7: Potek sporočil pri ISUP klicu

2.2 Omrežja nove generacije

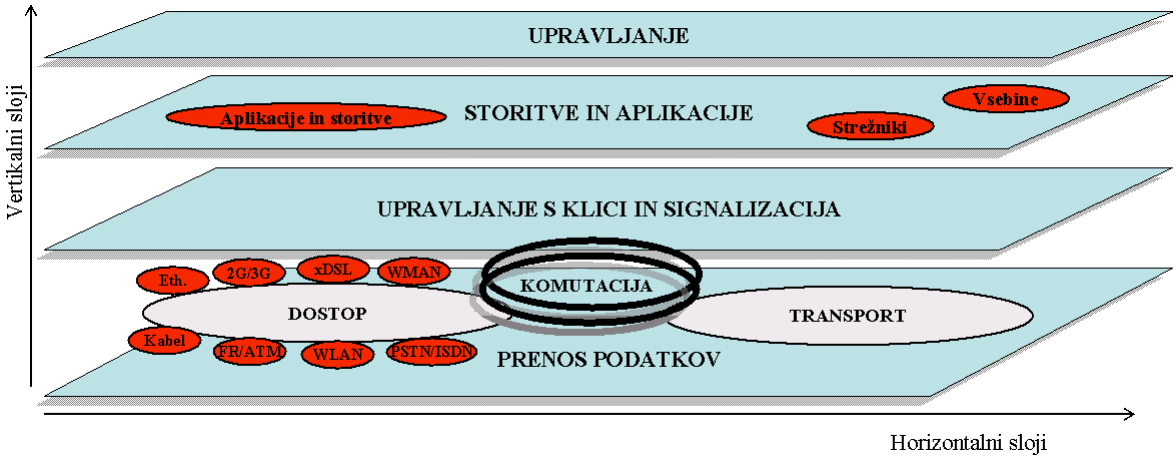
Omrežje nove generacije (Next Generation Networks - NGN) je koncept načrtovanja in vzpostavitve telekomunikacijske infrastrukture, ki na osnovi formalne separacije v različne sloje ter uporabe odprtih vmesnikov nudi ponudnikom storitev in operaterjem platformo, ki se lahko postopoma razvija, s ključnim ciljem ustvarjanja, vpeljave in upravljanja inovativnih storitev.

Telekomunikacije so v zadnjem času doživele korenite spremembe. Količina digitalnega prometa je izredno narasla, meje med do sedaj ločenimi govornimi in podatkovnimi omrežji so vedno manj izrazite. Uporabniki postajajo čedalje bolj zainteresirani za uporabo komunikacijsko in predstavnostno naprednejših storitev, deregulacija telekomunikacijskega trga pa je uvedla odprto konkurenco med operaterji in ponudniki storitev.

Koncept načrtovanja in gradnje NGN telekomunikacijske infrastrukture se od klasičnih, danes uveljavljenih telekomunikacijskih sistemov ločuje v več pogledih:

- arhitektura je slojevita in jasno ločuje sloj prenosa podatkov, sloj nadzora klicev in signalizacije, aplikacijski in storitveni sloj ter upravljavski sloj;
- uporablja podatkovno osnovano širokopasovno paketno transportno in komutacijsko infrastrukturo; vsesplošna prisotnost IP omrežij je danes odlično izhodišče za vzpostavitev tovrstnih sistemov;
- novi so omrežni elementi: klicni strežniki, aplikacijski strežniki, signalizacijski in medijski prehodi, medijski strežniki, različni NGN terminali;
- pojem komuniciranja je razširjen in predstavlja preplet različnih tehnologij in predstavnostnih principov ter združuje govorne, podatkovne in video komunikacije v enotno večpredstavnostno komunikacijsko platformo, ki deluje nad skupno širokopasovno transportno infrastrukturo na transparenten način;
- nudi odprto, skalabilno, standardizirano okolje za načrtovanje, vpeljavo in upravljanje vsakršnih storitev (t.j. storitveni aplikacijski programski vmesniki za storitve (znane ali še ne znane), ki uporabljajo kakršen koli medij, avdio, vizualni, s kakršnimi koli kodnimi shemami in podatkovnimi storitvami),
- dobro definirane funkcionalne entitete nadzorujejo politiko delovanja, seje, medij, vire, zagotavljanje storitev, varnost, ipd.,

- zagotovljeno je medsebojno delovanje NGN in obstoječih govornih in podatkovnih sistemov preko ustreznih prilagodilnih elementov;
- omogoča podporo za obstoječo in novo terminalno opremo;
- skrbi za širokopasovnost, mobilnost, personalizacijo, varnost in prilagodljivo kakovost storitev.



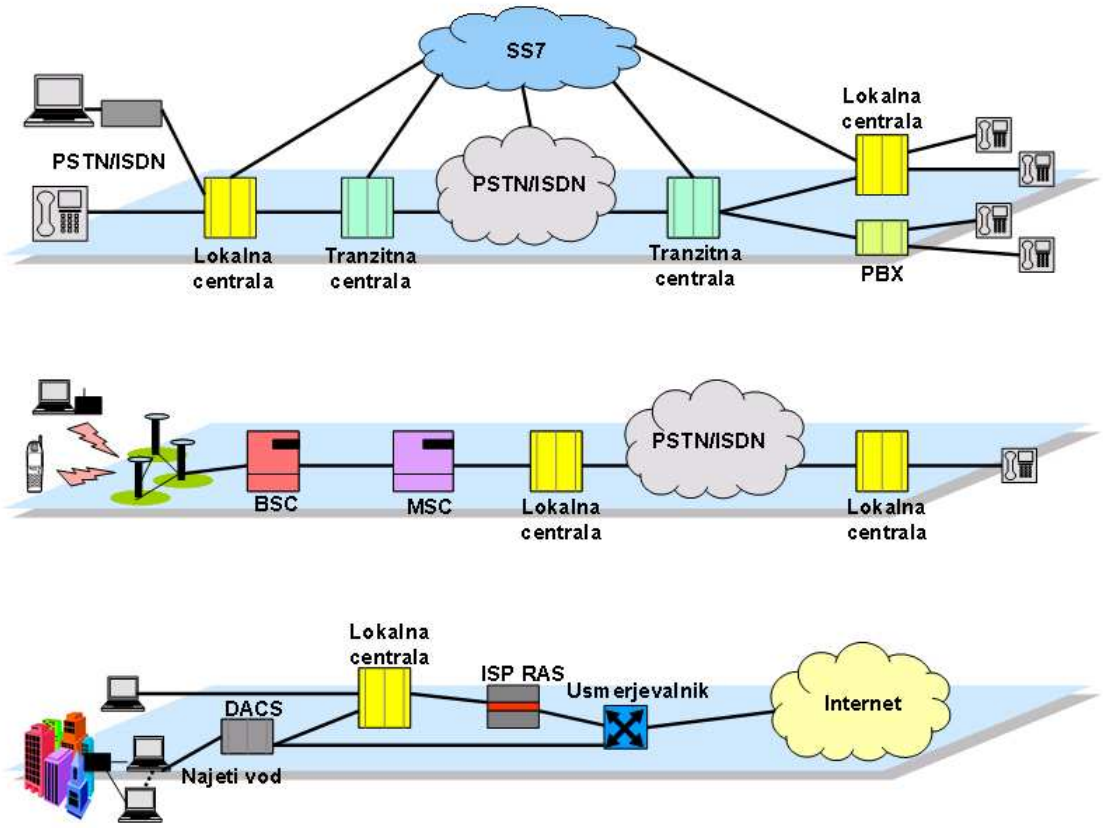
Slika 2.8: Koncept omrežij nove generacije

Današnji telekomunikacijski sistem je zgrajen iz niza vzporednih, nepovezanih omrežij, ki jih lahko razdelimo v dve skupini:

- tokokrogovno komutirana telefonska omrežja (PSTN/ISDN in mobilna omrežja),
- paketno komutirana podatkovna omrežja. (angl. Public Switched Data Network - PSDN).

Situacijo ponazarja Slika 2.9.

Govorno omrežje je tipične mrežne konfiguracije preklopnih vozlišč in pristopnih točk, povezanih v dostopovno omrežje, z višje ležečim signalizacijskim sistemom SS7. Podatkovno omrežje je od govornega v celoti ločeno. Sorazmerno



Slika 2.9: Današnja nepovezana omrežja

manjša podatkovna omrežja danes izkazujejo izjemno rast, kar je rezultat interneta, intranetov, navideznih zasebnih omrežij (VPN) in oddaljenega dostopa.

Tradicionalna omrežja, v obliki, kot je današnja, se niso spremenila že dalj časa. Problematika takšne ureditve je dejstvo, da je večino rasti prometa zaznati v podatkovnem omrežju, večina dohodka pa je na strani govornega omrežja. Pri tem sta oba tipa omrežij nefleksibilna, nadgradnja in migracija med obema tipoma pa je zahtevna.

Omrežja naslednje generacije transparentno združujejo tokokrogovno komutirana omrežja ter paketno komutirana omrežja v enoten večstoritveni sistem, ki združuje in izkorišča prednosti obstoječih ločenih omrežij.

Tako imenovana paketizacija omrežij omogoča uspešno konvergenco prenosa

različnih tipov informacij v enotno omrežje. Signalizacija poteka preko namenskih strežnikov, nosilni promet, govor, podatki in video pa potekajo po nosilnih povezavah v paketnem omrežju.

Postopnost migracije omogoča, da se prehod na IP platformo zgodi v vseh segmentih sočasno. Za to so namenjeni ustrezni mejni omrežni elementi, ki poskrbijo za translacijo metod in procedur ter s tem omogočajo kompatibilnost ne glede na znatno spremenjen način delovanja dela sistema. Migracijske in konverzijske storitve, ki omogočajo prehod obstoječega omrežja na novo IP platformo, so ključne. Stare storitvene tehnologije so pogosto osnovane na tokokrogovni SS7 storitveni logiki. Procedura konverzije prilagodi uporabniško vsebino storitvene logike IP računalniški platformi z ustreznim protokolom za krmiljenje seje.

Najbolj težaven segment je upravljanje. Ta del je kritičen tako s storitvenega kot tudi s poslovnega vidika in mora ustrezno delovati ne glede na tekoče in občasne spremembe v vseh ostalih delih omrežja. Iz tega razloga ima upravljanje v omrežjih naslednje generacije pomembno vlogo, obenem pa ostaja to tudi področje najobsežnejših raziskovalnih in razvojnih aktivnosti na področju VoIP. V fazi migracije kompleksnost sistema narašča, tako s stališča enotne zasnovanosti posameznih segmentov kot tudi s stališča števila in načina izrabe različni tehnologij, ki so v omrežju sočasno prisotne. Cilj po opravljeni migraciji je doseči ponovno stanje manjše kompleksnosti ter s tem večjo obvladljivost in stabilnost sistema.

2.2.1 Telefonija

IP telefonija je ena ključnih storitev v omrežjih naslednje generacije. Telefonija se v celoti ali delno prenaša prek paketnega omrežja IP in ne več prek omrežja TDM. Pogosto se uporabniki sploh ne zavedajo, da je njihov telefonski klic usmerjen prek omrežja IP, kjer opravi večino poti. Promet IP lahko poteka prek javnega Interneta ali pa je razvit na zasebnih omrežjih IP. Uporaba paketne komutacije prinaša

mnoge prednosti. Govor v obliki paketov IP pošiljamo prek omrežja le takrat, ko je potrebno, torej ko kličoči govori. Poleg učinkovitosti paketne komutacije k temu spada tudi krajši čas vzpostavitve povezave med dvema sistemoma, kar zmanjša obremenitev omrežja. Obe komunicirajoči strani sta prosti, da poleg govora oddajata ali sprejemata tudi druge informacije.

2.2.2 Elementi omrežja

Pri izvedbi omrežij NGN nastopa več elementov, ki se lahko pojavljajo kot samostojne naprave ali kot poljubna kombinacija v integrirani napravi. Pomembnejši elementi omrežja NGN so: medijski prehod (MG), signalizacijski prehod (SG), klicni strežnik ter različni aplikacijski oz. storitveni strežniki. Komunikacija v omrežjih NGN temelji na dveh sistemih: H.323 in SIP.

Medijski prehod (MG) je naprava, prek katere lahko terminali iz TDM omrežja komunicirajo s terminali v omrežju IP. MG 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 NGN so medijski prehodi ključnega pomena. Omogočajo povezljivost različnih dostopovnih omrežij in hrbteničnega paketnega omrežja in s tem uporabo storitev neodvisno od dostopovnega omrežja. Naprava, ki vključuje medijski in signalizacijski prehod se navadno imenuje prehod IP.

Signalizacijski prehod (SG) je naprava, prek katere si terminali iz omrežij TDM in IP z različnimi signalizacijskimi protokoli izmenjujejo signalizacijska sporočila. Kjer poteka signalizacija ločeno od toka podatkov, izvorni terminal pošilja signalizacijska sporočila (npr. zahteve za vzpostavitev ali rušenje zveze, potrjevanje ipd.) signalizacijskemu prehodu, ta jih pretvori v protokol drugega omrežja in pošlje ponornemu terminalu. Signalizacijski prehod ima podobno vlogo kot medijski, le da prenaša signalizacijska sporočila in ne samih podatkov. Naprava, ki vključuje medijski in signalizacijski prehod, se navadno imenuje pre-

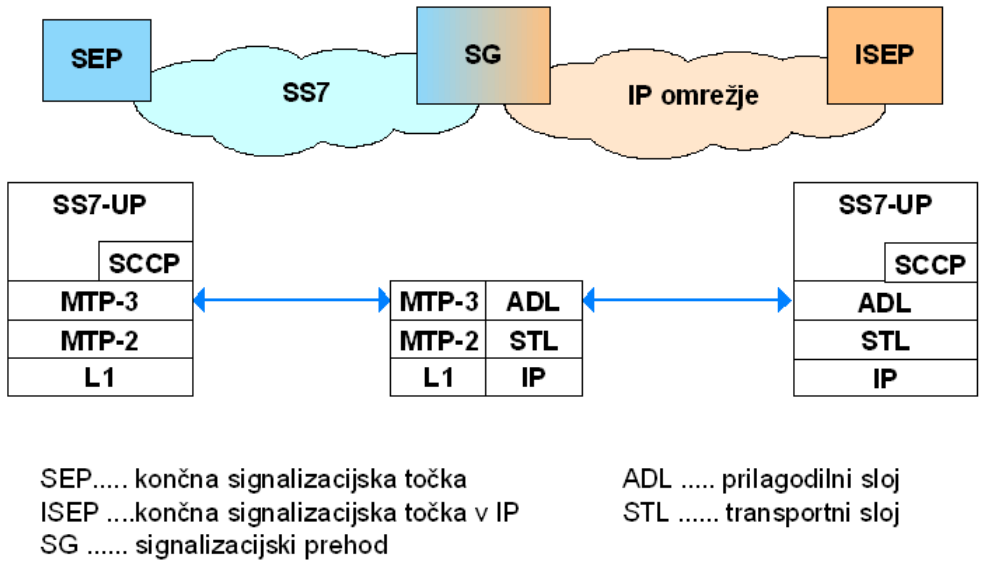
hod IP.

V arhitekturi NGN vloga **klicnega strežnika** ni povsem natančno definirana. Z vidika omrežij TDM opravlja klicni strežnik podobne funkcije kot telefonska centrala v omrežju TDM, pri čemer navadno skrbi le za osnovne "telefonske" funkcije. Z vidika omrežij IP, opravlja klicni strežnik funkcije, kot so kontrola klicev, upravljanje s pasovno širino, omejevanje vzpostavljanje sej in podobno, kar je ekvivalentno vratarju v sistemu H.323 oz. proxy strežniku v sistemu SIP. Kompleksnejše funkcije, ki se tičejo izvajanja telekomunikacijskih storitev so v omrežjih NGN v domeni aplikacijskih in storitvenih strežnikov. Zaradi interoperabilnosti z obstoječimi telekomunikacijskimi sistemi danes večina izvedb omrežij NGN temelji na integriranih klicnih strežnikih, ki so kombinacija klasičnih telefonskih central z dodano funkcionalnostjo IP.

2.3 Transport signalizacije SS7

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 [9]. Delovna skupina SIGTRAN, ki je ta opis izdelala, posebno pozornost posveča prenosu signalizacije med signalizacijskim prehodom (SG) in krmilnikom prehodov (MGC). Vloga krmilne enote in njena pozicija v omrežju bo natančneje razložena v poglavju 1. Signalizacijski prehod je postavljen med omrežje z SS7 ter omrežjem z IP in je ko tak ključnega pomena za povezavo SS7 omrežij z omrežij naslednje generacije. Signalizacijski prehod zaključuje transportne protokolne sloje (MTP1 - MTP3) na strani SS7-omrežja, vendar ne izvaja funkcij uporabniških slojev SS7. Uporabniški sloji SS7 (na primer ISUP) se nahajajo v končnih signalizacijskih točkah (Signaling End Point, SEP) omrežja SS7 in IP. SEP v omrežju IP imenujemo internetna končna signalizacijska točka ISEP, ki lahko predstavlja MGC, krmilno enoto navideznega stikala (klicni strežnik), podatkovno bazo ali na IP

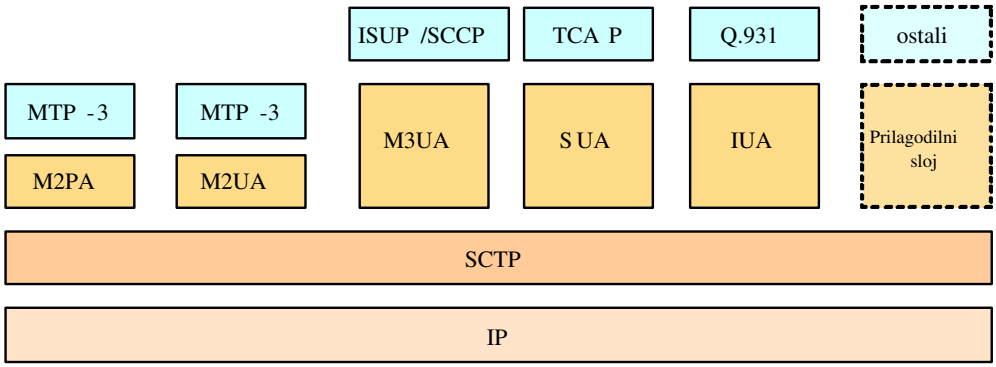
osnovano storitveno krmilno točko SCP. Vsaka ISEP je zaradi zanesljivosti in porazdeljevanja prometne obremenitve signalnih vodov lahko povezana z več signalizacijskimi prehodi. V tem primeru signalizacijski prehod s stališča SS7 deluje kot storitvena transportna točka (STP), končna signalizacijska točka v internetnem omrežju pa kot ena od SEP signalizacijskega omrežja številka 7.



Slika 2.10: Potek sporočil pri ISUP klicu

Prilagodilni sloji so definirani tako, da ostane prenos signalizacije prek IP skrit za višje protokolne sloje. To pomeni, da se na primer pri prenosu ISUP-sporočil prek IP-omrežja, protokol ISUP in njegov vmesnik do nižjih protokolnih skladov ne spremenita. Glede na vrsto signalizacije, pozicijo v arhitekturi SS7/IP in področje uporabe ločimo različne prilagodilne sloje. Slika 2.11 prikazuje protokolno arhitekturo, na kateri je predstavljenih nekaj od prilagodilnih slojev. Prilagodilni sloj M3UA (MTP-3 User Adaptation Layer) zagotavlja vse potrebne funkcije MTP-3 sloja, ki jih zahtevajo MTP-3 uporabniški protokoli (ISUP, SCCP), M2UA (MTP-2 User Adaptation Layer) pa nadomešča MTP-2 sloj SS7 protokolne arhitekture. IUA (ISDN Q.921 User Adaptation Layer) se uporablja za prenos Q.931 uporabniške signalizacije na D-kanalu ISDN vmes-

nika do aplikacije v IP svetu. Vsi trije prilagodilni sloji, M2UA, M3UA in IUA uporabljajo storitve SCTP sloja.



Slika 2.11: Protokolni sklad SIGTRAN

2.3.1 Protokol za nadzor prenosa pretokov - SCTP

Tako TCP, kot UDP ne izpolnjujeta strogih zahtev signalizacijskih protokolov in nista najbolj primerna kandidata za protokol transportnega sloja STL. Zaradi tega je bil v delovni skupini SIGTRAN razvit protokol SCTP (Stream Control Transmission Protocol), katerega transportne lastnosti so prilagojene zahtevam STL.

TCP-protokol igra danes ključno vlogo zanesljivega prenosnega protokola v internetnih omrežjih, vendar za že omenjene aplikacije prenosa signalizacije preko IP, TCP ne nudi zadostne podpore in je preveč omejen. Med omejitvami TCP-protokola izstopajo:

- Zakasnitve zaradi blokade sporočilne vrste, ki so posledica strogega ohranjanja zaporednosti poročil. TCP zagotavlja zanesljiv prenos in dostavo podatkov višjemu protokolnemu sloju v pravilnem zaporedju glede na njihovo oddajo. Določeni uporabniški sloji sicer zahtevajo zanesljiv prenos, obenem pa jim ustreza sekvenčno neurejen ali delno urejen prenos protokolnih po-

datkovnih enot. Blokada nastane zlasti v primerih, ko se je del sporočila izgubil, saj TCP čaka na potrditev prejema.

- Pretočno 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.

- 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 (OS); največje število hkratnih zvez TCP določeno z omejitvami jedra OS.

- Nezmožnost aplikacije, da krmili inicializacijo TCP-protokola ter posega v nastavitve časovnikov.

Zaradi omejitve TCP je bila edina rešitev za premoščanje zgornjih problemov uporaba UDP protokola z zagotavljanjem zanesljivega in urejenega prenosa na višjih (aplikacijskih) protokolnih slojih. Protokol, ki bi uspešno premostil naštete probleme, bi moral združevati lastnosti TCP in UDP-protokolov transportnega sloja iz česar so izhajali avtorji protokolov RUDP (Real-time UDP) ter MDTP (Multi-protocol Datagram Transport Protocol). Slednji je vzbudil pozornost SIGTRAN delovne skupine pri IETF, ki ga je preimenovala v SCTP in dopolnila do današnje različice. SCTP nudi svojim uporabnikom naslednje storitve:

- prenos uporabniških podatkov brez napak in podvajanja,

- razstavljanje uporabniških podatkovnih enot za prilagoditev na dovoljeno velikost MTU,

- zaporedna dostava uporabniških sporočil znotraj več pretokov z možnostjo dostave posameznih sporočil v vrstnem redu sprejema,

- združevanje več različnih uporabniških sporočil v en SCTP paket,
- podpora večdomnosti na enem ali obeh koncih SCTP zveze za povečano odpornost na napake v omrežju.

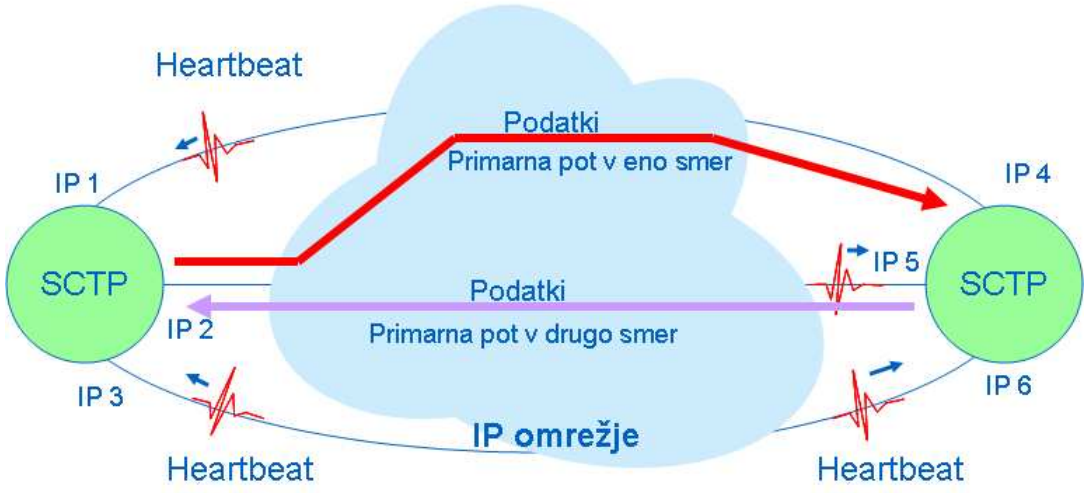
SCTP omogoča prenos sporočilno oblikovanih signalizacijskih informacij prek omrežij z internetnim protokolom. V protokolni arhitekturi TCP/IP se uvršča na transportni sloj, poleg TCP in UDP protokolov, torej neposredno nad IP.

SCTP omogoča prenos sporočilno oblikovanih signalizacijskih informacij prek omrežij z internetnim protokolom. V protokolni arhitekturi se uvršča na transportni sloj poleg TCP in UDP protokolov, torej neposredno nad IP. Obstoječi signalizacijski protokoli lahko dostopajo do storitev protokola SCTP preko ustreznih prilagodilnih slojev. Prilagodilne aplikacije so uporabniki storitev sloja SCTP, v nadaljevanju jih bomo imenovani kar SCTP uporabniki. Prilagodilni sloji krmilijo in upravljajo s transportnim protokolom, tudi s protokolom SCTP. Slednji pa ni omejen le na prenos klasične signalizacije prek IP, temveč lahko ponudi svoje storitve tudi IP signalizacijskim protokolom in drugim aplikacijam.

SCTP nudi zanesljiv in strukturiran - časovno urejen - prenos uporabniških sporočil med istoležnimi uporabniki SCTP. Protokol deluje na potencialno nezanesljivih nepovezavnih paketnih storitvah, kakršne nudi IP. Protokol uporablja kontrolne vsote (checksums) in sekvenčne številke za odkrivanje napak ter mehanizme selektivne ponovitve prenosa za popravljanje le-teh. Čeprav je povezavno usmerjen protokol, je koncept SCTP-povezave (ang. association) širši od TCP-zveze. SCTP-povezava je protokolno razmerje med dvema SCTP-končnima točkama z informacijami o stanju protokola. Vsaka od dveh SCTP končnih točk pošlje drugi končni točki povezave številko SCTP-vrat in listo IP-naslovov. Vsaka povezava je določena z dvema številkama vrat in dvema listama IP-naslovov. Za razliko do TCP, pri katerem je podatkovni pretok oktetno usmerjen, SCTP prenaša podatkovne sklope v SCTP-storitvenih protokolnih enotah (SSPE), originalno imenovanih čhunks". SCTP storitvene protokolne enote

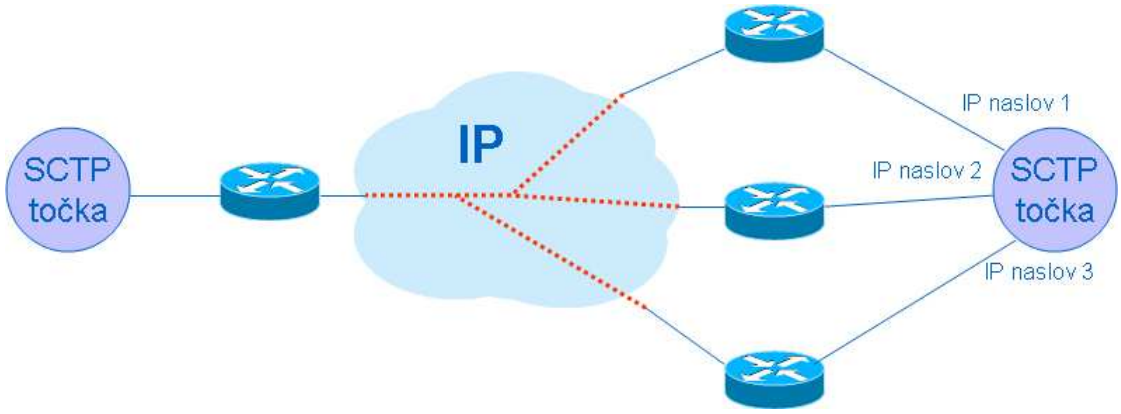
vsebujejo uporabniške podatke ali krmilne informacije. Protokol SCTP se je sposoben prilagoditi največji prenosni enoti (Maximum Transfer Unit, MTU) nosilne poti, to pomeni da določi največjo velikost protokolne podatkovne enote, pri kateri se IP-paketi pošljejo na ponorno točko brez razstavljanja v manjše enote. SCTP velika sporočila razstavi v SSPE, ki po velikosti ustrezajo prenosu v takih IP-paketnih. Kratka sporočila tvorijo majhne SSPE, ki se lahko sestavljajo v en IP-paket.

TCP ima strogo shemo urejanja zaporednosti dostavljenih podatkov na povezavo. SCTP ima bolj prilagodljivo shemo dostave sporočil, ki v okviru ene SCTP-povezave ločuje različne sporočilne pretoke (ang. streams). Ločevanje med sporočilnimi pretoki 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 mehanizem, ki omogoča posredovanje sporočila uporabniku, takoj ko je bilo to sprejeto v celoti (ang. order-of-arrival delivery).



Slika 2.12: Krmiljenje pretoka

Krmiljenje pretoka in zamašitev sta bila načrtovana tako, da se SCTP-promet obnaša podobno kot TCP-promet. S tem se poenostavi uvajanje SCTP-storitev v obstoječa IP-omrežja. Prednost SCTP pred TCP je podpora tako imenovanih večdomnih gostiteljev. Večdomni gostitelji so vozlišča oziroma SCTP-končne točke, ki so dosegljive na več IP-naslovih. TCP-zvezo določa par transportnih naslovov (IP-naslov in številka vrat). Pri SCTP vsaka stran povezave ponudi drugi strani listo večih IP-naslovov v kombinaciji z eno številko SCTP-vrat. Velja, da vsako končno točko SCTP določa kombinacija niza razpoložljivih ponornih in izvornih transportnih naslovov. Transportni naslovi posameznih končnih točk morajo biti pri tem unikatni.



Slika 2.13: Večdomnost končnih točk

SCTP-povezava se razširja med vsemi možnimi izvornimi/ponornimi kombinacijami med dvema končnima točkama. Vsaka večdomna končna točka je s tem z danega vozlišča dosegljiva prek več različnih poti. Krmilni del SCTP protokolnega sklada nadzira stanje vsake od teh poti z opazovanjem dosegljivosti, zakasnitve in števila zahtev po ponovnih prenosih sporočil. Opazovanje poti, ponavljanje prenosov po alternativnih poteh in izbira poti glede na njihovo trenutno stanje znatno povečajo robustnost SCTP-protokola na delne izpade v omrežju glede na TCP. Opisane lastnosti obenem povečujejo odpornost na naključne napade (obstreljevanje s prometom).

2.3.2 Prilagoditveni sloji

Kot primer prilagodilnega sloja si nekoliko podrobneje oglejmo M3UA. Zanesljiv transportni sloj ni zadosten pogoj za doseganje visoke zanesljivosti signalizacijskega omrežja. Le-ta se običajno zagotavlja s porazdeljeno arhitekturo in vnašanjem redundance tako na nivoju signalizacijskih vodov kot na nivoju signalizacijskih vozlišč (STP v omrežju SS7). Prenos SS7 signalizacijskih protokolnih sporočil prek IP mora ohraniti podobno strukturo omrežja.

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 (Stream Control Transmission Protocol), ki predstavlja zanesljiv nižje ležeči signalni transportni protokol.

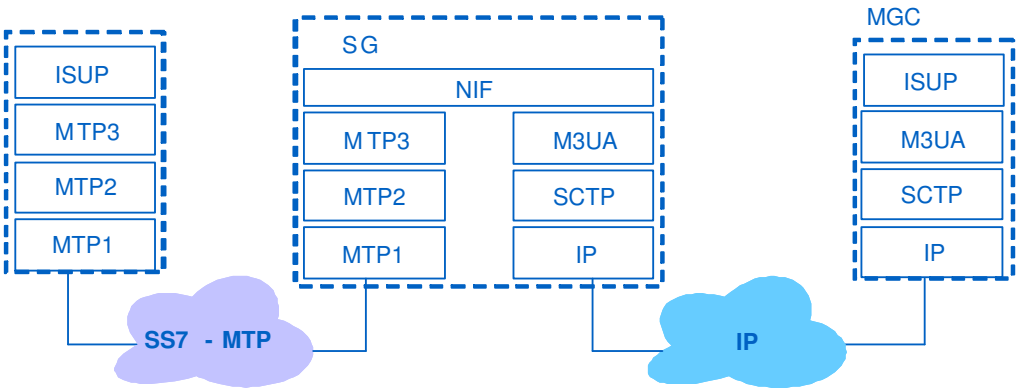
M3UA sloj zagotavlja ekvivalenten nabor primitivov višje ležečim uporabniškim slojem enakovredno kot MTP3 sloj svojim lokalnim MTP3-uporabnikom v SS7 signalni končni točki SEP (Signalling End Point).

Protokol M3UA protokolom višjih - uporabniških slojev SS7 zagotavlja transparentne storitve IP omrežnega sloja. M3UA sloj v aplikacijskem storitvenem procesu to zagotovi 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 sigalizacijskem prehodu.

Po drugi strani se tudi MTP3 sloj v sigalizacijskem prehodu ne zaveda, da so navidezno lokalni uporabniki dejansko oddaljeni uporabniki na različnih gostiteljih. M3UA razširja storitve MTP3 do oddaljenih uporabnikov v internetnih omrežjih, pri tem pa sam ne izvaja funkcij MTP3.

M3UA sloj se lahko uporablja tudi v primeru točka-točka (point-to-point) sigalizacijske 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 MTP3 niso ponujene oddaljeno preko sigalizacijskega prehoda SG, saj zaradi poenostavljene povezave točka-točka dveh IPSP te storitve zagotavlja že podnabor MTP3 procedur.



Slika 2.14: Vloga M3UA protokola

2.4 SIP

Protokol za zagon seje (ang. SIP - Session Initiation Protocol) je signalizacijski, peer-to-peer (vsak z vsakim) protokol za vzpostavljanje oziroma kontrolo multimedijskih sej. Zagotavlja vzpostavitev govorne, video ali druge komunikacije ter pošiljanje sporočil med napravami. Na začetku se je uporabljal predvsem v internetni telefoniji, potem pa se je uporaba razširila na mnoga nova področja. SIP omogoča vzpostavljanje individualnih ali konferenčnih zvez, videokonferenc in točka-točka video zvez, mrežno sodelovanje (ang. Web collaboration) in klepete, ter pošiljanje hipnih sporočil (ang. Instant Messaging) med več SIP končnimi točkami, kot so IP telefoni, osebni računalniki, dlančniki (PDA) in mobilni telefoni. Kot IETF standard se SIP vse bolj uveljavlja, saj omogoča uporabo IP omrežij novim operaterjem, predvsem zaradi ogromno različnih možnosti in fleksibilnosti pri gradnji konvergenčnih omrežij. V TDM omrežjih so funkcije in storitve zagotavljale centrale, pri SIP signalizaciji pa protokol prenaša nadzor komunikacije iz jedra omrežja proti uporabniškemu nivoju, ter tako odpira možnosti

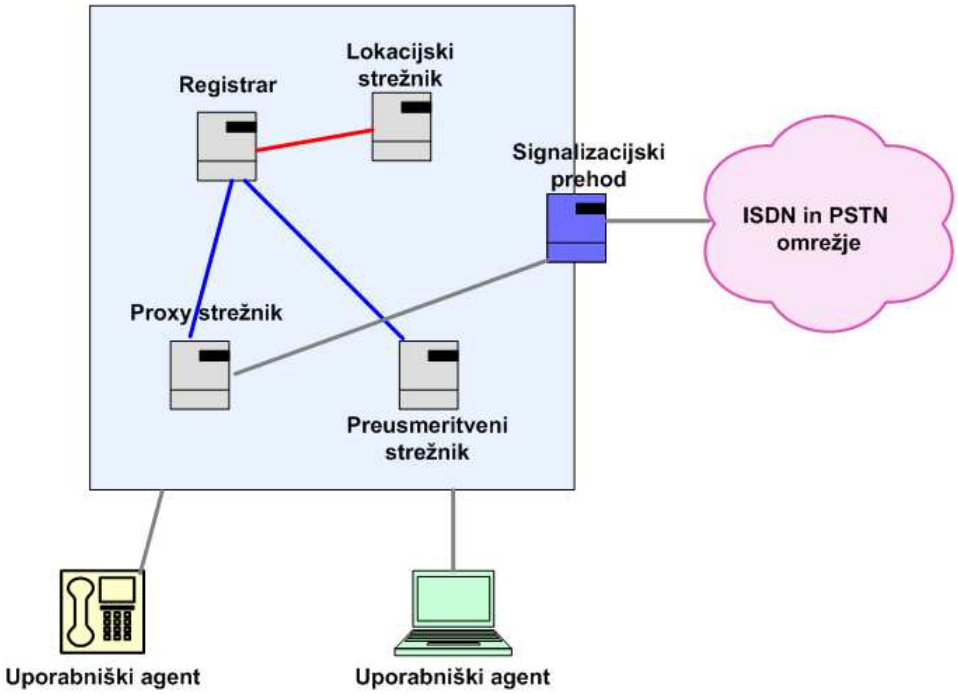
razvoja različnih aplikacij brez sprememb v centralah. Tako je neodvisnim razvijalcem programske opreme omogočen dostop na specifične trge telekomunikacij.

IETF je standard načrtoval tako, da so definirali osnovne funkcije za interoperabilnost in obenem pustili dovolj prostora za razlike na aplikacijskem nivoju. Vlogo SIP-a v konvergenčnih komunikacijah lahko primerjamo z vlogo HTTP protokola pri prenosu informacij v svetovnem spletu (ang. WWW - World Wide Web), saj uporabniku omogoča transparentnost komunikacijske infrastrukture in omogoča dostop do različnih načinov komuniciranja. Z uporabo URI (ang. Unified Resource Identifier) omogoča obravnavo zahtev za komunikacijo na enak način kot HTTP zahtevo, kar predstavlja naravno izbiro za uporabo pri komunikacijskih storitvah in aplikacijah. SIP skupaj z mnogimi drugimi standardi omogoča razvoj odprtih, zanesljivih in multimedijsko bogatih komunikacij. SIP lahko opišemo kot protokol aplikacijskega sloja OSI modela, ki v prvi vrsti skrbi za vzpostavitev, spreminjanje in prekinitev komunikacijskih sej. SIP omogoča precej več kot samo vzpostavitev telefonskih zvez.

Razširljiva zasnova omogoča tako pošiljanje hipnih sporočil preko tekstovnih kanalov, kot tudi mehanizem naročanja oziroma objavljanja informacije o prisotnosti ali dostopnosti. Po vzoru HTTP modela, tvori jedro protokola izmenjava tekstovnih zahtev (ang. request) in odgovorov (ang. response) direktno med končnimi točkami (peer-to-peer). SIP je razširljiv in omogoča vključevanje novih funkcij, na primer: izmenjavo zmožnosti vpletenih točk (ang. Capability Exchange), zahtevo za usmerjanje in preusmerjanje (ang. Request Routing and Rerouting) ali klic na več ponornih točk (ang. Forking). Komunikacija med končnimi točkami ni v celoti zagotovljena znotraj SIP protokola, temveč lahko uporablja tudi že uveljavljene omrežne protokole ter tehnologije aplikacijskega nivoja .

V skladu z IETF filozofijo uveljavljanja preprostih protokolov velikih zmogljivosti, SIP protokol temelji na arhitekturi peer-to-peer z majhnim naborom metod oziroma tipov sporočil. Sporočila in odzivi nanje so sorodni HTTP

sporočilom in se prenašajo preko UDP, TCP ali SCTP (ang. Stream Control Transfer Protocol) protokola. SIP sporočila v svoji glavi (ang. Header) nosijo informacijo o posamezni komunikacijski seji (naslovnik, pošiljatelj...), kot uporabniški del sporočila pa prenašajo SDP (ang. Session Description Protocol) informacijo, potrebno za vzpostavitev medijskih kanalov (tip medija, UDP vrata). Vzpostavitev signalizacijske seje lahko poteka preko različnih SIP strežnikov (proxy ali preusmeritveni) ali direktno, medtem ko se govorna povezava vzpostavi direktno med končnima točkama, naprimer preko RTP (ang. Real Time Protokol) protokola.



Slika 2.15: SIP arhitektura

2.5 SIP-T

Protokol za vzpostavljanje sej za telefonijo (SIP-T - ang. Session Initiation protocol for Telephones) je osnovan na protokolu SIP. Nadgrajuje ga s procedurami za povezavo omrežja IP s PSTN/ISDN, zato SIP-T poskrbi za prepustnost

lastnosti iz PSTN/ISDN. Uporabniki SIP telefonov lahko tako uporabljajo iste funkcije kot uporabniki telefonov, priključenih na PSTN-ISDN. Informacije SS7 morajo biti na voljo brez izgub, da se na točkah prehodov IP/PSTN/ISDN in obratno zagotovi prepustnost funkcionalnosti, ki jih SIP ne podpira. Usmerjanje v omrežjih SIP mora biti zagotovljeno tudi za klice iz PSTN/ISDN, zato mora imeti proxy SIP strežnik dovolj informacij, da klic usmeri do ponora. SIP-T poskrbi za omenjene funkcije z enkapsulacijo SS7 sporočil v telo sporočila SIP na prehodih PSTN/ISDN/IP ter s prevajanjem določene informacije iz sporočil SS7 ISUP v glavo SIP in tako omogoči usmerjanje sporočil SIP. Sporočilo SIP INFO uporabi za prenos informacij ISUP med klicem. Prenos sporočil SCCP (ang. Signalling Connection Control Part - Krmilni del signalizacijske zveze) in TCAP (ang. Transaction Capabilities Application Part - Aplikacijski del za transakcijske zmožnosti) ni podprt v SIP-T. Staro ime za SIP-T je bilo SIP-BCP-T (ang. SIP Best Common Practice for Telephony) ali še prej SIP +.

2.6 H.323

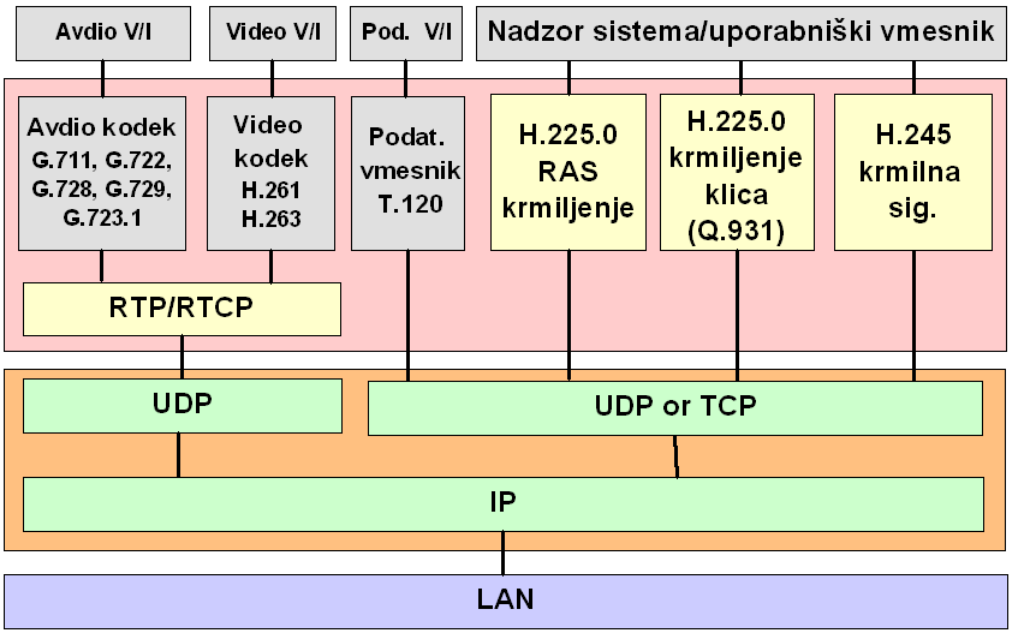
H.323 predstavlja enega od temeljnih standardov za vzpostavljanje povezav za prenos govora, slike in podatkov prek omrežij IP. Podaja več dokumentov za večpredstavne komunikacije prek omrežij, ki ne zagotavljajo kvalitete storitev, kar je značilno za večino današnjih lokalnih omrežij. Standard H.323 pokriva specifikacije za kodiranje zvoka in slike, kompresijo in dekompresijo medijskih tokov in s tem omogoča uporabo različnih večpredstavnostnih aplikacij.

Komunikacijski sistem H.323 tvorijo naslednje komponente: Terminali, ki predstavljajo končne točke v omrežju in prek katerih je možna dvostranska komunikacija v realnem času. Podpirajo zvočne ter opcijsko video in podatkovne komunikacije; Prehod (GW) je točka v omrežju, ki omogoča dvostransko komunikacijo v realnem času med terminali H.323 v paketnem omrežju in drugimi terminali v vodovnem omrežju oz. drugimi prehodi H.323. Prehod opravlja

funkcije prevajanja formatov in kodiranja, vzpostavljanja in sproščanja zvez ter komuniciranja s protokoli vodovnega omrežja. Prehod je neobvezen element v arhitekturi H.323.

Vratar (GK) izvršuje dve pomembni funkciji kontrole klica (po specifikaciji RAS), in sicer prevajanje naslovov med imeni terminalov in prehodov v LAN in naslovi IP ter upravljanje s pasovno širino. Vratar je neobvezen element v arhitekturi H.323. Večtočkovna kontrolna enota (MCU) je končna točka v omrežju, ki podpira večtočkovne povezave med tremi ali več terminali ali prehodi. Obstaja več različic protokola H.323, in sicer: H.323v1, H.323v2, H.323v3 in H.323v4. Prva različica podpira predvsem komunikacije prek lokalnih omrežij, druga pa delovanje prek večjih paketnih omrežij (Internet in WAN), s podporo za varnost, skalabilnost, uporabo alternativnih vratarjev in dodatne storitve. Tretja različica izboljšuje integracijo s telefonskimi omrežji ter skalabilnost. V okviru četrte različice je dodatno povečana skalabilnost, uvedene dodatne storitve (podpora storitvam prek protokola HTTP, izboljšane klicne funkcije), opredeljene zahtevane funkcije (poročila o uporabi, identifikacija klicočega, izboljšane telefaks storitve) ter uvedeno ogrodje, ki omogoča razširljivost standarda z novimi funkcijami.

Medijski tok se v okviru standarda H.323 prenaša s pomočjo protokola RTP prek UDP. Prvi skrbi za prenos dejanske vsebine, drugi pa za krmilne informacije. Signalizacija H.323 poteka prek protokola TCP ob souporabi protokolov RAS (za registracijo, dostop in stanje), Q.931 in H.245 (za posredovanje pri uporabi kanala in kapacitete). Tuneliranje signalizacije se izvaja preko sporočil H.225. Podprto je tudi tuneliranje signalizacije SS7 preko protokola H.323 Annex M, z dopolnilnimi storitvami CCBS, CCNR in AOC, ter funkcionalnostjo izločanja tišine (VAD) za vsak profil H.323 (Trunk Group). Poleg tega je podprt prenos dvotonske večfrekvenčne signalizacije - (DTMF) "In-band"in Out-of-band preko signalizacije H.323, posebno v primeru uporabe komprimiranih kodekov.



Slika 2.16: Protokolni sklad H.323

2.7 MGCP

MGCP je protokol tipa odjemalec - strežnik in predvideva že znano arhitekturo krmiljenja klica s centralizacijo funkcij krmiljenja klica v krmilni enoti ali klicnem agentu (MGCP poimenovanje). Klicni agent uporablja MGCP za krmiljenje objektov v prehodu, ki ima omejeno funkcionalnost. Model zveze, na katerem je zasnovan protokol, uvaja pojma končna točka in povezava. Končna točka je definirana kot izvor ali ponor prometa. Lahko ima fizičen značaj (vmesnik na tranzitnem prehodu za povezavo na stikalo PSTN, naročniška zanka na rezidenčnem prehodu za priključevanje analognih telefonov ali vmesnik na dostopovnem prehodu za priključevanje PBX) ali je navidezne narave (na primer strežnik avdio vsebine).

Protokolna specifikacija definira povezave s topologijo tipa točka-točka ali večtočkovne povezave. Povezave so logične zveze med končnimi točkami in so lahko vzpostavljene prek različnih transportnih omrežnih tehnologij, kot so

ATM ali IP. V tehnologijah VoIP je povezava objekt protokola MGCP, ki modelira prenos medijske vsebine po kanalu RTP/UDP/IP. Princip končnih točk in povezav služi vzpostavitvi medijskih pretokov med vmesniki prehoda, princip signalov in dogodkov pa vzpostavitvi in rušenju zvez in krmiljenju nosilcev. Koncept dogodkov in signalov je ključnega pomena za delovanje krmilnega protokola. Protokol krmilni enoti omogoča detekcijo dogodkov in predvajanje signalov na posameznih končnih točkah. O nastopu dogodkov, za katere je bilo nastavljeno proženje, prehod obvesti nadrejeno krmilno enoto. Na podlagi teh informacij klicni agent izvede določeno krmilno operacijo.

Dogodki in signali so mehanizem za izmenjavo signalizacijskih sporočil med končno točko in krmilno enoto. Primer je krmiljenje rezidenčnega prehoda s signalizacijo na analogni naročniški zanki. Aplikacijski programski vmesnik za MGCP vsebuje osem ukazov. Vsak od ukazov ima obširen nabor argumentov. Argumenti so namenjeni izmenjavi lastnosti in nastavitev z ukazi naslovljenih krmiljenih osebkov. Z ukazi in njihovimi argumenti klicni agent spreminja lastnosti končnih točk in povezav ter relacije med njimi in s tem krmili delovanje prehoda. Krmilna enota lahko prek MGCP v prehodu definira načrt oštevilčenja, ki omogoča učinkovitejši prenos in detekcijo izbiranja številk. V specifikaciji MGCP je določeno naslavljanje elementov krmilne arhitekture in struktura naslavljanja končnih točk krmiljenih enot.

MGCP velja za predhodnika protokola Megaco/H.248, ki bo opisan v nadaljevanju. Megaco/H.248 je trenutno najnovejši krmilni protokol, ki ustreza porazdeljeni arhitekturi prehodov v NGN in konceptu programskega stikala. Za razliko od svojih predhodnikov ni bil načrtovan za točno določeno ciljno aplikacijo oziroma področje uporabe, temveč skuša ponuditi čim bolj univerzalno, splošno zasnovo.

2.8 MEGACO/H.248

Po definiciji MeGaCo/H.248 je MGC entiteta za oddaljeno krmiljenje klicev in medija. Vsebuje inteligenco za signalizacijo in obdelavo klicev. MG je mrežni element, ki izvaja obdelavo medija in oddajanje. Tako vrši pretvorbo med audio signali, ki se prenašajo preko telefonskega omrežja, in podatkovnimi paketi, ki se prenašajo preko IP ali drugih paketnih omrežij.

MGC uporabljajo MeGaCo/H.248 za kontroliranje MG. Tako vzpostavljajo medijske poti skozi porazdeljeno omrežje. MeGaCo/H.248 nudi prilagodljiv in abstrakten model, ki omogoča združevanje omrežij (IP, ATM, Frame Relay in PSTN/ISDN) za veliko število multimedijskih aplikacij.

Model protokola MeGaCo/H.248 vpeljuje povezavni model, ki vsebuje logične entitete ali objekte znotraj MG in se lahko kontrolirajo z MGC.

Glavne entitete so konteksti in zaključitve. Opisovalec topologije pa opisuje smeri medijskih tokov med zaključitvami v določenem kontekstu. Kontekst (Context) je logična entiteta v MG in združuje v določeno skupino več zaključitev. Kontekst opisuje topologijo in mešanje medija in/ali parametre preklapljanja, če se v skupini nahajata več kot dve zaključitvi. Identifikator ContextID določa posamezen kontekst. Ničelni kontekst vsebuje vse zaključitve, ki niso povezane z nobeno drugo zaključitvijo.

Zaključitev (Termination) je logična entiteta v MG, ki je ponor in izvor medijskih in kontrolnih pretokov. Opisovalci vsebujejo lastnosti, ki opisujejo zaključitev, in so vključeni v ukazih. Zaključitev je lahko fizična ali pa kratkotrajna (ephemeral). Fizične zaključitve predstavljajo fizične entitete, ki imajo delno stalen obstoj. Kot primer lahko vzamemo zaključitev, ki predstavlja TDM kanal. Ta zaključitev obstaja vse dokler obstaja TDM kanal do MG. Kratkotrajne zaključitve predstavljajo povezave ali podatkovne tokove kot so RTP in ponavadi obstajajo samo v času uporabe te povezave v določenem kontekstu.

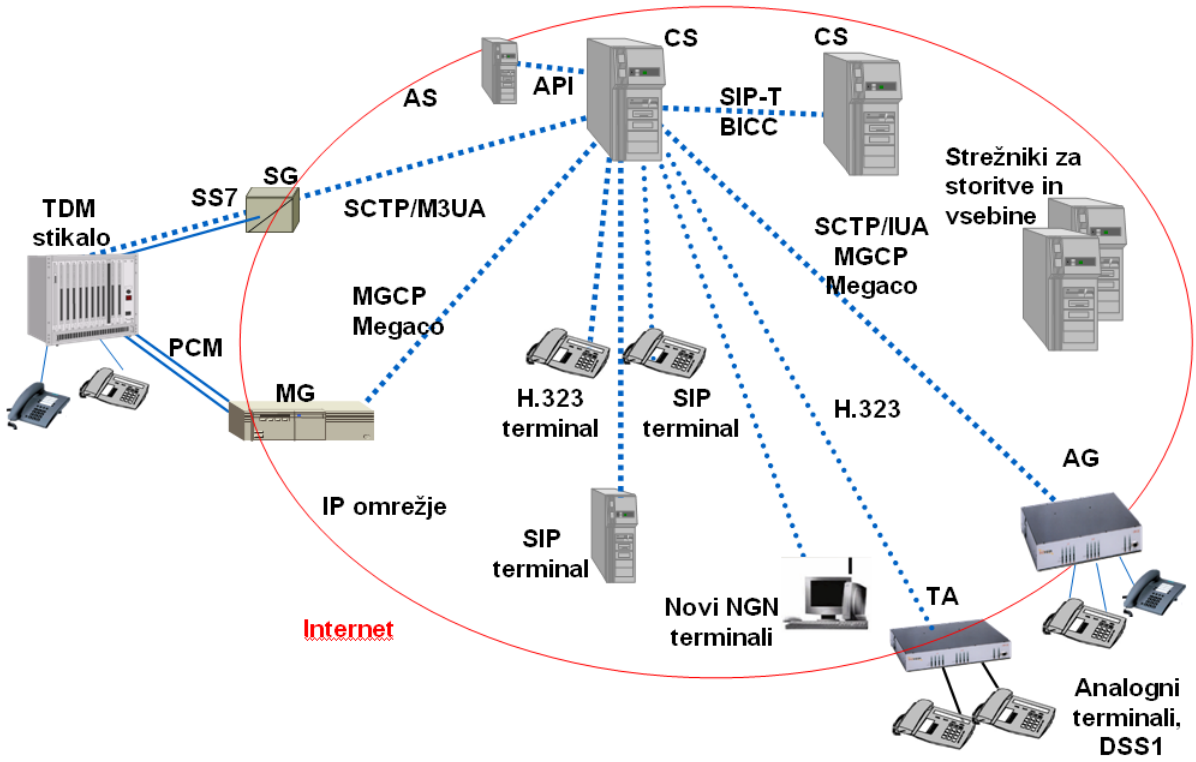
Tokovi (Streams) predstavljajo medijske tokove določene zaključitve. Tokovi tečejo med zaključitvami, ki so vsebovane v kontekstu, v skladu s pravili predpisanimi s strani opisovalcev topologije.

Opisovalci topologije (Topology Descriptor) določajo smeri medijskih tokov med zaključitvami v določenem kontekstu. Osnovna topologija določa, da oddajanje vsake zaključitve sprejmejo vse zaključitve. Opisovalec topologije je sestavljen iz zaporedja oblike (T1, T2, asociacija). T1 in T2 določata zaključitvi znotraj konteksta. Asociacija pa opisuje pretok med T1 in T2. Asociacije so lahko enosmerne, dvosmerne in izolacijske (ne povezujejo).

Protokol nudi ukaze za krmiljenje logičnih entitet (konteksti in zaključitve) povezavnega modela protokola. Tako so na voljo ukazi za dodajanje zaključitev kontekstom, spreminjanje zaključitev, odvzemanje zaključitev kontekstom, preverjanje lastnosti kontekstov in zaključitev. Ukazi nudijo popolno kontrolo lastnosti kontekstov in zaključitev.

Model protokola MeGaCo/H.248 je veliko bolj zapleten kot model protokola MGCP in nudi večjo prilagodljivost pri določanju kontrole medija. Pri protokolu MGCP se lahko vzpostavi konferenca in s tem mešanje tokov, vendar pa se ne da doseči podrobnejše kontrole, ki jo omogoča MeGaCo/H.248. Pri slednjem lahko upravljamo s posameznimi medijskimi tokovi. Pri MeGaCo/H.248 je klic predstavljen z zaključitvami znotraj konteksta klica, medtem ko je pri MGCP klic predstavljen s končnimi točkami znotraj posamezne povezave. Pri MeGaCo/H.248 vsebujejo tipi klica katerokoli kombinacijo multimedije in konferenc, medtem ko pri MGCP tipi klica vsebujejo samo načine točka-točka in točka-več točk.

Slika 2.17 prikazuje uporabo protokola MeGaCo/H.248 in drugih signalizacij.



Slika 2.17: Uporaba signalizacij v NGN

3. Nadzor signalizacije številka sedem

Poglavje obravnava koncept nadzora SS7. Opisane so tiične funkcionalnosti sistema za nadzor SS7. Poudarek je na trinivojski arhitekturi sistema. Na koncu je predstavljen produkt Symonet, ki je bil razvit v Laboratoriju za telekomunikacije v sodelovanju z Iskratel in MG-Soft.

3.1 Potreba po nadzoru

Omrežje SS7 je v osnovi načrtovano kot zaprto omrežje, zato ne podpira varnostnih mehanizmov. Ker se omrežje SS7 z razvojem omrežij nove generacije odpira, se povečuje nevarnost vdorov in napadov. Omrežje SS7 je zaradi uvajanja novih storitev vse bolj obremenjeno, zato se tudi povečuje kompleksnost zaračunavanja.

Nadzor signalizacijskega prometa je najenostavnejša metoda za odkrivanje nenamernih (recimo zaradi napačne konfiguracije) in namernih zlorab omrežja SS7. Namerne ali druge akcije, ki poslabšajo zmogljivosti signalizacije, lahko povzročijo:

- veliko različnih scenarijev izpadov,
- nepravilno zaračunavanje,
- pomanjkljivost funkcionalnosti mobilnega gostovanja,
- neuspešno prenašanje SMS (Short Messaging Service),
- nepričakovana prekinitev klica,

- slabo mobilno prehajanje,
- večkratno vzpostavljanje klica.

Kvaliteta storitev omrežja SS7 neposredno vpliva na kvaliteto storitev uporabnikov. Vse to so razlogi za vedno večjo potrebo po ločenem nadzoru omrežja SS7.

V omrežjih naslednje generacije se lahko klic vzpostavi preko več signalizacijskih protokolov. Nadzorni sistem, ki podpira tako konvergentno okolje, omogoča operaterju sledenje klica, ki zajema celotno pot.

Prednosti uporabe nadzornega sistema so:

- **Zadovoljstvo naročnika** - V preteklosti so se informacije zbirale decentralizirano na stikalih. Operaterji so se opirali na pritožbe naročnikov za informacije o napakah na omrežju. Kvaliteta storitev se lahko meri v sprotnem času skozi meritve kot sta odstotek zaključenih klicev ali analiza uporabniških zmogljivosti. Zajeti podatki so shranjeni v skupni bazi in so lahko uporabljeni za kasnejše obdelavo, recimo planiranje razširitve omrežja.
- **Preverjanje zaračunavanja**
- **Poslovno povezane možnosti** - Rudarjenje podatkov za generiranje statistik kot je količina klicev v in iz konkurenčnega operaterja.

3.2 Arhitektura sistema

Nadzor se lahko izvaja na katerikoli skupini linkov. Pomembne so povezave z drugimi omrežji (primer linki na točkah STP). Nadzorni sistem mora nadzirati večje število linkov skozi omrežje SS7, tako lahko dobimo sliko celotnega omrežja SS7. Nadzorne točke so zgrajene iz tako imenovanih sond, ki omogočajo zajem

signalizacijskega prometa v sprotnem času. Informacije dobljene iz nadzornih točk - sond se zbirajo in obdelujejo na centralni lokaciji - kontrolnem centru. Arhitektura nadzornega sistema je v tem primeru dvo ali tri nivojska. Nivo zajema podatkov opravlja še razne statistične meritve in alarmni sistem, medtem ko se na višjem nivoju dela pametna obdelava, detekcija vdorov in varnostni nadzor. Če želimo imeti centraliziran sistem nadzora, moramo v kontrolnem centru imeti podatkovno bazo. Za uporabniški dostop je lahko v nadzornem sistemu še nivo odjemalcev, kjer aplikacije poskrbijo za primeren prikaz informacij ter konfiguriranje nadzornega sistema.

Sistemi za nadzor signalizacije tipično temeljijo na dveh arhitekturnih pristopih.

1. Dvonivojska arhitektura z procesorsko zmogljivimi sondami za zajem signalizacije in aplikacijami za prikaz informacij. Na sondah se generirajo zapisi o klicih (Call Detail Records - CDR). Prav tako se na izvaja hranjenje podatkov.

2. Drug pristop je trinivojski, kjer sonde samo zajemajo signalizacijski promet. Trinivojska arhitektura sistema za nadzor SS7 omrežja je sestavljena iz:

   - zajema podatkov s signalnih povezav - sonde,
   - shranjevanja podatkov - kontrolni center in podatkovni strežnik,
   - obdelave in nivoja aplikacij - odjemalci.

   Zajeti promet pošlje drugemu nivoju, kjer se podatki obdelujejo in hranijo. V tem primeru je večina procesorske moči na drugem nivoju. Sonde opravljajo poleg zajema le filtriranje in nekaj meritev.

Na najnižjem nivoju potrebujemo sonde za zajem sporočil v sprotnem času, ki ne motijo signalizacijskih linkov.

Zbrani podatki se potem zbirajo in obdelujejo na drugem nivoju, to je kontrolnem centru. Kontrolni center skrbi za generiranje zapisov CDR in njihovo

shranjevanje v podatkovne baze. Čas shranjevanja in tip podatkov sta odvisna od zahtev uporabnika sistema.

Najvišji nivo vsebuje vsebuje aplikacije za prikazovanje in analizo informacij dobljenih z zajemom sporočil. Ključne funkcionalnosti aplikacijskega dela so:

- listanje CDR,
- analiza prometa,
- analiza zmogljivosti,
- analiza kakovosti storitev,
- sledenje klicem,
- protokolna analiza,
- detekcija vdora,
- izvajanje meritev,
- računanje statistike.

3.2.1 Zajem podatkov

Za zajem podatkov se uporabljajo nadzorne sonde. Funkcija nadzorne sonde je, da v realnem času zajema podatke s signalne povezave. Visokoohmska priključitev omogoča nemoteno delovanje signalne povezave ne glede na stanje sonde. Nadzorna sonda zajema:

- stanja signalne povezave (Events),
- signalna sporočila (Signal Units),
- izvaja določene meritve zmogljivosti in prometa.

Sonda uporablja princip filtrov za selektivni zajem podatkov in posredovanje v nadzorni center. Opremljena je z vmesnikom Ethernet za priključitev v paketnih omrežjih. Prenos podatkov v nadzorni center se izvaja prek protokola TCP/IP. V slučaju izpada omrežne povezave, se podatki shranjujejo na lokalni disk, od koder se po ponovni vzpostavitvi povezave prenesejo v nadzorni center. Celotno upravljanje z nadzorno sondo se izvaja iz nadzornega centra v grafičnem upravljavskem okolju aplikacije. Uporabnik lahko spreminja konfiguracijo sonde (nastavitve signalnih linkov, nastavitve zajema podatkov nastavitve filtrov) in nadzoruje stanje sonde (status monitor). Signalni link je določen s priključkom in časovnim oknom (Time Slot - TS) za obe smeri (Rx in Tx glede na bližnji omrežni element). Poleg zajema opravlja še funkcijo filtriranja sporočil in statistične meritve prometa. Zajeta in filtrirana sporočila pošlje kontrolnemu centru v nadaljnjo obdelavo.

Časovna žig

Da zagotovimo časovno sledljivost sporočil, mora sonda vsa zajeta sporočila opremiti s časovnim žigom. Za SS7 sporočila potrebujemo točnost časovnega žiga reda milisekunde. Zaradi tega morajo biti vsi elementi sistema za nadzor časovno sinhronizirani.

Časovna sinhronizacija

Če se uporablja podatke, ki so zajeti iz sond (ali drugih merilnikov), je pomembno čim bolj natančno merjenje časa dogodka (time stamp). Sonda mora imeti čim bolj točen absolutni čas. Za časovno sinhronizacijo sond, je trenutno najboljša rešitev GPS (Global positioning system) sprejemnik točnega časa.

Cenejša alternativa za časovno sinhronizacijo predstavlja uporaba protokola NTP (Network Time Protocol). Protokol NTP uporablja za sinhronizacijo računalnikove ure posebne algoritme, ki skrbijo (za razliko od preprostejših protokolov) za zveznost in monotonost procesorskega časa. Skokovite spremembe

časa ali preskok časa nazaj imajo lahko namreč neprijetne posledice na delovanje programov. Uravnavanje časa je izvedeno z izmenjavo kratkih občasnih paketov z NTP strežniki - to so strežniki, katerih ura je usklajena s cezijevimi oscilatorji ali GPS satelitskimi sprejemniki. NTP omogoča časovno sinhronizacijo prek omrežij IP s točnostjo reda nekaj milisekund. Izvedba protokola NTP je protokol SNTP (Simple Network Time Protocol), ki je v splošnem nekoliko manj točen. Protokol SNTP je manj kompleksen in zato lažji za realizacijo. Osnova delovanja NTP protokola je v merjenju skupnega časa od zahteve do odgovora NTP strežnika. Privzamemo, da je zakasnitev omrežja enaka v obe smeri (polovica skupnega časa) in na osnovi tega popravimo trenutni čas.

Filtriranje zajema signalnih sporočil

Filtriranje se izvaja po posameznih poljih v signalnih stavkih. Na linijskem nivoju je možno filtriranje glede na tip signalnih stavkov. Za vsako vrsto signalnih stavkov lahko posebej dovolimo ali prepovemo prenos. Tip je določen s poljem LI (Length Indicator - indikator dolžine) :

- signalne stavke FISU, če je vrednost polja LI enaka 0,
- signalne stavke LSSU, če je vrednost polja LI enaka 1 ali 2,
- signalne stavke MSU, če je vrednost polja LI enaka med 3 in 63.

Za MSU lahko dovolimo ali prepovemo prenos ponovljenih MSU. Na mrežnem nivoju lahko filtriranje izvaja glede na polja:

- indikator storitve - SIO - service indicator octet. Omogoča ločevanje sporočil signalizacije številka 7 na nivoju mrežne plasti glede na servis (MTP, ISUP, SCCP) in omrežje (nacionalno, mednarodno). Filtriranje MSU sporočil se izvaja ločeno glede na indikator storitve (SI - Service Indicator) ter indikator omrežja (NI - Network Indicator). Filtriranje določimo za vsak NI,

- koda ponorne točke - DPC - Destination Point Code,
- koda izvorne točke - OPC - Originating Point Code.

Prepuščena signalna sporočila se z nadzornim protokolom prenesejo v nadzorni center.

Redundanca na zajemu

Za potrebe zaračunavanja je potreba po redundanci zajema SS7 prometa. Vsak SS7 link je potrebno nadzorovati z dvema SS7 sondama, najbolje na vsaki strani linka ena.

V normalnem delovanju obe sondi zajemata signalna sporočila in jih shranjujeta v vmesni pomnilnik. Samo ena od sond (aktivna) pošilja sporočila v nadzorni center.

V primeru prekinitve povezave z aktivno sondo (npr. zaradi napake na sondi ali na IP povezavi med sondo in nadzornim centrom), nadzorni center aktivira pasivno sondo. Od nje zahteva prenos SS7 sporočil za manjkajoče časovno obdobje.

3.3 Shranjevanje podatkov

Za doseganje visoke razpoložljivosti podatkovne baze potrebujemo zmogljiv podatkovni strežnik.

3.3.1 Podatkovni strežnik

Aplikacija na podatkovnem strežniku upravlja s podatkovno bazo. Podatkovna baza vsebuje vse zajete in obdelane podatke, ki so bili poslani iz nadzornih sond.

Podatkovni strežnik tipično omogoča:

- vnos podatkov,
- pregled in analizo podatkov,
- brisanje podatkov (ročno ali avtomatizirano),
- arhiviranje podatkov,
- prenos podatkov na druge podatkovne strežnike,
- planiranje (sheduling) dnevnih akcij
- in proženje (triggering) trenutnih (near real time) akcij.

Podatkovni strežnik mora biti zasnovan tako, da predvsem dosega visoke zmogljivosti pri vpisovanju podatkov.

3.4 Odjemalci

Aplikacijski odjemalci so aplikacije, ki delujejo kot podatkovni odjemalec ter omogočajo povezavo s podatkovni strežniki preko interneta/intraneta. Odjemalec komunicira s podatkovnim strežnikom preko TCP/IP povezave. Odjemalec dosega podatke na strežniški aplikaciji na podlagi poizvedb. Poizvedbo je sestavljajo naslednje informacije:

- tip poizvedbe, ki je odvisen od tipa podatkov,
- časovno okno poizvedbe,
- filtri, ki so odvisni od tipa poizvedbe.

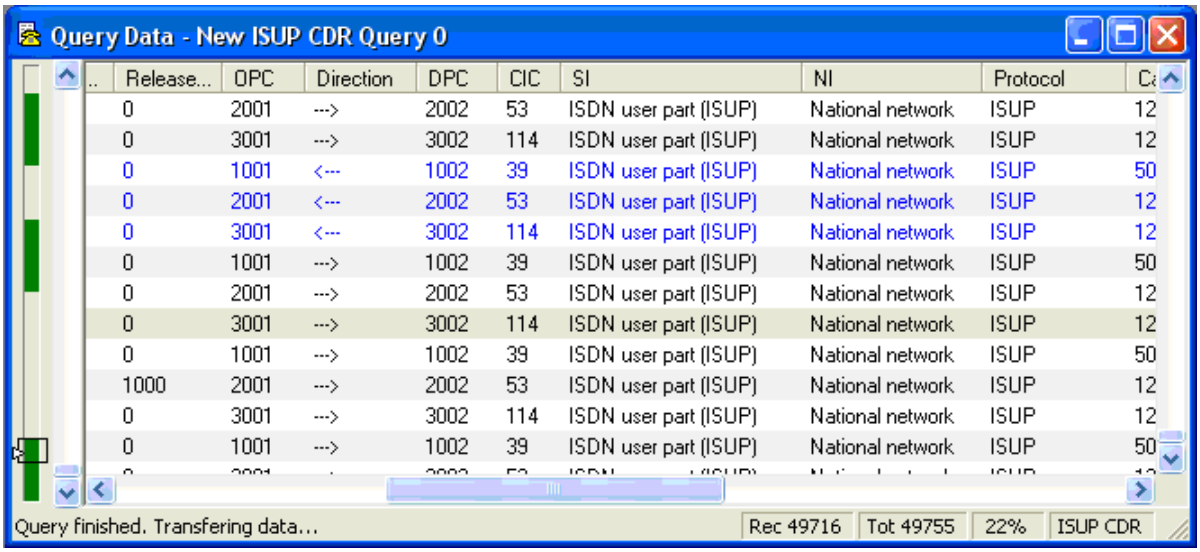
Časovno okno pove znotraj katerega časovnega intervala se nahajajo zahtevani podatki. Z uporabo filtrov lahko dodatno zmanjšamo število zahtevanih podatkov. Vsi podatki, ki ustrezajo tipu poizvedbe in se nahajajo znotraj zahtevanega časovnega okna se preberejo in po potrebi filtrirajo na strani strežniške

aplikacije.

Odjemalec tipično omogoča poizvedbo po naslednjih podatkih:

- poizvedba po signalnih stavkih (SU -Signal Units) po izbranih povezavah,
- poizvedba po informativnih zapisih (xDR - Details Records),
- poizvedba po signalnih sporočil (MSU - Message Signal Units) na podlagi katerih je bil generiran posamezen xDR zapis,
- poizvedba po meritvah oz. statističnihs poročilih (Q.752, E.422).

Na sliki 3.1 je primer poizvedbe po ISUP CDR v aplikaciji odjemalca.



Slika 3.1: Primer poizvedbe ISUP CDR

3.5 Aplikacije sistema za nadzor signalizacije

Aplikacije nadzornega sistema predstavljajo uporabniški vnesnik. Aplikacije posredujejo koristne informacije uporabniku nadzornega sistema. Tipične funkcionalnosti aplikacij v sistemih za nadzor so:

- upravljanje in konfiguriranje sistema,

- prikaz topološke slike omrežja,
- analiza alarmov,
- generiranje CDR,
- prikazovanje meritev in računanje statistike
- detekcija zlorab,
- sledenje klicem.

3.5.1 Upravljanje in konfiguriranje sistema

Aplikacija mora omogočati upravljanje in konfiguriranje celotnega nadzornega sistema. Nastavlja se konfiguracijske parametre sonde kot npr. nastavitev časovnega okna in priključka (time slot in port). Takšen način omogoča centralizirano upravljanje in konfiguriranje vseh sond iz ene točke.

Pomembne informacije pri upravljanju sistema so:

- stanje SS7 sond,
- detaljne informacije o stanju SS7 povezav,
- detaljne informacije o stanju nadzorovanih vozlišč omrežja.

3.5.2 Topološka slika omrežja

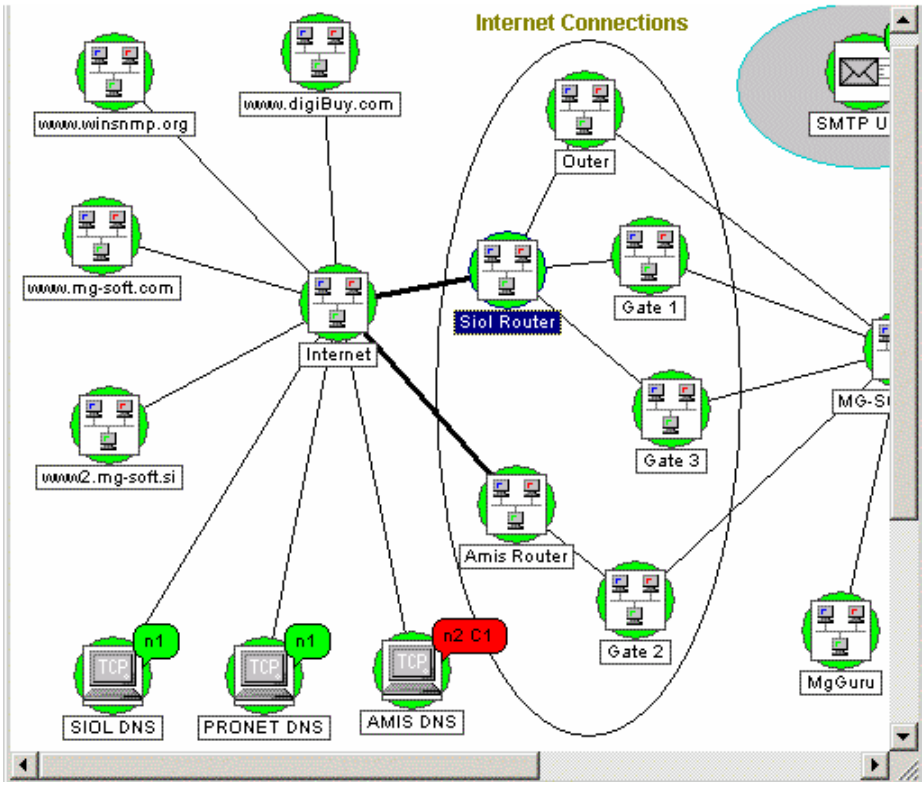
Topološka slika omrežja omogoča grafično spremljanje stanja na nivoju MTP1, MTP2 in MTP3. Z barvnimi in grafičnimi efekti je nazorno prikazano stanje omrežja in alarmi. Prav tako lahko v istem grafičnem vmesniku izvajamo konfiguracijo nadzornega sistema.

Glavne prednosti topološke slike omrežja so:

- neprekinjen nadzor vseh SS7 linkov v sprotnem času,

- takojšen vizualni prikaz napake na linku ali napravi,
- hiter dostop do podrobnih informacij linka, ki je v okvari.

Slika 3.2 predstavlja primer topološke slike omrežja.



Slika 3.2: Primer topološke slike omrežja

3.5.3 Analiza alarmov

Nadzor stanja signalizacijskega omrežja se izvaja preko nadzora stanj posameznih linkov. Ob spremembah se v nadzorni center prenašajo alarmi. Nadzoruje se dogajanje na signalnem linku in na fizični povezavi (E1 link). Za nadzor sond se preko on-line sistemske diagnostike zajemajo sistemski alarmi:

- napake pri delu z diskom,
- napake na napajalniku,

- izpadi in obnovitev sistema,
- pregrevanje.

Alarmi se posredujejo procesom nadzora SS7 in se v nadzorni center prenašajo enako kot alarmi na signalnih linkih.

Upravljalec alarmov zbira alarme nadzorovanih objektov v sprotnem času. Zbrani alarmi so ustrezno filtrirani, prikazani in po možnosti posredovani na različne izhodne naprave preko E-mail, SMS ipd. Upravljavec alarmov omogoča uporabniku pregled vsebine alarmov, filtriranje alarmov na različne kriterije.

Alarmi vsebujejo naslednje informacije:

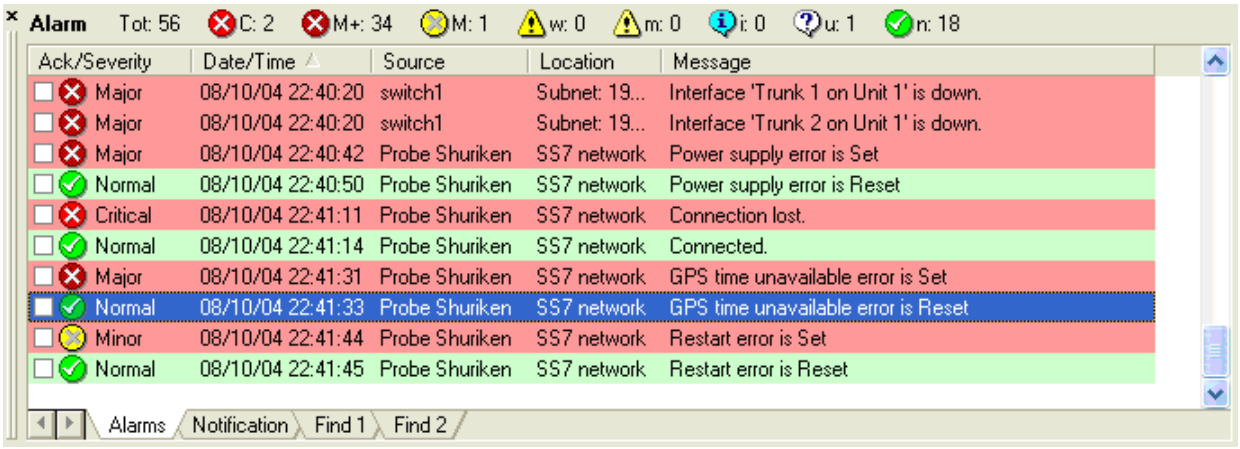
- čas in datum alarma,
- izvor alarma (oznaka nadzorovanega objekta in njegova lokacija),
- težo alarma,
- informacijo o potrditvi alarma,
- verjeten vzrok za sprožitev alarma,
- opis alarma.

Alarme v sistemu za nadzor ločimo v tri skupine:

- sistemski alarmi, med katere spadajo alarmi na datotečnem sistemu, napajalnem sistemu, pregrevanje ali ponovni zagon sistema,
- alarmi na fizičnem nivoju,
- alarmi na signalnem novoju, primer - *Link Failure, No Flags, Congestion.*

Slika 3.6 prikazuje primer upravljavca alarmov.

Način shranjevanja alarmov mora omogočat naknadno pregledovanje njihove zgodovine. Zgodovina alarmov se lahko pregleduje po različnih kriterijih kot so časovno okno, izvor alarma in teža alarma.



Slika 3.3: Primer alarmov sistema za nadzor SS7

3.5.4 Generiranje zapisov o klicih

Zapisi o klicih (Call Detail Records - CDR) vsebujejo podrobne informacije o klicu ali signalizacijski proceduri v celoti. Orodje za generiranje zapisov CDR s prilagodljivim vmesnikom do aplikacij omogoča operaterju prenos informacij o klicih v sprotnem času.

Zaradi novih storite je velikost zapisa CDR je v zadnjih letih zrasla iz povprečne velikosti 80 oktetov na 200 oktetov. Kot rezultat novih informacij, se CDRji danes uporabljajo za nadzor omrežja, analizo prometa, sisteme zaračunavanja in detekcijo vdora. Brez beleženja CDR in posredovanja v sistem zaračunavanja, bi bili operaterji brez možnosti zaračunavanja novih storitev. Operaterji morajo ščititi svoje obdelane CDR z visoko mero varnosti.

Vsebina CDR je odvisna od protokola in tipa klica. ISUP CDR vsebuje naslednje informacije:

- Begin time,
- End time,
- Set-up time,
- Conversation time

- Release time
- Originating point code - OPC
- Destination point code - DPC
- Circuit identification code
- Service information octet
- Protocol
- Direction (input/output)
- A Number
- B Number
- Category of address A
- Cause family
- Cause value
- Location value
- Bearer service
- Signaling capability
- Number of message signal units
- Message signal unit

3.5.5 Protokolna analiza

Z uporabo ločene strojne opreme za nadzor omrežja SS7, postane tradicionalna lokalna protokolna analiza distribuirana protokolna analiza, ki je lahko vključena v zunanji sistem za nadzor. Komponenta protokolne analize omogoča večnivojsko

dekodiranje in možnosti filtriranja. Prednosti takega porazdeljenega pristopa od navadne lokalne protokolne analize so:

- operater lahko dela raziskavo iz enega, centralnega mesta in ni potrebna posamezna analiza na različnih lokacijah,
- filtriranje množice podatkov omogoča delo na bistvenih podatkih,
- prikaz raziskave je predstavljen v razumljivi obliki.

3.5.6 Meritve na signalnih linkih

Mednarodna zveza za telekomunikacije je v sektorju za standardizacijo v telekomunikacijah izdala priporočila za nadzor in meritve omrežja SS7 Q.752 [1]. Priporočila definirajo primerne meritve za vodenje razpoložljivosti omrežja SS7. Te meritve služijo kot osnova za detekcijo zlorab, upravljanje konfiguracije, analizo lastnosti, štetje prometa in upravljanje ter načrtovanje omrežij.

Sonda zajema statistične podatke, ki jih standard definira kot obvezne za podatkovno plast SS7. Ostale meritve na omrežnem nivoju MTP-3 in meritve uporabniškega prometa (ISUP) se izvajajo v nadzornem centru.

skupine meritev na siganlnih linkih so:

- napake na linkih,
- razpoložljivost,
- obremenjenost,
- prometna razporeditev,
- napake na krmilnem delu signalizacijske zveze - SCCP
- promet SCCP,
- kvaliteta storitev SCCP,

- promet ISUP.

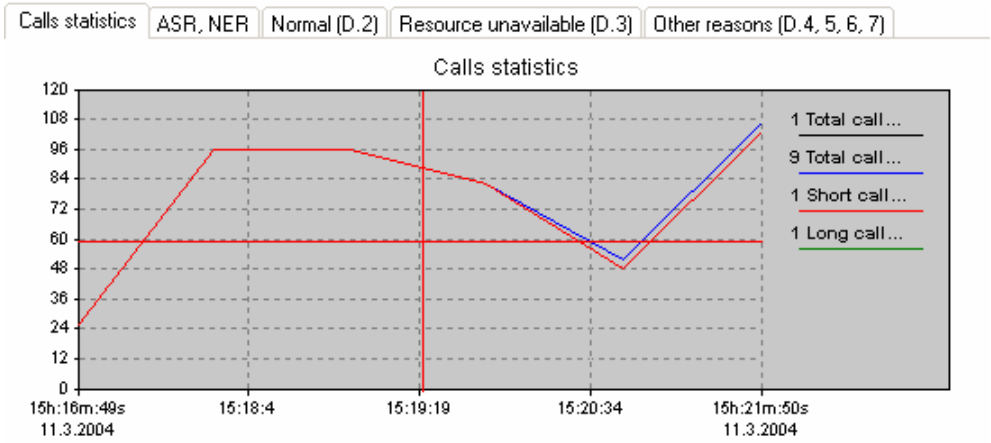
3.5.7 Meritve uporabniškega prometa

ITU-T priporočilo E.422 opisuje parametre za opazovanje kvalitete storitev do naročnika. Pri tem je pomembno da opazujemo bistvene parametre za določanje kvalitete storitev (kot so število uspešnih in neuspešnih klicev).

Statistika se danes večinoma meri avtomatsko iz naslednjih razlogov razlogov:

- zniževanje stroškov za ugotavljanje kvalitete storitev,
- možnost neprekinjenega opazovanja,
- izključen faktor človeške napake,
- olajšana avtomatska obdelava podatkov,
- možnost večje količine vzorcev.

Na sliki 3.4 je primer grafičnega prikaza statistike gostote prometa.



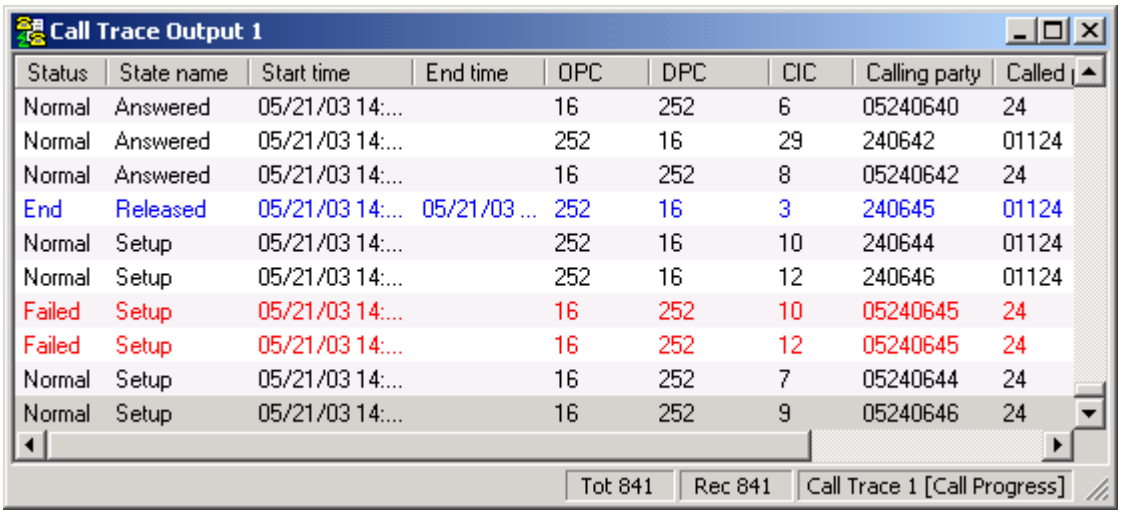
Slika 3.4: Primer E.422 statistike

3.5.8 Call trace - sledenje klicem

Bistvo sledenja klicem je, da aplikacija sestavi signalizacijo iz različnih povezav od klicočega do klicanega preko vseh vmesnih povezav. Z nastavitvijo različnih filtrov lahko uspešno poiščemo iskani klic. Filtriranje za sledenje klica se dela navadno za:

- kodo izvorne točke - OPC
- kodo usmeriščne točke - DPC
- kodo za identifikacijo voda - CIC
- klicočo ali klicano stevilko.

Povezava s protokolno anlizo omogoča prikaz detajlnih informacij o klicu. Aplikacija za sledenje klicem prikazuje vse trajajoče klice v sprotnem ali kasnejšem času (slika 3.5).



Slika 3.5: Primer prikaza trajajočih klicev

3.5.9 Detekcija zlorab

Avtomatska zaznava zlorab je izvedena z iskanjem določenih (zlorabnih) vzorcev, predpogoj pa je zajemanje informacij za vsako komunikacijo, ki se zgodi v sistemu. Vse kar je izven vzorcev, ki predstavljajo normalno delovanje, sproži alarm. Izven normalnih vzorcev so ponavadi:

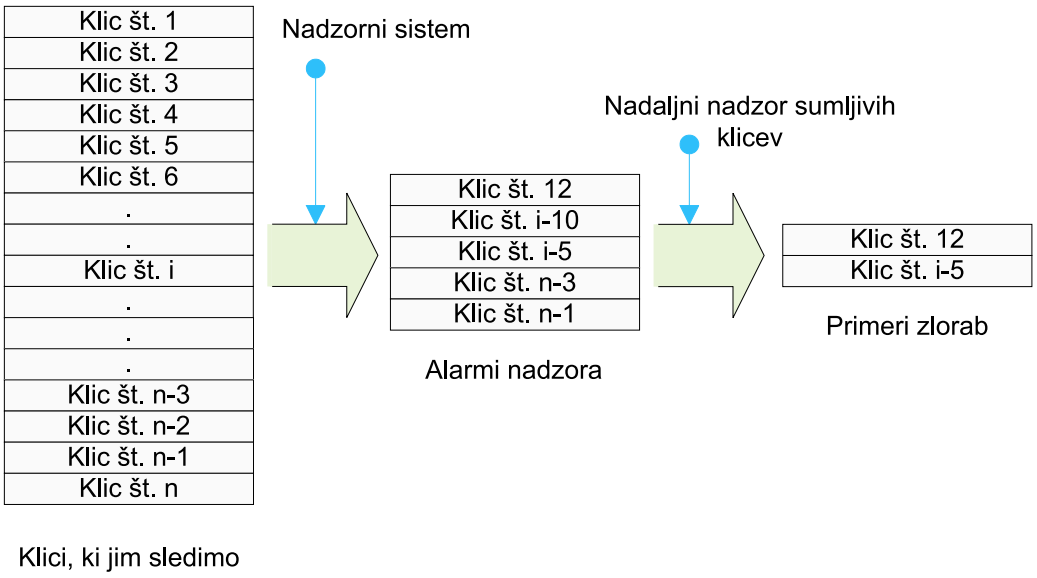
- zaznani klici, ki trajajo dalj časa,
- ponavljajoči klici določenih številk v isti omrežni skupini,
- ponavljajoči klici na številke iz druge omrežne skupine,
- veliko število dolgih klicev s številke, kateri se storitve ne zaračunavajo,
- klicanje posebnih številk,
- klicanje na veliko številk, za katere ni potrebno plačati storitve.

Vzorce, ki predstavljajo zlorabo, v tem primeru ne iščemo v podatkih, ki jih prenašamo (govor), pač pa v signalizaciji, ki omogoča nadzor. Velika prednost takšnega zajemanja podatkov je majhno število podatkov, ki jih obdelujemo in s tem veliko večja hitrost detektiranja zlorabe.

Ko se enkrat sprožijo alarmi so akcije sistema zelo različne, odvisne so tudi od vrste alarma:

- shrani zajete podatke,
- nadaljuje s sledenjem zlorabe in tako pridobiva dodatne informacije o vdoru in o načinu zlorabe,
- avtomatsko obravnava zlorabe,
- obvesti operaterja.

Slika 3.6 prikazuje princip javljanja alarmov.



Slika 3.6: Alarmi pri detekciji zlorab

Detekcija v realnem času - Stohastični model

Pri detekciji zlorab na področju telekomunikacij v realnem času je potrebno omeniti tudi metodo, ki temelji na stohastičnem generativnem modelu. V tem modelu imamo tri spremenljivke:

- **žrtev**, ki govori o tem ali je bil uporabniški račun napaden ali ne,
- **zloraba**, kjer oseba pravkar zlorablja sistem,
- **klic**, ki govori o tem ali je trenutno klic vzpostavljen.

V tem načinu detektiranja zlorab uporablja model preklopnega režima časovnih serij. Spremenljivke so v časovnih serijah binarne, preklopne spremenljivke pa imajo hierarhično strukturo. Prednost hierarhične strukture je ta, da omogoča modeliranje časovnih serij v različnih časovnih skalah. Na najnižjem nivoju se modelirajo posamezni klici. Na naslednjem nivoju se modelirajo prehodi iz normalnega načina v zlorabljen način, na najvišjem nivoju pa prehod v zlorabljen. Pri metodi uporabljamo skrite Markove modele.

Uporabniški profili

Uporabniški profili so podatki o uporabniku, ki nam govorijo o tem, kako se določen uporabnik obnaša oziroma, kakšne so njegove navade. Podatke, ki jih potrebujemo za izdelavo takšnih profilov, dobimo s pomočjo opazovanja uporabnika. Vsako uporabnikovo akcijo posnamemo in zabeležimo. Vendar pa se pri takšnem pristopu, ko beležimo vsako akcijo, pojavijo problemi, ki se kažejo predvsem v količini teh podatkov. Potrebno se je zavedati, da je v telekomunikacijskem sistemu ogromno uporabnikov, tako da bi ogromne količine zasedle ogromno prostora, zelo pa bi se podaljšal čas procesiranja informacij, ki se skrivajo v teh obsežnih podatkovnih bazah.

Zaradi zgoraj opisanega problema je potrebno narediti uporabniške profile takšne, ki bodo predstavljali popolno uporabniško obnašanje z minimalno količino podatkov.

Uporabniški profil kreiramo iz podatkov, ki so relavantni in ki nosijo neko informacijo o klicu, vendar ta ne sme vsebovati podatkov o vsebini govora ali kakaršnih koli drugih podatkov. Vse podatke, ki ne prispevajo k informaciji o klicu ali pa se dajo izračunati iz ostalih podatkov ne shranjujemo v bazo podatkov. Pri kreiranju uporabniških profilov se moramo zavedati dveh pomembnih stvari. Prva in najpomembnejša stvar je učikovitost shranjevanja podatkov in osveževanja le teh. Druga pomembna stvar pa je, da morajo uporabniški profili predstavljati dejansko obnašanje nekega uporabnika. Vse informacije, ki jih potrebujemo za kreiranje, lahko dobimo iz podatkov, ki jih uporablja operater za kreiranje in izdajanje računov. Najpomembnejši parametri, ki se uporabljajo pri detekciji zlorab so[7]:

- **Charged_IMSI** identifikacija uporabnika,
- **First_Cell_ID** karakteristika lokacije v mobilnem omrežju,
- **Chargeable_Duration** osnova za vse ocenitve stroškov klica,

- **B_Type_of_Number** osnova za razločevanje med nacionalnimi in mednarodnimi klici,
- **Non_Charged_Party** katera številka je bila klicana,
- **Charging_Start_Time** čas začetka klica.

Ko imamo uporabniške profile narejene, jih je potrebno znati uporabljati. Načeloma obstajata dva načina uporabe uporabniških profilov, absolutni in diferencialni.

Absolutni način uporabe uporabniških profilov pomeni, da imamo narejene uporabniške profile, ki nosijo informacijo o nekem uporabniku. Ko se zazna delovanje uporabnika, ki bolj ali manj odstopa od informacije o tem kako naj bi uporabnik uporabljal storitve, se aktivirajo sprožilci. Na osnovi teh sprožilcev pa se nato nadalje obdela klic in se določi ali gre za zlorabo ali ne. V tem primeru zaznamo zlorabo tistega določenega klica, ki ga preverjamo.

Drugi način uporabe profilov je diferencialni način. Ta postopek se je razvil na podlagi dejstva, da je zlorabo težko odkriti iz enega samega klica. Ponavadi je potrebno pregledati daljše časovne obdobje delovanja uporabnika, da se lahko detektira zloraba, razen redkih izjem, ko gre na primer za prekrivajoča se klica. Diferencialni način se opira na dva uporabniška profila za enega uporabnika, kratkoročen in dolgoročen profil. Ko se zazna sprememba vzorca obnašanja uporabnika, ko pride do odstopanj med kratkoročnim in dolgoročnim profilom, se aktivirajo sprožilci na osnovi katerih nadalje ugotavljamo ali gre za zlorabo ali ne.

3.6 Primer sistema za nadzor signalizacije

V sodelovanju podjetji Iskratel in MG-Soft je bil v laboratoriju za telekomunikacije razvit produkt SYMONET SI2000 [12]. Produkt je tipičen predstavnik sistema za nadzor SS7.

3.6.1 Produkt SYMONET SI2000

SYMONET SI2000 je namenjen nadzoru elementov SS7 v sprotnem času in kasnejši analizi zajetih podatkov za nadzor, upravljanje in načrtovanje.

Iskratel SYMONET SI2000 omogoča :

1. nadzor signalnega omrežja v realnem času :
   - nadzor stanja elementov (status monitor)signalne povezave, nadzorni sistem,
   - odkrivanje napak (alarm management),
   - analiza zmogljivosti (performance management) - skladno s ITU-T Q.752,
2. analizo SS7 omrežja :
   - analiza prometa (traffic analysys),
   - analiza protokola (protocol analysys),
   - sledenje klicem (call trace),
   - analiza klicev z nastavljivimi filtri (multicriterial filtering),
   - odkrivanje preobremenitev.
3. nadzor uporabniškega omrežja (iz SS7 podatkov) :
   - status v realnem času,
   - promet v realnem času.
4. kakovost storitev (QoS , ITU-TE.422)
5. odkrivanje napak (npr. visoka stopnja nerealiziranih klicev v določeno smer)

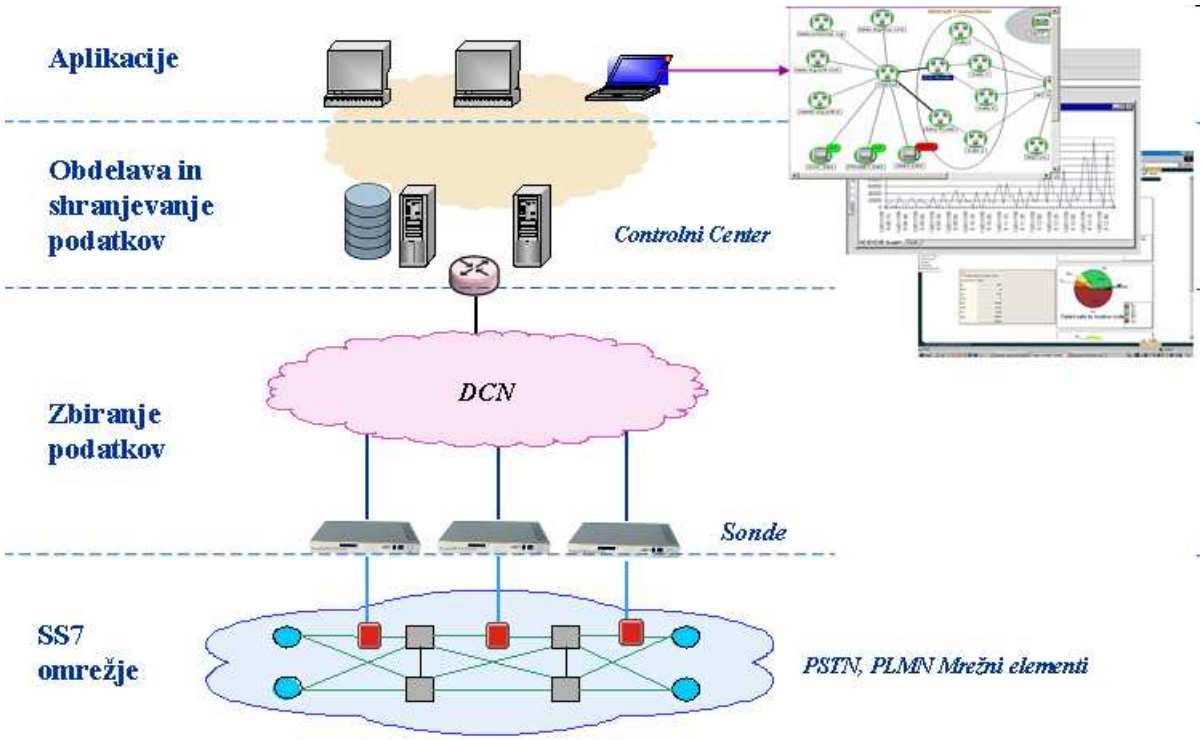
Sistem SYMONET SI2000 deluje kot skupna platforma, ki omogoča omrežno rešitev zbiranja glavnih kazalcev zmogljivosti in podrobnih zapisov o klicih ali transakcijah. Poleg tega omogoča nadzor SS7 protokolov in v prihodnosti nadgradnjo k protokolom naslednje generacije, kot so H.323, SIP in MGCP. Sonde sistema SYMONET SI2000 zbirajo podatke s signalnih povezav v realnem času. Visokoimpedančni vmesniki na sondah omogočajo nemoteno povezavo z nadzorovanim omrežjem, tako da se podatki o zmogljivosti zbirajo brez vpliva na njegovo delovanje. Programska oprema sonde filtrira zbrani signalni promet in lokalno shrani podatke, dokler se ti ne prenesejo v nadzorni center sistema SYMONET, kjer poteka nadaljnja obdelava.

Sonde posredujejo signalne podatke, podatke meritev o zmogljivosti in podatke o stanju povezav nadzornemu centru, kjer poteka osnovna obdelava. Zapisi podatkov o klicih ali transakcijah se generirajo in shranijo v pomnilnik nadzornega centra. To je odlagališče, ki istočasno oskrbuje in podpira več aplikacij. Dostop do podatkovne baze je možen neposredno prek odjemalske aplikacije, ki je del paketa produkta SYMONET, ali prek vmesnika uporabniškega programa (API).

Najvišji sloj zajema odjemalske delovne postaje z različnimi aplikacijami za napredno obdelavo podatkov, zbranih v sistemu SYMONET. Iskratel ponuja sistem za analizo omrežja, ki je bil razvit v sodelovanju z operaterji, da bi kar najbolj zadovoljili svoje poslovne potrebe. Orodja so namenjena za analizo prometa v telekomunikacijskih omrežjih v realnem času.

Sistem analize predvsem zagotavlja informacije o dolgoročni zmogljivosti omrežja in služi za ovrednotenje poslovnih parametrov. Predstavlja učinkovito orodje za optimizacijo obstoječih omrežij, načrtovanje razširitve omrežja in ovrednotenje poslovnih kazalcev posameznih storitev. Generirana poročila se lahko preprosto prilagodijo zahtevam kupcev, da bi kar najučinkoviteje zadostili svoje specifične potrebe.

Slika 3.7 prikazuje zgradbo sistema SYMONET.



Slika 3.7: Arhitektura sistema SYMONET [12].

4. Razširitev nadzora signalizacij

V zadnjem času se telefonski operaterji odločajo za integracijo tradicionalnih SS7 omrežij s paketno orientiranimi IP omrežji. Razlogov je več:

- zmanjšanje stroškov; VoP (Voice over Packet) omrežna oprema in vzdrževanje je cenejše,
- lažje vpeljevanje novih storitev, ki temeljijo na dopolnilnih in inteligentnih aplikacijah,
- preusmerjanje podatkovnega prometa iz SS7 omrežju na IP omrežje.

Pri nadzoru signalizacije je pomemben podatek zapisa klica. V omrežjih nove generacije (New Generation Networks - NGN) se za zapis podatkov klica uporablja IPDR (Internet Protocol Detail Record).

4.1 Nadzor signalizacij v NGN

Takšno hibridno IP/SS7 omrežje prinaša večje število medsebojnih povezav, ki so tudi bolj rizične. Primernih orodij za nadzor prometa v hibridnem omrežju IP/SS7 pa je še zelo malo.
Potrebno je pokriti naslednje signalizacije:

- SS7 over IP (SCTP, M3UA, ...),
- H.323,

- SIP,
- MGCP,
- H.248/Megaco.

Zaradi kompleksnosti NGN omrežij in velike količine podatkov v sistemu nadzora je potrebno doseči zelo dobro skalabilnost na področju obdelave in predstavitve podatkov. Omenjeno skalabilnost se lahko doseže z uporabo porazdeljene arhitekure (cluster design).

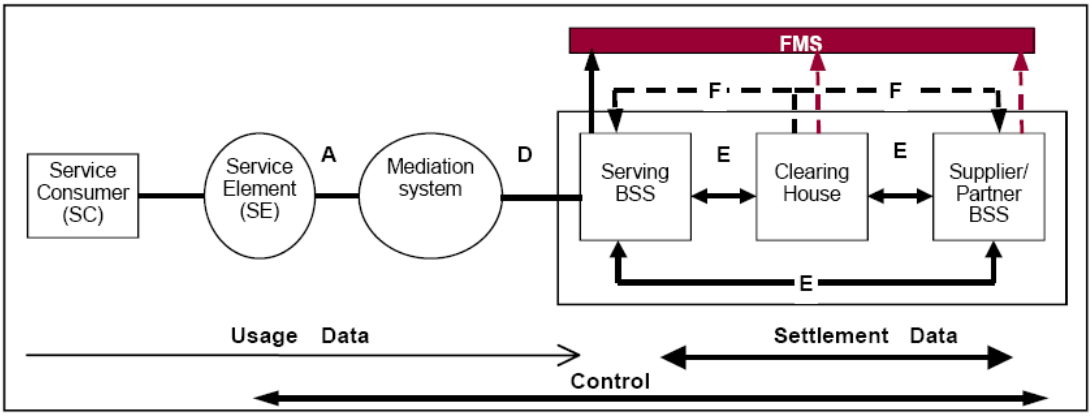
IPDR (Internet Protocol Detail Record) zapisi so bistvenega pomena za hitro implementacijo zaračunavanja novih storitev ter za nadzor parametrov SLA (Service Level Agreement).

4.1.1 Zapis podatkov klica

Za zapis podatkov klica in storitev se v omrežjih NGN uporablja IPDR (Internet Protocol Detail Record). Vsebino IPDR standardizira IPDR.org. To je konzorcij vodilnih ponudnikov storitev in proizvajalcev mrežne opreme in sistemov za zaračunavanje. Njegov cilj je zmanjšanje cene in časa uporabe meritev ter razširitev interoperabilnosti za izmenjavo podatkov o zaračunavanju med telekomunikacijskimi sistemi za NGN storitve, kar je doseženo skozi definicijo in razvoj odprtega standarda za storitve v IP. Model ki specificira vmesnike za izmenjavo IPDRjev med napravami in sistemi je prikazan na sliki 4.1.

VoIP IPDR

VoIP (Voice over Internet protocol) je postal sinonim za internetno telefonijo, ki v nasprotju s klasičnimi analognimi ali digitalnimi preklopnimi telefonskimi omrežji za govorno komunikacijo uporablja isto omrežje, kot ga uporabljajo podatkovne komunikacije – Internet. Dejstvo, da je VoIP postala ena izmed trenutno najbolj rastočih tehnologij na svetu, je povsem razumljivo, saj se je število širokopasovnih



Slika 4.1: Model vmesnikov za izmenjavo IPDR [18]

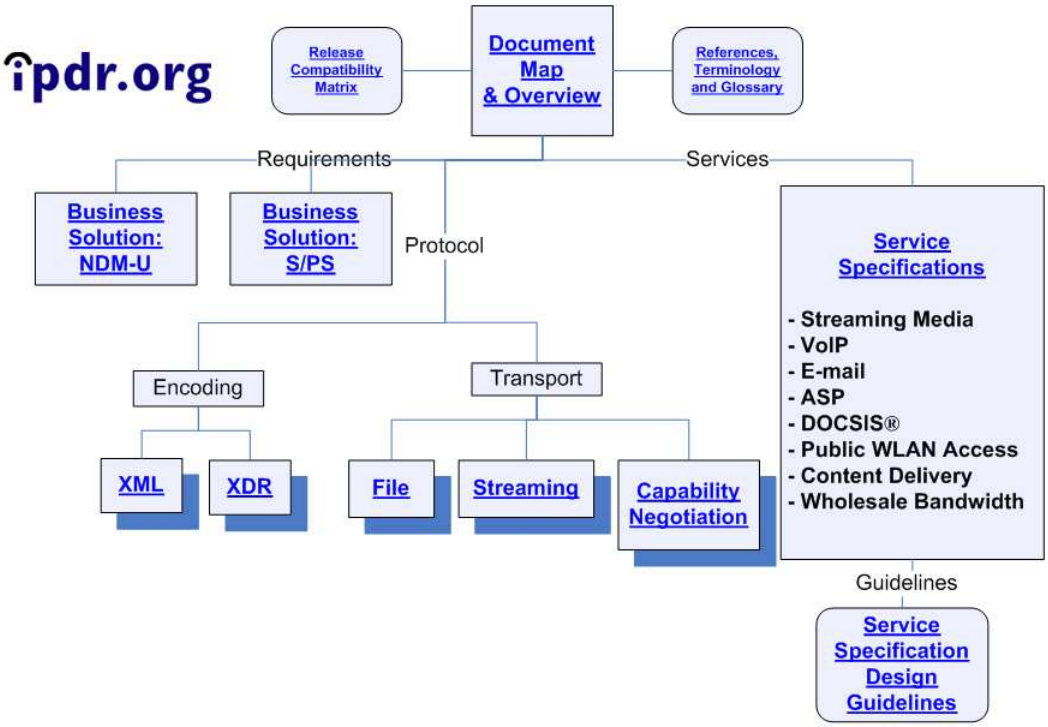
naročniških povezav v zadnjem času drastično povečalo, pri tem pa se le-te v večji meri koristijo le za podatkovni dostop. VoIP omogoča združevanje podatkovnih in govornih storitev na eni sami naročniški liniji in s tem fiksno telefonijo za mnogo nižje stroške, kar vzbuja velik interes tako na strani ponudnikov kot tudi potrošnikov govornih in podatkovnih storitev. Z razširjanjem VoIP se povečuje tudi zahteva po nadzoru in merjenju VoIP storitev.

IPDR se generira na koncu vsake klicne zveze, ne glede na to ali je bila uspešna ali ne. Druga možnost je, da se IPDR generira med potekom klicne zveze kot odziv na določene dogodke kot so začetek klica, sprejetje klica, zelo dolgo trajanje klica, detekcijo vdora ali zaključitev klica.

VoIP IPDR mora vsebovati naslednje:

- indentifikacije vseh udeležencev v klicu (klicana in klicoča številka),
- čas začetka in konca klica,
- potek stanja klica,
- za potrebe zaračunavanja, final call completion codes..,

- časi morajo biti zapisani v formatu ISO 8601[1]. Za potrebe zaračunavanja mora biti natančnost časovnega žiga najmanj 1 sekunda,
- tip plačila klica (zastonj, zaračunan klicočemu ali klicanemu, predplačniški).



Slika 4.2: Zemljevid dokumentov IPDR.ORG [11]

[1]ISO 8601 je mednarodni standard, ki definira numerično predstavitev časa in datuma.

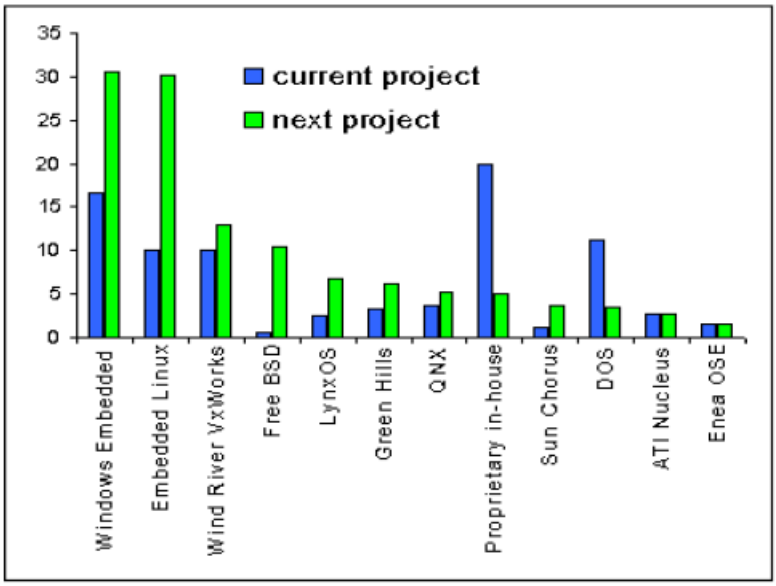
5. Nov koncept sonde za zajem signalizacij

Ključni del sistema za nadzor signalizacij je naprava, ki zajema signalizacijske podatke v omrežju. Tako napravo imenujemo sonda za zajem. Sonda mora biti dovolj zmogljiva in prilagodljiva, da zbira podatke s signalnih povezav v sprotnem času. Namen poglavja je predstavitev nadgradnje SYMONET nadzorne sonde. Prvi del nadgradnje je zamenjava z zmogljivejšo strojno opremo, ki temelji na operacijskem sistemu Linux. Drugi del nadgradnje pa je razširitev zajema na NGN omrežja. Tu bo poudarek na zajemu SIGTRAN signalizacij.

5.1 Izbira operacijskega sistema

Komercialni operacijski sistemi za delo v sprotnem času so se začeli pojavljati proti koncu 1970 in danes jih je na voljo na trgu več deset. Največji igralci na tem področju so VxWorks, pSoS, Neculeus, Windows CE 5.1. Glede na raziskavo podjetja EDC (Evans Data Corp), se delež Linuxa v vgrajenih sistemih nezadržno veča. Če je leta 1999 bil Linux le opcija, je danes povsem realno trditi, da lahko postane Linux vodilni operacijski sistem na področju vgrajenih sistemov. V raziskavi [14], se je $30,2\%$ vprašanih razvijalcev vgrajenih sistemov opredelilo za Linux kot operacijski sistem za naslednji projekt. Za Windows CE se je opredelilo $16,6\%$, medtem ko bo Windows XP embedded uporabljalo v prihodnjih projektih $14,4\%$ vprašanih. Windowsi imajo tako le neznatno prednost v primerjavi z Linux-om. Zanimivo, da celo VxWorks, ki je dolgo veljal za vodilnega na področju vgrajenih sistemov, rahlo zaostaja za Linux-om glede na trenutno uporabo po projektih. Pri prihodnjih projektih pa se bo razlika

občutno povečala v korist Linux-a. Potrebno pa je omeniti, da raziskava prikazuje le uporabo operacijskih sistemov po projektih in ne prihodke od licenc in orodij za projekt. Spekter uporabe Linuxa v različnih napravah je res širok. Najdemo ga v dlančnikih (Sharp Zaurus), mobilnih telefonih (nova serija Motorolinih telefonov), domačih zabaviščnih centrih (NEC, SONY), požarnih zidovih, robotiki in še bi lahko naštevali.



Slika 5.1: Uporaba linuxa v vgrajenih sistemih [14]

5.1.1 Linux

Linux je zmogljiv brezplačen odprtokoden operacijski sistem, ki ga odlikujeta predvsem varnost in stabilnost. Zanj se odloča vse več proizvajalcev in ponudnikov. Čeprav je Linus svoj operacijski sistem zasnoval predvsem z mislijo na varnost in zanesljivost ter pri tem nekoliko žrtvoval performance, se s časom stvari popravljajo. Do trenutno aktualnega jedra 2.6 je nastalo toliko načinov, ki omogočajo zelo hitro komunikacijo med aplikacijskim in jedrnim slojem, da je Linux primerljiv s katerimkoli drugim modernim operacijskim sistemom.
Linux je v zadnjih letih dosegel uspeh na področju namiznih računalnikov in

strežnikov. Glede na analize v industriji je pri večini novih projektov vgrajenih sistemov uporabljen operacijski sistem Linux. Napredek v strojni opremi dovoljuje visoke zmogljivosti programske opreme in operacijskih sistemov na vgrajenih (embedded) sistemih.

Ena najmočnejših in pomembnih prednosti Linuxa predstavlja tudi njegova fleksibilnost in zmožnost delovanja na različnih platformah. Linux podpira mnogo različnih tipov procesorjev (X86, Sparc, PowerPC, MIPS, ARM, itd), ter različne arhitekture le teh (enoprocesorske, SMP, večprocesorske). Prav tako je v Linuxu podpora za različne vhodno izhodne naprave kot so USB, Ethernet, velike pomnilniške enote in grafika.

Gonilniki v Linuxu so navadno integrirani v jedro kot moduli[1], kar jim omogoča preprostejši dostop do strojne opreme, več privilegijev, ter klasičen način komunikacije z aplikacijami v uporabniškem prostoru.

5.1.2 Distribucije Linux-a za vgrajene sisteme

Pri razvoju naprav, ki bodo uporabljale Linux, imamo na voljo tri možnosti. Lahko sami zgradimo svojo distribucijo s pripadajočim jedrom, korenskim datotečnim sistemom in vsemi potrebnimi orodji, za kar se na svetovnem spletu najde mnogo priročnikov in navodil, kako to storiti. Druga možnost je, da vzamemo eno od nekomercialnih distribucij (ETLinux, uClinux, ThinLinux, PeeWee Linux,...). Tretja možnost pa je, da se odločimo za katero od komercialnih distribucij. Pri prvih dveh možnostih smo prepuščeni lastnemu znanju in podpori, ki jo najdemo na spletu. Ta je precej dobra, vendar lahko zataji ravno takrat, ko je to najmanj primerno. Če torej Linux-a ne poznamo dobro in bi radi izdelek hitro spravili na tržišče, je tretja možnost najprimernejša. Na trgu je prisotnih veliko ponudnikov Linux distribucij za vgrajene sisteme (LynuxWorks - BlueCat , Embedix - Lineo, MontaVista Software - Hard Hat, RedHat embedded Linux)[14].

[1]Modul (kernel module) je binarna izvedljiva oblika,ki predstavlja funkcionalno razširitev jedra. Modul je minimalna oblika kode, ki se da naložit v jedro.

Ti ponudniki navadno ne prodajajo Linux-a ampak podporo zanj in pa orodja, ki nam olajšajo delo z njim. Vse distribucije opravijo v osnovi enako delo: pripravijo jedro, zgradijo korenski datotečni sistem in vključijo potrebne aplikacije. Kako to storijo in kakšno podporo ter dokumentacijo vsebujejo, je različno od ponudnika do ponudnika. Vsi ponujajo preizkusne verzije svojih orodij.

5.1.3 Hitrost Linux Jedra

Za gonilnike signalizacij na Linux OS je pomembno poznati predvsem odzivnost samega Linuxa. Ker je bil Linux primarno mišljen kot namizni OS, je imel (in še vedno ima) zelo veliko prepustnost podatkov, žal pa nekoliko slabšo odzivnost. Zato so se z jedrom 2.4 začeli pojavljati popravki, ki so zmanjšali odzivni čas (preemptile patch, MontaVista Preemptile kernel,...) tako pa je postal tudi Linux primernejši za vgrajene naprave. Razlika med jedri s popravki in jedri brez njih je postala tako velika, da so se začeli tudi uporabniki namiznih računalnikov vedno pogosteje odločati za nadgradnjo jeder. Tipični prehodni čas (latency) (v 99.9% primerov) je s popravki v nekaj stotinah ali celo desetinah mikrosekund. Razvoj je šel dalje in danes so na voljo popravki in prirejena jedra, ki povečajo odzivnost tudi do 30krat in več v primerjavi z originalnim jedrom. Najbolj znana in uporabljana distribucija v vgrajenih napravah je Monta Vista Linux (MVL), ki s svojimi dopolnitvami jedra podira vse rekorde. Primerjava odzivnosti med originalnim 2.6.12.3 in MVL jedrom 2.6.10 pokaže, da je razlika resnično velika. Tabela 5.1 prikazuje hitrosti Linux jeder.

Meritve je opravil ponudnik MVL na računalniku Pentium4 3.2GHz in meril 20 ur pod maksimalno obremenitvijo. Dani podatki kažejo, da je MVL za dani namen primerna, seveda pa rezultati meritev ne morejo biti boljši kot jih ponuja samo jedro.

	Originalno jedro 2.6.12.3	MVL jedro 2.6.10
Skupno število vzorcev	72, 159, 547	72, 245, 786
Povprečna latenca	9 mikro s	2 mikro s
Prehodni čas pod 10us	66.66%	99.27%
Prehodni čas pod 100us	99.98%	100%
Maksimalna prehodni čas	2036 mikro s	65 mikro s (30x bolje)
Min. prekinitveni prehodni čas	997 mikro s	47 mikro s (20x bolje)
Prehodni čas ob preklopu (max)	241 mikro s	20 mikro s (10x bolje)

Tabela 5.1: Primerjava hitrosti Linux jeder [15]

5.2 Uporaba odprte kode za zajem signalizacije

Obstaja nekaj odprtokodnih projektov, ki se ukvarjajo z implementacijo signalizacije številka 7. Najbolj znan je OpenSS7 projekt. Implementacija zajema SS7 lahko temelji na implementaciji SS7 tako da uporabimo samo del za sprejem, del za oddajo pa izključimo. Za polno izkoriščenost fizičnih portov - priključkov moramo oddajnim priključkov spremeniti konfiguracijo, da delujejo kot sprejemni.

5.2.1 Odprta koda in licence

Pri uporabi odprte kode se moramo zavedati nekaj dejstev v zvezi z licenciranjem kode pod licenco GPL.

Linus Torvalds je izdal Linux jedro, ki je pokrito z GPL (General public Licence) licenco, kar na kratko pomeni, da lahko uporabljamo in distribuiramo njegovo kodo brez plačila licenc, vendar pod pogojem, da daste kupcem na voljo tudi izvorno kodo. Če izvorno kodo spreminjate in jo prilagajate svojim potrebam, pade vaše delo avtomatsko pod GPL licenco, ker izhaja iz izdelka, ki je bil pokrit z GPL licenco. Tukaj se ponavadi pojavi strah, da so vsi izdelki, ki temeljijo na Linux-u, avtomatsko pokriti z GPL licenco. Če bi bilo to res, bi to

pomenilo, da bi vsi naši konkurenti imeli vedno na voljo izvorno kodo. Vendar to vsekakor ni povsem tako. Poglejmo si najprej, kakšno posledico ima GPL na gonilnike, ki jih zelo verjetno rabimo pri svojem izdelku. Pri Linux-u lahko gonilnik naprave uporabimo na dva načina. Lahko ga prevedemo skupaj z jedrom in je torej statično vključen v jedro. Druga možnost je, da ga prevedemo posebej in ga dinamično vstavimo v delujoče jedro. Pri prvem načinu naš gonilnik avtomatsko pade pod GPL licenco in moramo izvorno kodo razkriti. Če pa gonilnik vstavimo v delujoče jedro dinamično, se izognemo GPL licenci in gonilnik ostane naša intelektualna lastnina. Podobno je pri programski opremi. Če je program povsem naš in ne vsebuje delov programov, ki so pokriti z GPL licenco, potem lahko naš program distribuiramo brez GPL licence, razen če si tega ne želimo sami. Če naš program vsebuje dele programov, ki so pokriti z GPL, potem tudi naš program avtomatsko pade pod GPL. Ravno tako lahko naš program prizadene GPL, če ga statično ali dinamično povezujemo s knjižnicami, ki so pokrite z GPL. Ker bi to pomenilo, da je skoraj nemogoče napisati program brez GPL licence, je večina knjižnic pokrita z LGPL licenco (tudi glibc), ki nam omogoča razvoj programske opreme brez implikacije GPL licence. Linux in GPL torej ne pomenita, da bomo morali naše znanje posredovati drugim.

5.2.2 OpenSS7

OpenSS7 je odprtokodni razvojni projekt. Njegov namen je posreduje robusten in pod licenco GPL narejen sklad za SS7 in SIGTRAN za Linux in druge UNIX tipe operacijskih sistemov. Namen OpenSS7 je poskus razširitve uporabe SS7 zunaj operaterskih skupnosti. Glavni razlogi za to so:

1. Visoka Cena: Komercialni in zaprti SS7 skladi so zelo dragi. Visoka cena predstavlja problem za male podjetja in raziskovalce, da bi preizkušali SS7 in tako pripomogli k izboljšavi protokola in večji robustnosti ter efektivnosti že implementiranih produktov. OpenSS7 rešuje ta problem z odprtokodnim

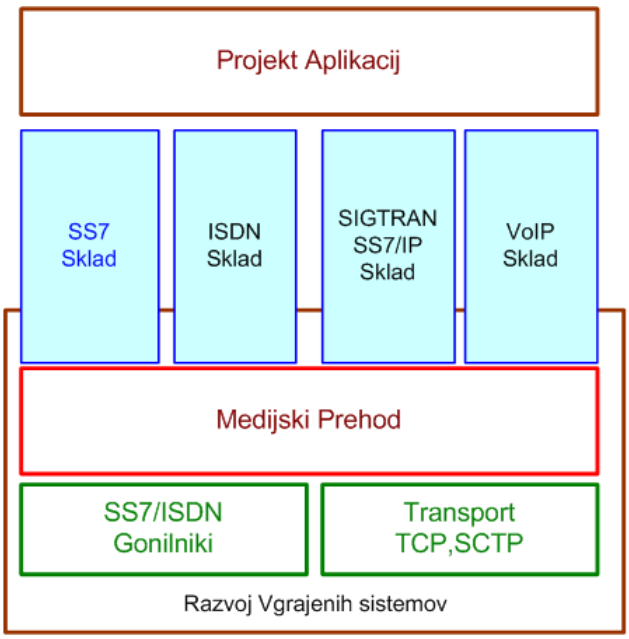
in javno dostopnim SS7 skladom.

2. Kompleksnost: Komercialni SS7 skladi so navadno zgrajeni skupaj z velikimi telekomunikacijskimi produkti in paketi, zato je težko razvijati in integrirati enostavne aplikacije bazirane na SS7.

3. Sodelovanje: Lastniški SS7 sklad imena navadno zaščiteno izvorno kodo, ki ni dostopna drugim. Z odprto kodo lahko veliko pregledovalcev prispeva k boljši implementaciji in večji robustnosti kode.

4. Strokovno znanje: SS7 sklad z dobro definiranim aplikacijskim vmesnikom, omogoča razvijalcem aplikacij lažje delo in manj potrebnega strokovnega znanja o sami implementaciji SS7 na nižjih slojih.

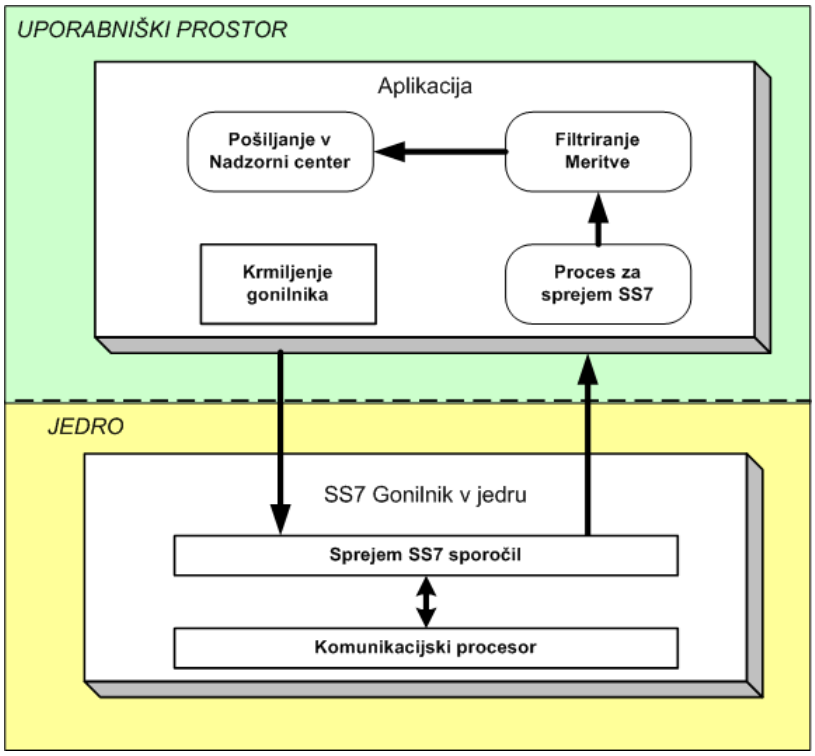
Slika 5.2 prikazuje področje dela OpenSS7 projekta. Področje vključuje projekte od razvoja v vgrajenih sistemih do posebnih aplikacijskih projektov. Glavno področje dela je SS7 sklad, SIGTRAN sklad, gonilniki in transportni skladi.



Slika 5.2: OpenSS7 projekt [10]

5.3 Zasnova sonde za zajem SS7 na Linuxu

Podatke iz signalnega linka zajema gonilnik (driver) SS7. Iz obeh smeri signalnega linka zajema signalne enote in jih najprej obdela ločeno (na zunanjem linku ne moremo govoriti o sprejemni Rx in oddajni Tx smeri). Analiza je podobna kot pri aktivnem signalnem linku (Q.703). Nekateri parametri iz obeh smeri se primerjajo in ugotovi stanje linka ter morebitni alarm. Sprejeta MSU sporočila se filtrirajo in opremijo z glavo. Preko TCP/IP se pošljejo v nadzorni center in shranijo v krožni pomnilnik (buffer) na disk. Hkrati z nadzorom linka in zajemom signalnih sporočil se izvajajo meritve Q.752. Po izteku merilnega ciklusa, na zahtevo iz nadzornega centra, se rezultati opremijo z glavo in pošljejo v nadzorni center.



Slika 5.3: Zasnova sonde za zajem SS7

Programska oprema na sondi je razdeljena na dva dela:

- modul - SS7 gonilnik , ki teče v jedru,

- aplikacijski del.

Gonilniki je obliki dinamičnega modula[2] v jedru Linuxa. Dinamični modul je primernejši zaradi ohlapnejše licence LGPL in enostavnega dodajanja v jedro. Linux omogoča nalaganje delov jedra po potrebi (funkcionalnost zelo podobna .dll datotekam v Oknih)- taki moduli so dinamični, tisti, ki so del samega jedra pa so statični.

Zelo pomemben del gonilnika je komunikacija med prilagoditvenim delom in delom v jedru (komunikacija modul - aplikacija).

5.3.1 Komunikacije med uporabniškim prostorom in modulom v jedru

Operacijski sistem navadno razdeli sistemski pomnilnik na jedrni prostor (kernel space) in uporabniški prostor (user space). Jedrni prostor je strogo rezerviran za pogon jedra, gonilnikov za naprave in razširitev jedra. Na drugi strani pa je uporabniški prostor v pomnilniku uporabljen za vse uporabniške aplikacije. V ta namen je potrebno za komunikacijo med gonilnikom in aplikacijo uporabljati posebne metode.

Komunikacija med aplikacijo in jedrom poteka preko IOCTL funkcije[3]. Preko IOCTL se modulu v jedru posreduje ukaze za izvedbo posamezne funkcije.

V parametrih IOCTL se poda kazalec na strukturo z informacijami posameznega ukaza. Vsebina te strukture se potem lahko prenese v jedro z različnimi metodami. Klic IOCTL povzroči klic funkcije na nivoju jedrnega dela gonilnika, kjer se znotraj te funkcije odloča glede na ukaz, ki je bil vhodni parameter v funkcijo. Ena izmed enostavnejših metod komunikacije med jedrom in aplikacijo, primerna tudi za prenašanje večjih blokov podatkov je uporaba funkcij *copy_from_user*(cilj, izvor, dolžina), *copy_to_user* (cilj, izvor, dolžina).

[2]Modul (kernel module) je binarna izvedljiva oblika, ki predstavlja funkcionalno razširitev jedra. Modul je minimalna oblika kode, ki se da naložit v jedro

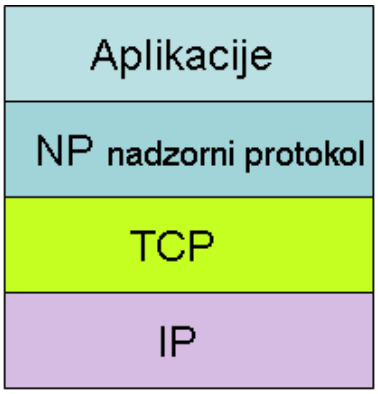
[3]IOCTL je sistemska funkcija v Linuxu namenjena za posredovanje ukazov modulu v jedru.

Ko posredujemo ukaze in informacije do jedra, jih zapišemo v ustrezni člen strukture in te informacije potem preberemo iz strukture. Posamezna kopiranja se opravijo s funkcijama *copy_from_user* in *copy_to_user*. Funkciji se poleg prenašanja podatkov ukazov uporabita tudi za prenos okvirjev.

5.3.2 Komunikacija z nadzornim centrom

Povezava med sondo SS7 in nadzornim centrom poteka preko interneta/intraneta po protokolu TCP/IP. S stališča protokola TCP/IP je nadzorni center strežnik (server), sonda pa uporabnik (client). Ob zagonu sonda SS7 poskušala vzpostaviti povezavo TCP/IP do nadzornega centra. (Nato se center poveže s sondo z nadzornim protokolom).

Glede na specifikacijo funkcij se različne tipe sporočil prenaša med sondo in nadzornim centrom preko treh različnih port-ov[4]. Glavni razlog za to je, da se zagotovil pošiljanje različnih sporočil preko različnih vrst in omogoči prehitevanje. Na aplikacijskem nivoju se uporablja namensko narejen protokol, ki se imenuje Nadzorni protokol (NP).



Slika 5.4: Vmestitev nadzornega protokola

Nadzorni protokol je protokol, ki je s stališča ISO OSI referenčnega modela pozicioniran nad protokolom TCP/IP (slika 5.4). Za natančen opis protokola

[4]Logični priključki na nivoju povezave TCP

med sondo in nadzornim centrom je torej potrebno definirati delovanje protokola TCP/IP in delovanje nadzornega protokola.

S stališča protokola TCP/IP je nadzorni center strežnik (server), sonda pa uporabnik (client). Ob zagonu sonda SS7 poskušala vzpostaviti povezavo TCP/IP do nadzornega centra. (Nato se center poveže s sondo z nadzornim protokolom).

Glede na specifikacijo funkcij se različne tipe sporočil prenaša med sondo in nadzornim centrom preko treh različnih port-ov (logičnih priključkov na nivoju povezave TCP). Glavni razlog za to je, da se zagotovil pošiljanje različnih sporočil preko različnih vrst in omogoči prehitevanje.

Prenos zajetih podatkov

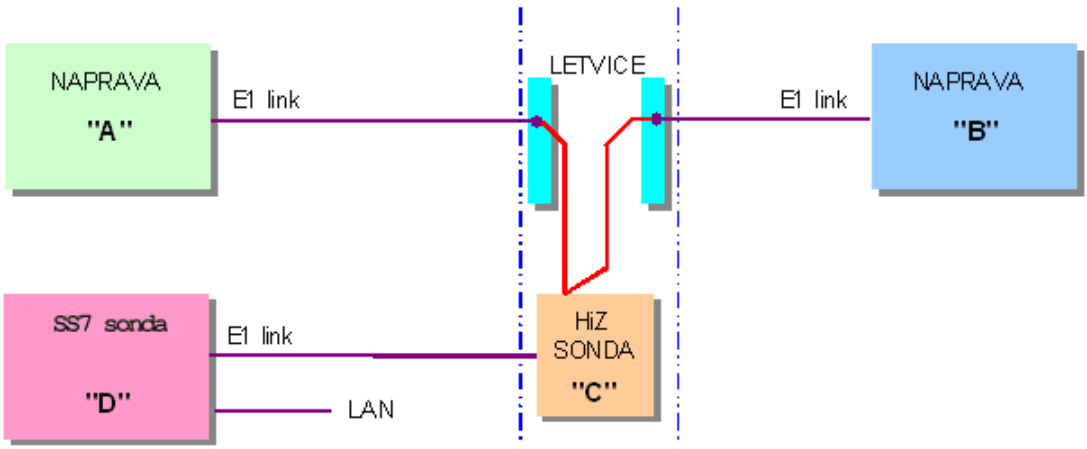
Pri pošiljanju podatkov iz sonde v nadzorni center se uporablja povezavno orientiran protokol TCP. Vzdržuje se TCP seja, po kateri pošiljamo podatke. Ker deluje sistem v realnem (sprotnem) času je potrebno zagotoviti dovolj kvalitetno omrežje. TCP omogoča zanesljiv prenos podatkov, odpravljanje napak – ponovno pošiljanje segmentov v primeru izgube le-teh številčenje paketov (sekvenčne številke) in razvrščanje v pravem zaporedju. S krmiljenjem pretoka in zamašitev TCP preprečuje stanja, v katerem bi potrebe po virih presegale količino razpoložljivih virov.

V paketnih omrežjih lahko pri večjih razdaljah pride do velikih zakasnitev in prekinitev povezav. Zaradi teh problemov je potrebno pri vzpostavljanju TCP seje uporabiti NON_BLOCKING[5] tipa TCP vtičnice (socket). To pomeni da vtičnica ne bo blokirala procesa pri pošiljanju zaradi čakanja na sistemska sredstva. S tem dobimo v aplikaciji delno kontrolo nad TCP sejo. Aplikacija mora poskrbeti, da se vsa sporočila pošljejo. Medtem ko v prejšnjem primeru za to poskrbi TCP.

[5]Opcija pri kreiranju vtičnice, pomeni način delovanja vtičnice

5.3.3 Visokoohmsko priključevanje

Nadzorna sonda se na omrežje SS7 (E1 PCM) priključuje na delilniku. Priključevanje nadzorne sonde SS7 na se izvaja s pomočjo visokoohmskega ločilnega člena (HiZ modul), kot je prikazano na Slika 5.5.



Slika 5.5: Princip vključitve v E1 link preko visokoohmskega modula

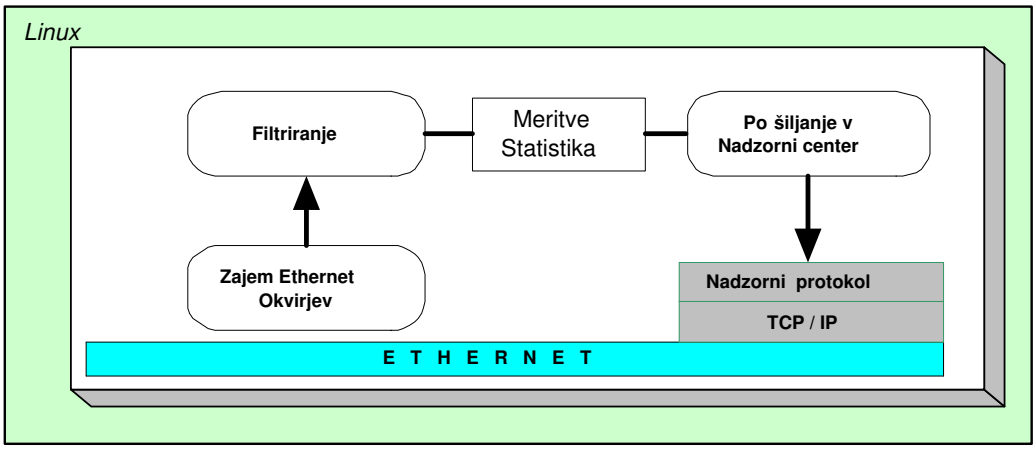
5.4 Razširitev sonde na zajem SIGTRAN signalizacije

Nadzor SIGTRAN signalizacije je namenjen zajemu SS7 signalizacijskih sporočil pri prenosu preko IP in njihov prenos v aplikacijo za obdelavo le teh v realnem času. Dejansko pomeni razširitev sistema za nadzor SS7 na nadzor signalizacij preko IP. Promet zajemamo na Ethernet nivoju in ga potem filtriramo. Po filtriranju najprej SCTP prometa se potem iz M3UA sporočila filtrira sporočilo SS7 signalizacije. M3UA namreč samo prenaša SS7 preko IP. Kot transportni protokol pa se uporablja SCTP. Zajeta SS7 sporočila se potem preko TCP transportnega protokola prenašajo do nadzornega centra, kjer aplikacija v kontrolnem centru obdela ta sporočila.

Na aplikacijskem nivoju je uporabljen Nadzorni protokol.

Aplikacija je sestavljata dveh niti[6]:

- nit za zajem paketov na Ethernetu in filtriranje,
- nit za pošiljanje podatkov Net Inspectorju.



Slika 5.6: Arhitektura aplikacije na sondi za zajem SIGTRAN signalizacij

Za zajem paketov na Ethernet nivoju je bila uporabljena knjižnica libpcab. Knjižnica vsebuje funkcije za zajem in filtriranje okvirjev na Ethernet nivoju. Programska oprema sonde za zajem SIGTRANa je sestavljena iz treh delov:

- zajem in filtriranje podatkov,
- komunikacijski del,
- meritve in statistika.

Filtriranje SS7 sporočil poteka v treh korakih:

- filtriranje SCTP datagrama,
- filtriranje M3UA,

[6]Razlika niti od procesov je v tem, da si niti delijo uporabo osnovnih sredstev (npr. delajo nad skupnimi podatki).

- filtriraje SS7 sporočila.

Vsebino zajetega okvirja za IAM sporočilo prikazuje slika 5.7

```
▷ Frame 12 (130 bytes on wire, 130 bytes captured)
▷ Ethernet II, Src: 00:d0:50:00:3f:f8, Dst: 00:50:04:32:c7:03
▷ Internet Protocol, Src Addr: 10.0.6.63 (10.0.6.63), Dst Addr: 10.0.6.8 (10.0.6.8)
▽ Stream Control Transmission Protocol
    Source port: 2905
    Destination port: 2905
    Verification tag: 0x7ba25b46
    Checksum: 0x9d109ff1 (correct CRC32C)
  ▷ DATA chunk(ordered, complete segment, TSN: 11780, SID: 6, SSN: 0, PPID: 3, payload length:
▽ MTP 3 User Adaptation Layer
    Version: Release 1 (1)
    Reserved: 0x00
    Message class: Transfer messages (1)
    Message type: Payload data (DATA) (1)
    Message length: 68
  ▷ Routing context (1 context)
  ▷ Protocol data (SS7 message of 35 bytes)
▽ ISDN User Part
    CIC: 5
    Message type: Initial address (1)
  ▷ Nature of Connection Indicators: 0x0
  ▷ Forward Call Indicators: 0x2001
  ▷ Calling Party's category: 0xa (ordinary calling subscriber)
  ▷ Transmission medium requirement: 0 (speech)
  ▷ Called Party Number: 7060060
    Pointer to start of optional part: 8
  ▷ Calling Party Number: 2130
  ▷ Access transport (4 bytes length)
  ▷ User service information, (3 bytes length)
    End of optional parameters (0)
```

Slika 5.7: Vsebina okvirja pri prenosu IAM

Prestrezanje paketov

Za zajem SIGTRAN signalizacij moramo zajemati okvirje na Etrhernet nivoju. Poznamo več načinov prestrezanja paketov:

1. Uporaba stikala v zrcalnem načinu.V osnovnem načinu delovanja stikala, je sondi, priključeni na enega od njegovih fizičnih vmesnikov, prestrezanje paketov onemogočeno. Nanj namreč prispejo le paketi s ponornimi naslovi MAC[7] (Media Access Control), ki ustrezajo tovarniško vgrajenemu naslovu

[7]Fizičen naslov, ki enolično označuje vsako napravo v omrežju.

MAC omrežnega vmesnika. Potreben je administratorjev poseg v konfiguracijo stikala, to je nastavitev poljubnega stikalnega vmesnika na delovanje v zrcalnem načinu (mirroring/hub mode). Ta način omogoča prisluškovanje aktivnostim na poljubnih vratih stikala.

2. Uporaba optičnega T člena v optičnih omrežjih. Prednost tega načina je, da ne posegamo aktivno v signal, prav tako pa nimamo nobenega aktivnega elementa. Vendar pa moramo uporabo takih T členov upoštevati že pri gradnji optičnega omrežja.

3. Uporaba vozla (hub). Zaradi uporabe Half-Duplex načina se vozli vedno manj uporabljajo.

5.5 Testni sistem za nadzor signalizacij

V namene testiranja sond za zajem signalizacije smo v Laboratoriju za telekomunikacije uporabili Aplikacijo Net Inspektor, ki je del sistema za nadzor SYMONET proizvajalca Iskratel.

Net Inspector je splošen in odprt program za nadzor naprav na daljavo. Net Inspector Engine (Engine) deluje kot strežnik in nima uporabniškega vmesnika, ampak se v ozadju izvaja kot servis, ki nadzira naprave. Net Inspector Client pa se poveže z Enginom in nudi uporabniški vmesnik za Engine. Nadzorovane naprave kontaktira in nadzoruje Engine, ki prav tako skrbi tudi za pošiljanje obvestil oddaljenemu uporabniku. S pomočjo Clienta se lahko nastavljajo parametri delovanja Engine aplikacije in se tako posredno nadzirajo naprave. Več Clientov se lahko hkrati poveže na isti Engine. Na ta način je možen oddaljen nadzor naprav z različnih lokacij. Uporabnost Net Inspectorja je odvisna od števila in tipa inštaliranih Proxy Front-end Server (PFS) modulov. PFS moduli komunicirajo z agenti na nadzorovanih napravah po poljubnem mediju (LAN, WAN, ISDN, PSTN, serijski, ...) in prenašajo podatke o stanju nadzorovanih

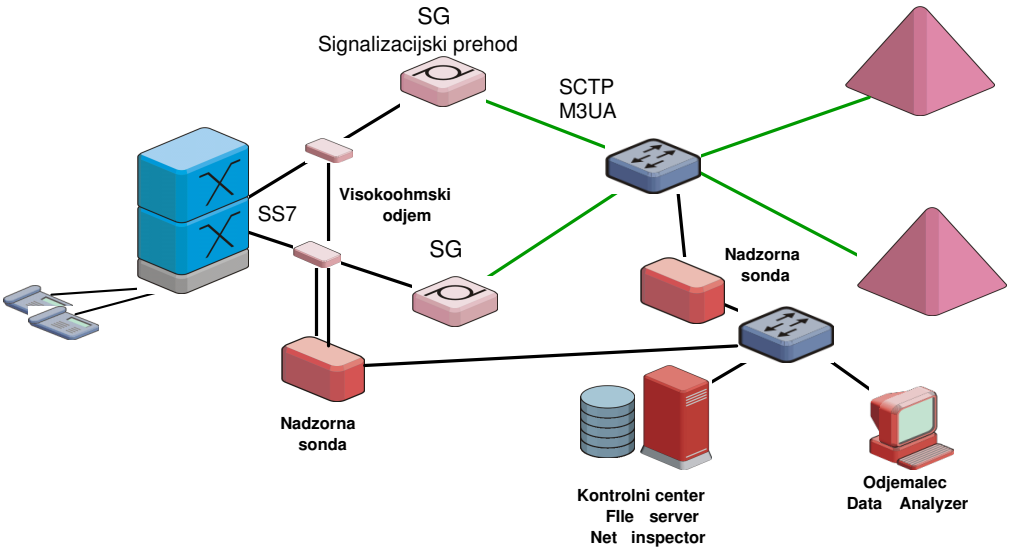
naprav Net Inspectorju preko PFS aplikacijskega programskega vmesnika. Net Inspector omogoča zbiranje, zapisovanje ter obdelavo podatkov in dogodkov, ki jih posredujejo PFS moduli. User Notification Carrier (UNC) moduli omogočajo posredovanje obvestil ali dogodke na sistemu oziroma iz nadzorovanega omrežja preko elektronske pošte (e-mail) z uporabo SMTP protokola ali SMS-ov z uporabo TAP in UCP protokolov. Modularna zasnova aplikacije Net Inspector na bazi PFS modulov omogoča veliko razširljivost sistema tako s stališča protokolov (NGN) kot z vidika funkcionalnosti. Nadzorni sistem Net Inspector je zasnovan kot strežnik in odjemalec. Net Inspector strežnik (Net Inspector Engine - NIE) deluje v okolju Windows ter omogoča povezavo z odjemalci preko interneta/intraneta, ki so realizirani v okolju Windows NT/2000/XP ali pa kot Java aplikacija. Net Inspector strežnik nima uporabniškega vmesnika. Uporabniški vmesnik predstavlja Net Inspector odjemalec (Net Inspector Client - NIC). Z uporabo Net Inspector odjemalca se lahko nastavijo vsi parametri delovanja strežnika.

V sistemu SYMONET se za prikaz podatkov uporablja aplikacija Data Analyzer (DA). Data Analyzer (DA) aplikacija deluje kot podatkovni odjemalec v okolju Windows 2000/XP ter omogoča povezavo s podatkovni strežniki (File Server aplikacija) preko interneta/intraneta. Data Analayzer aplikacija komunicira s File Server aplikacijo preko TCP/IP povezave s File Server protokolom (FSP).Data Analyzer aplikacija omogoča prikaz in naknadno obdelavo podatkov, ki so shranjeni na podatkovnem strežniku.

Prototip nove sonde smo povezali z aplikacijo Net inspector. V našem primeru smo za zajem SS7 signalizacije uporabili SYMONET sondo, za zajem SIGTRAN signalizacije pa novo sondo. Vkljucitev nove funkcionalnosti sonde ni potrebovala sprememb v Net inspectorju. S stališča Net inspectorja je bila nova sonda kot navadna sonda za zajem SS7. Končni cilj obeh sond je prenos SS7 sporočil do Nadzornega centra, ne glede na to kje so bila zajeta (na SS7 linku ali na IP pri prenosu SS7/IP).

Signalizacijski promet med signalizacijskim prehodom in klicnim strežnikom

smo zajemali na fizičnem vmesniku, ki je bil nastavljen na delovanje v zrcalnem načinu. Shemo testnega okolja prikazuje slika 5.8.



Slika 5.8: Testno okolje

6. Zaključek

Potreba po nadzoru siganlizacij se povečuje. Za operaterje je nadzor siganlizacij pomemben vir informacij za upravljanje in načrtovanje telekomunikacijskih omrežij.

Namen magistrskega dela je bila zasnova sonde za zajem SIGTRAN signalizacij. Za osnovo je bila vzeta nadzorna sonda produkta SYMONET. Za izboljšanje zmogljivosti sonde je potrebno zamenjati strojno opremo. Na razpolago imamo veliko platform s komunikacijskimi kontrolerji. Testni primer sonde smo naredili na platformi z komunikacijskim kontrolerjem PowerQuick III. Uporabili smo operacijski sistem Linux distribucije Montavista. Uporabljena distribucija vsebuje popravke Linux jedra za delo v sprotnem času.

Zasnova nove sonde je taka, da v primerjavi z SYMONET sondo, izboljša zmogljivosti zajema SS7 signalizacije in omogoča nadzor SIGTRAN signalizacije. Rešitev osnovana na linux platformi nudi dovolj možnosti za razširitve na zajem drugih signalizacij v omrežjih nove generacije.

Za zajem drugih signalizacij v NGN je potrebno v Aplikativnem delu sistema implementirati zapis podatkov klica in storitev IPDR.

Prikazana zasnova pomeni enega od načinov razširitve in nadaljnjega razvoja sistema SYMONET.

7. Uporabljene kratice

IPDR	Internet Protocol Detail Record	Razčlenjeni zapis IP
UDR	Usage Data Records	Zapis podatkov o uporabi
ISO	International Organization for Standardization	Mednarodna organizacija za standardizacijo
TCP	Transmission Control Protocol	Protokol za krmiljenje prenosa
MAC	Media Access Control	Fizični naslov
ETSI	European Telecommunications Standards Institute	Evropska inštitucija za standatdizacijo v TK
IETF	Internet Engineering Task Force	
ISUP	ISDN User Part	ISDN uporabniški del
M3UA	MTP3 User Adaptation layer	MTP3 Uporabniški prilagodilni sloj
MEGACO	Media Gateway Control	Protokol za kontrolo medijskih prehodov
QoS	Quality of Service	Kvaliteta storitve
TDM	Time Division Multiplex	Časovni multipleks

NGN	Next Generation Networks	Omrežja nove generacije
SS7	Signalling System no. 7	Signalizacija številka 7
PSTN	Public Switched Telephone Network	Javno komutirano telefonsko omrežje
SSP	Signalling Switching Point	Točka preklapljanja storitev
STP	Signalling Transfer Point	Točka prenosa storitev
SCP	Signalling Control Point	Točka krmiljenja storitev
PBX	Private Branch Exchange	
ISDN	Integrated Services Digital Network	Digitalno omrežje s storitvami
TCP	Transmission Control Protocol	Protokol za krmiljenje transporta
IP	Internet Protocol	Internetni protokol
VoIP	Voice over IP	Prenos govora preko IP
SMS	Short Messaging Service	Kratka besedna sporočila
QoS	Quality of Service	Kvaliteta storitev
ITU	International telecommunication union	Mednarodna organizacija za telekomunikacije
NTP	Network Time Protocol	Protokol omrežnega časa
CDR	Call Detail Records	Podrobni zapis o klicu
MTP	Message Transfer Part	Sporočilno-prenosni del
GPL	General public Licence	Odprtokodna licenca
OPC	Originating point code	Koda izvorne točke
DPC	Destination point code	Koda usmeriščne točke
CIC	Circuit identification code	Koda za identifikacijo voda
DCN	Data communication network	Omrežje za podatkovne komunikacije

Literatura

[1] ITU-T Rec. Q.752, *Monitoring and Measurements for Signalling System No. 7 Networks*, (06/97).

[2] ITU-T Recommendation E.422, *Observations on international outgoing telephone calls for quality of service*, (02/96).

[3] ITU-T Recommendations Q.700, *Introduction to CCITT Signalling System No.7.*

[4] ITU-T Recommendations Q.701, *Functional Description of the Message Transfer Part.*

[5] ITU-T Recommendations G.772, *Monitoring Point*

[6] R. J. Bolton, D. J. Hand, *Statistical Fraud Detection: A Review*, 2002.

[7] P. Burge, J. Shawe-Taylor, C. Cooke, Y. Moreau, B. Preneel, C. Stoermann, *Fraud Detection and Management in Mobile Tellecommunications Networks.*

[8] RFC 2960, *Stream Control Transmission Protocol.*

[9] RFC 2719, *Framework Architecture for Signaling Transport*

[10] `http://www.openss7.org`, Overview.

[11] `http://http://www.ipdr.org/public/DocumentMap/DocMap.htm`

[12] `http://webtool.iskratel.si/PRODUCTS_slo.asp?book=resitve/Control_and_management_solutions/Network_performance_monitoring_and_control.htm`.

[13] `http://thc.org/papers/C7-MONIT.TXT`, *CCiTT SS7 Monitoring*

[14] `http://www.linuxdevices.com/articles/AT7342059167.html Linux, Windows neck-and-neck in embedded`, Rick Lehrbaum (Oct. 29,2002).

[15] `http://www.mvista.com/products/realtime_benchmarks.html`, *Real-Time Linux Benchmark*.

[16] `http://www.cotsjournalonline.com/home/article.php?id=100129&pg=1`, *Linux for Embedded Systems*, Green Hills Software, Santa Barbara, CA.

[17] MA Bihina Bella, JHP Eloff, MS Olivier *Using IPDR standard for NGN biling anf fraud detection*, Information and Computer Security Architectures (ICSA) Research Group Department of Computer Science University of Pretoria, Pretoria South Africa

[18] Andrej Krenker, Roman Kotnik, Franci Katrašnik, *Nadzor signalizacij v telekomunikacijskih omrežjih*, ERK 2004.

[19] Rok Ostrovršnik,*Uporaba RTLinux-a v sistemih avtomatizacije, diplomsko delo* , Maribor 2002.

[20] Craig Hollabaugh, *Embedded Linux: Hardware, Software, and Interfacing*, Addison-Wesley 2004.

[21] Lee Dryburgh, Jeff Hewett *Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services*, Cisco Press.

[22] Rok Žurbi, *Signalizacijski in krmilni protokoli v omrežjih naslednje generacije, magistrsko delo* , Ljubljana 2001.

[23] Andrej Krenker, *Detekcija zlorab, Seminar*, Ljubljana 2005.

[24] Tine Stegel, *Zanesljivosti in redundanca v SIGTRAN protokolih, diplomsko delo* , Ljubljana 2005.

Izjava

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