

# Prenos signalizacije SS7 preko IP, problemi i rješenja

Dragan Soldat

**Sadržaj** — Ovaj rad govori o problemima koji se sreću pri penosu signalizacije SS7 kroz paketske IP mreže i načinu njihovog prevazilaženja. Poseban akcenat je stavljen na probleme koje srećemo na transportnom sloju IP protokol steka i njihovom prevazilaženju definisanjem novog transportnog sloja SCTP.

**Ključne riječi** — SCTP, Signalizacija, Transportni sloj, VoIP,

## I. UVOD

SIGNALIZACIJA SS7 je univerzalni sistem signalizacije u telefonskim mrežama i trenutno je najzastupljeniji. Koristi se samo za prenos signalizacijskih poruka između elemenata mreže (telefonske centrale) a ne i kao korisnička signalizacija koja se razmjenjuje između krajnjih uređaja (telefon na primjer) i pristupnog elementa mreže (krajnja telefonska centrala). Spada u grupu sistema signalizacije po zajedničkom kanalu koji je odvojen od kanala koji prenose korisnički saobraćaj. Po ovom kanalu se razmjenjuju signalizacione poruke odgovorne za uspostavu, držanje i raskid veze, rutiranje, tarifiranje kao i širok spektar drugih informacija koje se razmjenjuju u javnoj telefonskoj mreži. SS7 nije jedinstven protokol već predstavlja skup protokola koji funkcionišu zajedno u cilju ostvarivanja prenosa signalizacionih poruka. Ove poruke su u suštini računarske HDLC (*High level Data Link Control*) poruke koje se prenose paketima između čvorova SS7 mreže koji su u stvari računari. Signalizaciona SS7 mreža je u principu potpuno razdvojena od mreže za prenos korisničkih informacija. Međutim, u praksi su ove dvije mreže prilično povezane na taj način da su elementi koji upravljaju signalizacionom mrežom tj. signalizacioni čvorovi smješteni obično u komutacionim čvorovima krajnjih i tranzitnih centrala (računar koji upravlja komutacijom i računar za signalizaciju se nalaze na istom mjestu). Moguća je i arhitektura, naročito kod starijih sistema, gdje je jedan dio resursa komutacionog čvora dodjeljen za upravljanje signalizacijom. Povezanost u prenosnom djelu ove dvije mreže je još veća, naime, SS7 signalizacione veze se realizuju alokiranjem prenosničkih PCM slotova (trankova). To je obično 16-ti slot jednog PCM linka iz

grupe linkova koji povezuju određeni pravac (rutu). Jedan ovakav signalizacioni link može da prenosi signalizacione informacije za do 1500 prenosničkih kanala. Radi pouzdanosti ovi kanali se obično udvajaju. Računari koji čine signalizacionu mrežu se nazivaju Signalizacione tačke. Pored prenosa signalizacionih poruka najčešći zahtjevi koji se postavljaju pred SS7signalizacionu mrežu su:

-**pouzdanost**: garantovana isporuka signalizacionih poruka kao i integritet njihovog sadržaja;

-**raspoloživost**: otpornost mreže na ispad iz rada. Pod ovaj zahtjev se može svrstati i zahtjev za radom i u slučaju otkaza pojedinih elemenata mreže. To se obično postiže udvajanjem osnovnih elemenata mreže;

Upravo velika pouzdanost je najvažnija karakteristika SS7 sistema signalizacije. Naime, ovaj sistem veoma lako ispunjava propisane norme u pogledu vjerovatnoće greške i kašnjenja (na primjer, vjerovatnoća gubitaka poruke ne smije biti veća od  $10^{-7}$ , a vjerovatnoća da poruka stigne u pogrešnom redoslijedu ne smije biti veća od  $10^{-10}$ ). Današnji komutacioni sistemi upravo zahvaljujući robusnosti i pouzdanosti sistema SS7 veoma lako zadovoljavaju tolerancije od svega nekoliko minuta totalnog ispada u toku godine. Ličnim iskustvom kao radnik na digitalnom komutacionom sistemu Siemens EWSD koji koristi SS7 sistem signalizacije mogu potvrditi da ovaj sistem od svoje instalacije 1999 godine do danas nije imao ni jedne sekunde totalnog ispada.

## II. PRENOS SS7 PREKO PAKETSKIH IP MREŽA

Ukoliko telefonski saobraćaj želimo da prenosimo preko paketske IP mreže (VoIP- Voice Over IP) tada ćemo morati prenositi i SS7 signalizacione poruke preko te iste mreže. Ovakva mreža je obično implementirana ili H.323 ili u *Softswitch* tehnologiji. Razmjena signalizacionih poruka (na primjer, IAM-*Initial Address Message* i ACM-*Answer Message*) između komunikacionih entiteta kroz SS7 mrežu traje najviše do 2 sekunde. U paketskoj IP mreži je za prenos ovih poruka potrebno izvršiti veliki broj transakcija i izmijeniti veliki broj raznih poruka između raznih entiteta mreže i postavlja se logično pitanje da li je paketska mreža sposobna da ispuni stroge zahtjeve SS7 signalizacije. Na rješenju ovog problema radi mnogo zainteresovanih grupa a najdalje je otišla IETF (*Internet Engineering Task Force*) radna grupa SIGTRAN (*SIGnaling TRANsport*).

Ova radna grupa je osnovana 1999 godine sa ciljem definisanja protokola koji omogućava prenos SS7 signalizacije preko IP mreža u relnom vremenu. U cilju ispunjenja ovog zahtjeva SIGTRAN radna grupa je definisala skup protokola za prenos SS7 i ISDN poruka preko IP mreža:

-**SCTP** (*Stream Control Transmission Protocol*): novi transportni protokol ;

-niz **adaptacionih nivoa** za prilagođenje korisniku, UA (*User Adaptation*), koji svojom funkcionalnošću oponašaju servise nižih nivoa arhitekture SS7 i ISDN protokol steka;

Jedan od osnovnih zahtjeva paketske mreže prilikom prenosa SS7 signalizacionih poruka je preslikavanje kodova signalizacionih tačaka u IP adrese. Dalje, pojavljuje i pitanje koji transportni protokol upotrebiti za prenos poruka. Takođe pojavljuje se problem rada SS7 aplikacija kao što je na primjer ISUP (*ISDN User Part*), u IP okruženju, koji očekuje usluge nižih nivoa (MTP – *Message Transfer Part*) kada ti niži nivoi ne postoje u IP mreži. Transportni protokol mora obezbjediti prenos ISUP poruka istom brzinom i istom pouzdanošću preko IP mreže kao da je riječ o SS7 mreži. Ukoliko koristimo standardne transportne protokole kao što su UDP (*User Datagram Protocol*) ili TCP (*Transmission Control Protocol*) ne možemo ispuniti ili zahtjev pouzdanosti ili zahtjev brzine prenosa. Naime, UDP protokol obezbjeđuje brzinu ali je zbog nedostatka mehanizma retransmisije veoma nepouzdan. Ako koristimo TCP protokol koji obezbjeđuje pouzdanu i u pravilnom redoslijedu isporuku poruka , gubimo na brzini prenosa jer ovaj protokol nije naročito brz. Iz svega ovog se nameće pitanje definisanja novog transportnog protokola Da bi riješila ove probleme SIGTRAN radna grupa je pripremila dokument RFC (*Request For Comment*) 2719 „*Framework Architecture for Signaling Transport*“ koji opisuje pristup i metodologiju za prenos signalizacije preko IP mreža.

### III. SIGTRAN ARHITEKTURA

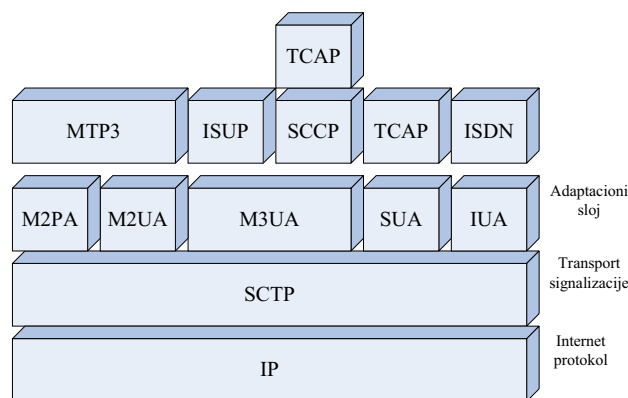
*Softswitch* arhitektura se sastoji od tri glavne komponente : MG (*Media Gateway*), MGC (*Media Gateway Controller*) i SG (*Signaling Gateway*). MG je odgovoran za konverziju i prenos govornih kanala iz PSTN (*Public Switched Telephone Network*) u paketsku mrežu i obrnuto. MGC je odgovoran za funkcije kontrole poziva kao što su uspostavljanje poziva, raskidanje poziva i monitoring nad vezom s kraja na kraj, pri čemu MGC kontroliše MG (ili više njih) koristeći *master-slave* princip uglavnom koristeći MEGACO protokol. SG služi kao interfejs za signalizaciju između PSTN i paketskih mreža gdje se vrši translacija između SS7 signala i SIGTRAN signala.

#### A. SIGTRAN protokol stek

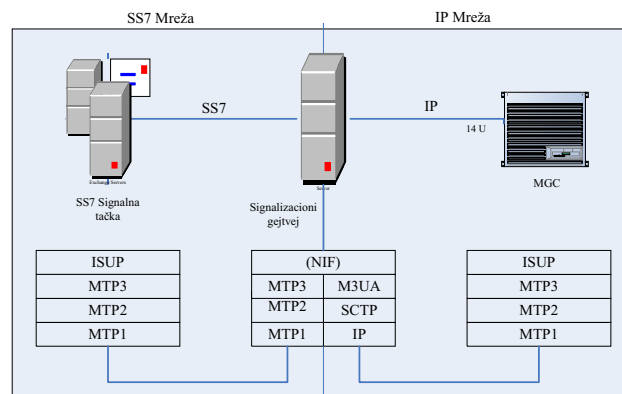
SIGTRAN protokol stek se sastoji od novog transportnog protokola za signalizaciju SCTP, niza adaptacionih podslojeva koji podržavaju specifične primitivne zahtjeve od pojedinih djelova aplikacionih protokola SS7 ili

ISDN, dok se na sloju mreže koristi IP protokol. Na Sl.1 je data SIGTRAN arhitektura koja se sastoji od tri komponente: IP protokol, SCTP i adaptacioni moduli. Kao što vidimo sa slike, u protokol steku su prisutni sledeći moduli:

-**MTP2 User Adaptation Layer (M2UA)**: M2UA prenosi MTP3 signale preko SCTP i IP umjesto MTP2 sloja SS7 i obezbjeđuje korištenje standardnog MTP3 sloja SS7 u IP mrežama. Na ovaj način IP- bazirani MGC može da komutira signalizacione poruke kao bilo koji mrežni element SS7 mreža (*STP-Signaling Transfer point* , *SCP-Service Control Point* ili *SSP-Service Switching Point*). Na Sl.2 je prikazan prenos ISUP poruke preko IP koristeći M2UA gdje je NIF- *Nodal Interworking Function*.



Sl.1 SIGTRAN arhitektura



Sl.2 Prenos ISUP poruke preko IP

-**SS7 MTP2 Peer-to-peer Adaptation Layer (M2PA)**: M2PA je protokol koji se koristi za prenos SS7 MTP3 signalizacionih poruka preko IP mreža koristeći kao transportni protokol SCTP. MTP3 poruke se u SS7 mrežama prenose između ravnopravnih MTP3 entiteta (*peer-to-peer* komunikacija). Korištenjem M2PA ovakva razmjena poruka je moguća i u IP paketskim mrežama. M2PA je dosta sličan M2UA. Razlike se ogledaju prvenstveno u dizajnu mreže, gdje SG koristeći M2PA, ima vlastitu SPC (*Signaling Point Code*) i radi kao IP – bazirani STP sa mogućnošću izvršavanja *Global Title Translation* (GTT) funkcije. M2PA je ravnopravan M2UA protokolu ali za razliku od njega ne obezbjeđuje vezu između udaljenih MTP2 i MTP3 entiteta. Funkcija MTP2

nivoa se izvršava u IP paketskoj mreži.

**-MTP3 User Adaptation Layer (M3UA):** M3UA zamjenjuje MTP3 sloj SS7 signalizacije koji koriste korisničke aplikacije (ISUP i SCCP) u IP mrežama. M3UA prenosi iste primitive prema višim slojevima kao MTP3 u SS7 ali ne obezbeđuje totalnu funkcionalnost MTP3 sloja. Generalno, M3UA se koristi između SG i MGC. Pored poruka korisničkih aplikacija preko M3UA se mogu prenositi neke poruke za upravljanje mrežom, mada M3UA ne obezbeđuje mogućnost potpunog upravljanja mrežom.

**-SCCP User Adaptation Layer (SUA):** SUA prenosi transakcione signalizacione poruke (tj. Poruke tipa upiti i odgovori za neku DB (DataBase)) kao SCCP protokol u SS7 protokol steku. MAP (Mobile Application Part), TCAP aplikacije koriste servise SUA u IP –baziranim mrežama na isti način kao što koriste SCCP u SS7 mreži.

**-SCTP:** osnovna usluga koju SCTP pruža je pouzdan prenos korisničkih poruka između ravnopravnih SCTP korisnika. Pored toga on obezbeđuje:

- prenos korisničkih podataka sa mehanizmom potvrde, bez grešaka i bez ponavljanja;

- fragmentaciju podataka kako bi njihova dužina bila prilagođena najvećoj dozvoljenoj veličini paketa koja se može prenijeti preko određene mreže;

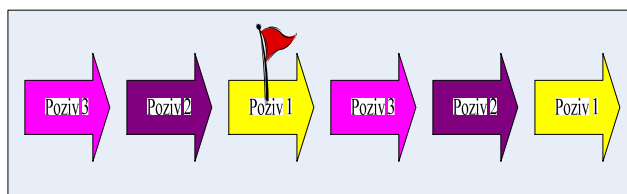
- prijem pristiglih poruka redom kojim su poslate u slučaju višestrukih tokova;

- mogućnosti prenosa različitih korisničkih poruka unutar jednog SCTP paketa;

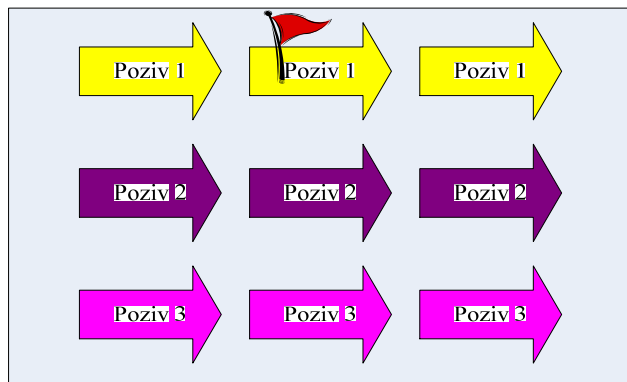
SCTP se od TCP razlikuje u dvije ključne karakteristike:

**-višestruki domaćin (multihoming):** za čvor u mreži se kaže da je višestruki domaćin ako posjeduje više IP adresa, tj. ako postoji više transportnih adresa (kombinacija IP adrese i SCTP porta) koje predstavljaju odedišnu adresu podataka koji se šalju ka tom čvoru. Protokoli višeg nivoa biraju jednu od ovih odredišnih adresa kao primarnu za slanje svojih podataka. U slučaju kvara na mreži, kada primarna postane nedostupna, podaci se usmjeravaju na alternativne odredišne adrese. TCP, za razliku od SCTP ne podržava multihoming;

**-višestruki tokovi (multistreaming):** karakteristika SCTP-a je mogućnost razdvajanja i prenosa korisničkih poruka višestrukim SCTP tokovima podataka. Ovi tokovi omogućavaju nezavisnu isporuku i isporuku u pravilnom redosljedu. Prednost višestrukih tokova je ta da ukoliko dođe do gubitka paketa u jednom toku, onda taj gubitak ne utiče na prenos paketa po drugim tokovima; Prednost korištenja višestrukih tokova možemo pokazati na primjeru ISUP protokola. Ukoliko za prenos ISUP signalizacionih paketa koristimo TCP tada svi paketi koriste jedan tok. Tako u slučaju greške na jednom paketu svi ostali paketi moraju čekati njegovu ispravnu isporuku (korištenjem metoda retransmisije) što dovodi do nedopustivog kašnjenja. SCTP koristi za svaki poziv poseban tok i tada greške na jednom toku ne utiču na ostale tokove. Ovo možemo ilustrovati na primjeru prenosa signalizacionih poruka za tri poziva:



Sl.3 Prenos signalizacionih poruka korištenjem TCP



Sl.4 Prenos signalizacionih poruka korištenjem SCTP

Sličnosti i razlike između transportnih protokola SCTP, TCP i UDP možemo dati u sledećoj tabeli:

TABELA 1: RAZLIKE I SLIČNOSTI IZMEĐU TRANSPORTNIH PROTOKOLA

Osobine protokola	SCTP	TCP	UDP
Pouzdan prenos podataka	Da	Da	Ne
Kontrola poziva	Da	Da	Ne
Očuvanje granica između poruka	Da	Ne	Da
Otkrivanje MTU rute i fragmentacija	Da	Da	Ne
Paketizacija	Da	Da	Ne
Podrška višestrukim domaćinima	Da	Ne	Ne
Podrška višestrukim tokovima	Da	Ne	Ne
Mogućnost neredosljednog isporuke	Da	Ne	Da
Sigurnosni mehanizam protiv SYN napada	Da	Ne	Ne
Provera dostupnosti ravnopravnog entiteta	Da	Ne	Ne

Pored prethodno pomenutih razlika između TCP i SCTP postoje i još neke:

**-uspostava veze i sigurnost:** oba protokola koriste skup poruka za uspostavu veze koji se međusobno razlikuju. TCP koristi princip trostrukog (*three-way*), dok SCTP koristi princip četverostrukog (*fourth-way*) rukovanja (*handshake*). Uspostavljanje veze sa TCP je kritično jer je on tada najranjiviji na napade. Najčešći napadi su SYN (poruke koje zahtevaju uspostavu veze korištenjem TCP) napadi koji utiču na otkaz resursa na strani servera jer on tada nije u stanju da prima legitimne zahtjeve za vezu. Naime, napadač šalje ogroman broj SYN zahtjeva i server tada šalje ACK poruku za prihvatanje SYN zahtjeva ka inicijatoru i zauzima određene resurse. Inicijator ne odgovara adekvatno i server ostaje u poluotvorenom stanju u kojem je od prijema SYN

zahtjeva. Server će nakon nekog vremena raskinuti vezu ali zbog velikog broja SYN zahtjeva od strane napadača neće moći primiti legitimne zahtjeve za vezom. SCTP posjeduje zaštitni mehanizam (*cookie* mehanizam) od ove vrste napada tzv. princip četverostrukog rukovanja. Kada primi zahtjev za vezom server ne zauzima resurse i u odgovoru šalje *cookie* zaštitni parametar. Tek pošto primi klijentov odgovor sa istim zaštitnim parametrom, server zauzima resurse potrebne za uspostavu veze i nazad šalje potvrdu za zadnju primljenu poruku;

**-prenos podataka:** TCP prenosi podatke između dvije krajnje tačke u vidu neprekidnog toka bajtova (*byte oriented*) i granice između korisničkih poruka nisu sačuvane. SCTP pravi jasnu razliku između korisničkih poruka i one se prijemnoj strani isporučuju u komadu. Izuzetak su poruke koje premašuju maksimalnu dužinu i one se prenose u dva ili više SCTP paketa;

**-neredosljedna isporuka poruka:** SCTP omogućava isporuku poruka različitim redom od onog kojim su poslate dok TCP nema ovu mogućnost ;

**-mehanizam potvrde:** SCTP koristi princip selektivne potvrde SACK (*Selective ACKnowledgment*) koji omogućava potvrdu prijema svih korisničkih paketa ali se potvrde ne šalju nakon svakog primljenog paketa;

**-raskid veze:** oba protokola imaju mehanizam za normalan raskid veze ali ima jedna bitna razlika. TCP omogućava poluzatvorena stanja gdje se jedan entitet u komunikaciji nalazi u otvorenom a drugi u zatvorenom stanju. Entitet u poluzatvorenom stanju ne šalje zahtjeve ali je sposoban da ih prima. SCTP ovo ne dozvoljava. Oba entiteta kada se inicira zahtjev za prekidom od strane jednog SCTP korisnika ulaze u zatvoreno stanje tek pošto su sve poruke poslone i potvrđene.

#### IV.ZAKLJUČAK

TDMA kao dominantna tehnologija za prenos govornog saobraćaja će biti u upotrebi bar još desetak godina dok ne bude u potpunosti potisnuta od strane IP ili neke druge tehnologije koja bi se eventualno pojavila u bližoj budućnosti. Zbog toga će morati uzimati u obzir specifičnosti i strogi zahtjevi ove tehnologije, naročito u pogledu prenosa signalizacije, upotrebom nekog od paketskih načina prenosa.

#### LITERATURA

- [1] IEEE NETWORK, The magazine of global interworking, Novembar/Decembar 2006, Vol. 20, No. 6
- [2] Tehnologija VoIP Sistema, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, Novi Sad, 2006 godine.
- [3] [www.nkt.ns.ac.yu](http://www.nkt.ns.ac.yu).
- [4] SSNC Operation and Maintenance tasks, Siemens documentation EWSD V 16, 2004 god.

#### ABSTRACT

This article is about problems which occur during transfer signalization SS7 over VoIP networks and about ways of overcoming these problems. Special remark is put on problems which we encounter on transportation layer TCP/IP of protocol stack, and overcoming these problems

by defining new transportation layer SCTP.

#### SS7 over IP, problems and solutions

Dragan Soldat