

Signalizácia SS7 v IP siet'ach

Prenos signalizácií SS7 a DSS1 cez IP siete - kľúč ku konvergencii hlasových a dátových sietí.

Portál: [E-learning na FEI STU](#)

Kurz: Integrácia digitálnych sietí a služieb

Kniha: Signalizácia SS7 v IP siet'ach

Dátum: Monday, 16 April 2012, 20:26

Obsah

[Úvod](#)

[SIGTRAN protokolová architektúra](#)

[Transportný protokol SCTP](#)

[Formát SCTP paketu](#)

[Adaptačné protokoly SIGTRAN](#)

[M2PA – MTP2 User Peer-to-Peer Adaptation Layer](#)

[M2UA – MTP2 User Adaptation Layer](#)

[M3UA – MTP3 User Adaptation Layer](#)

[SUA – SCCP User Adaptation Layer](#)

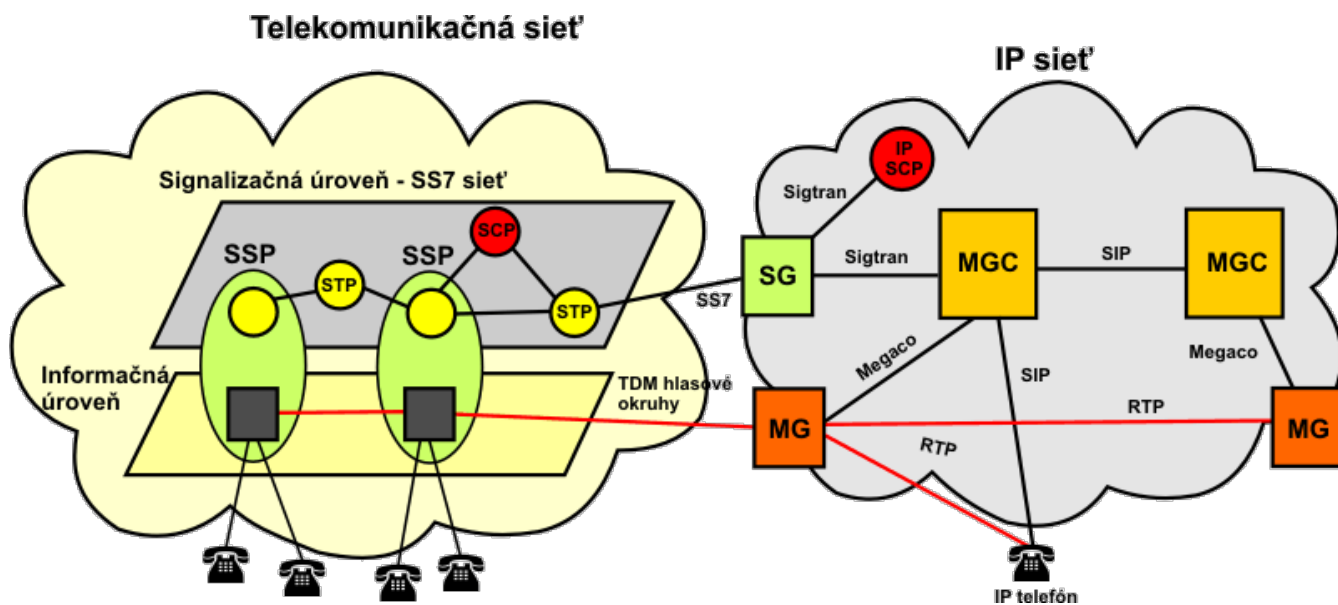
[IUA – ISDN Q.921 User Adaptation Layer](#)

Úvod

Komunikačný priemysel prechádza v súčasnosti obdobím zásadných zmien, ktoré smerujú ku konvergencii služieb a sietí. Poskytovatelia služieb hľadajú cesty ako zjednotiť hlasovú a dátovú prevádzku, služby a platformy za účelom zníženia výdavkov na prevádzku, údržbu a výstavbu sietí. Ako základ pre siete a služby novej generácie bola zvolená technológia IP, ktorá umožňuje efektívne prenášať užívateľské dáta a zároveň poskytovateľom dáva možnosti na rozširovanie sietí a zavádzanie nových služieb.

Masové rozšírenie komunikačných služieb, ako napríklad SMS, znamená aj prudký rast signalizačných sietí. Pôvodne sa uvažovalo s využitím ATM sietí na prenos signalizácie, aj tu sa však nakoniec presadila IP technológia. Štandardizačná organizácia IETF definovala novú množinu štandardov pod názvom **SIGTRAN** (Signaling Transport), ktorá poskytuje model pre prenos SS7 a ISDN signalizácií cez IP siete. **Výhody použitia IP technológie** v porovnaní s klasickou TDM sieťou zahŕňajú:

- **Jednoduché nasadenie** – pri použití signalizačných brán nie je nutné prerušovať existujúcu SS7 sieť a ďalšie rozšírenia v budúcnosti sú transparentné.
- **Nižšie náklady na zariadenia** – odpadá potreba ďalších investícií do drahých klasických signalizačných prvkov.
- **Vyššia efektívnosť** – prenos signalizácie cez IP nevyžaduje fyzické linky E1 cez SDH okruhy. Využitím technológií ako IP cez SDH či IP cez optiku je možné dosiahnuť oveľa vyššie priepustnosti.
- **Väčšie prenosové pásmo** – veľkosť SIGTRAN informácie prenášanej cez IP nie je obmedzená kapacitou linky ako v prípade SS7 siete. IP sieť je oveľa flexibilnejšia ako klasická TDM sieť.
- Implementácia IP sietí umožňuje poskytovať **nové riešenia a služby s pridanou hodnotou**.



Obr. 1. Spolupráca medzi PSTN a NGN IP sieťou

Na obr. 1 je znázornený príklad spolupráce medzi klasickou telefónnou sieťou (PSTN/ISDN) a IP sieťou poskytujúcou VoIP (*Softswitch* architektúra). Telekomunikačná sieť sa dá rozdeliť na informačnú úroveň určenú na prenos hovorov a signalizačnej úrovne SS7, ktorá prenáša signalizačné informácie. Čiernymi linkami sú v obrázku znázornené linky na prenos signalizácie, resp. riadiacich informácií.

V telekomunikačnej sieti je prenos signalizácie prostredníctvom SS7 signalizačných liniek, v IP sieti sa signalizácia a riadiace informácie prenášajú IP linkami, prostredníctvom príslušných protokolov (MEGACO, SIP, SIGTRAN). Konverziu transportu signalizácie na rozhraní sietí zabezpečujú **signalizačné brány** (*Signaling Gateways* - SG). Použitie signalizačných brán umožňuje bezproblémovo prevádzkovať existujúce a nové zariadenia cez chrbticovú IP sieť poskytujúcu veľké prenosové pásmo, škálovateľnosť a dostupnosť.

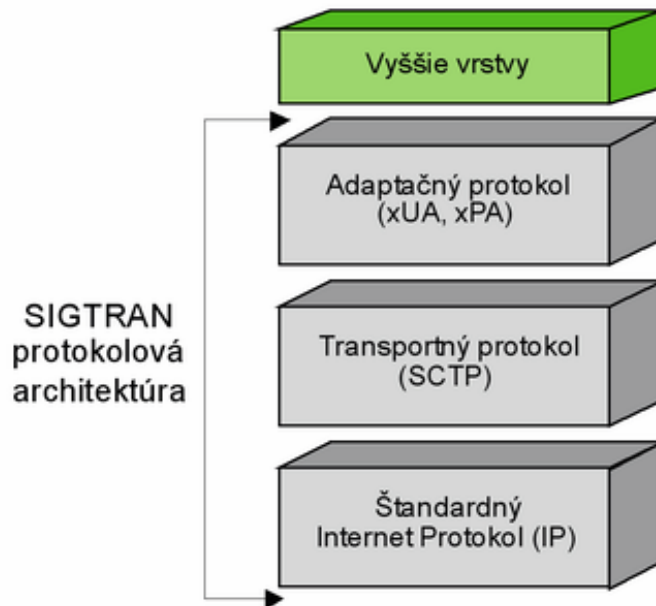
Červené linky znázorňujú prenos používateľských informácií (v tomto prípade telefónne hovory). **Sieťový prechod médií** (*Media Gateway* - MG) zabezpečuje prenos medzi sieťou s prepájaním okruhov a paketovou IP sieťou. Blok **riadenia sieťového prechodu médií** (*Media Gateway Controller* – MGC) riadi prestup medzi IP a TDM prostredím a podieľa sa na riadení hovorov. Taktiež vykonáva **preklad SIP správ na ISUP správy** a naopak.

SS7 signalačný bod vybavený IP pripojením sa nazýva **IP signalačný bod** (IPSP). Funkcionalita IPSP je rovnaká ako pri tradičnom SS7 signalačnom bode, avšak namiesto klasických SS7 liniek je na prenos signalačných správ použitá IP sieť. To umožňuje konvergenciu dátových a signalačných sietí, keďže SS7 signalačné body môžu mať prístup k databázam a aplikáciám v IP sieti.

SIGTRAN protokolová architektúra

Architektúra SIGTRAN pozostáva z nasledujúcich troch komponentov:

- Štandardný **IP protokol**.
- **Transportný protokol**, ktorý poskytuje množinu spoľahlivých prenosových funkcií pre prenos signalizácie. Týmto je nový protokol **SCTP** (*Stream Transmission Control Protocol*) definovaný organizáciou IETF.
- **Adaptačná podvrstva** poskytujúca základné funkcie požadované jednotlivými signalizačnými aplikačnými protokolmi. Definovaných bolo niekoľko protokolov adaptačnej podvrstvy – **M2PA**, **M2UA**, **M3UA**, **SUA** a **IUA**. Súčasne môže byť implementovaný len jeden protokol.



Obr. 2. SIGTRAN protokolová architektúra

Transportný protokol SCTP

Viacero obmedzení dostupného spojovo orientovaného prenosového protokolu TCP (*Transmission Control Protocol*) používaného v IP sieťach si vyžiadalo vývoj nového transportného protokolu pre prenos signalizácie SS7 cez IP siete. Medzi obmedzenia protokolu TCP patrí najmä oneskorenie spôsobované mechanizmami zabezpečujúcimi spoľahlivý prenos dát. Týmito mechanizmami sú potvrdzovanie a striktné dodržiavanie poradia doručenia paketov. Neželané oneskorenia sú nevhodné pre aplikácie v reálnom čase. Nevýhodou TCP protokolu je aj jeho slabšia bezpečnosť – je relatívne ľahko zraniteľný DoS (*Denial of Service*) útokmi.

Novým protokolom definovaným štandardizačnou organizáciou IETF je **Stream Control Transmission Protocol** (SCTP). Protokol SCTP nebol vyvinutý špeciálne len pre SIGTRAN, preto je možné využiť jeho funkcie transportnej vrstvy aj pre iné internetovské aplikácie.

Hlavné vlastnosti SCTP protokolu:

- Unicast protokol – výmena dát je realizovaná medzi dvoma známymi koncovými bodmi.
- **Spojovo orientovaný protokol - SCTP spojenie** sa nazýva **asociácia**.
- Poskytuje **spoľahlivý prenos** dát.
- Definuje časovače s oveľa kratšími intervalmi ako pri TCP protokole.
- Dokáže prispôbiť rýchlosť vysielania aktuálnemu stavu siete.
- Podporuje **fragmentáciu** signalizačných správ na viacero SCTP paketov.
- Podporuje **multi-homing** - každý SCTP koncový bod môže mať viacero IP adries a smerovanie na jednu adresu je v sieti nezávislé od smerovania na inú IP adresu. Ak je niektorá cesta nedostupná, použije sa iná. TCP protokol podporuje len *single-homed* dátové spojenia.
- Poskytuje **multi-streaming** – dáta je možné rozdeliť do viacerých tokov, pričom v každom toku je poradie doručovania správ nezávislé.
- Prenáša **štruktúrované rámce** dát (správy) – na rozdiel od TCP, ktorý prenáša tok bajtov.

Pri protokole TCP predstavuje spojenie komunikačný kanál medzi dvoma rozhraniami koncových bodov. **SCTP asociácia** predstavuje spojenie dvoch koncových bodov, pričom na oboch koncoch môže byť k jednej SCTP asociácii priradených viacero rozhraní (a teda aj IP adries). Dva uzly môžu tak byť spojené v rámci asociácie súčasne cez Ethernet aj Wi-Fi rozhranie. Asociácia je jednoznačne identifikovaná **množinou IP adries a príslušných portov** na oboch jej koncoch a náhodným 32-bitovým číslom (*Verification Tag*) dohodnutým pri vytvorení asociácie.

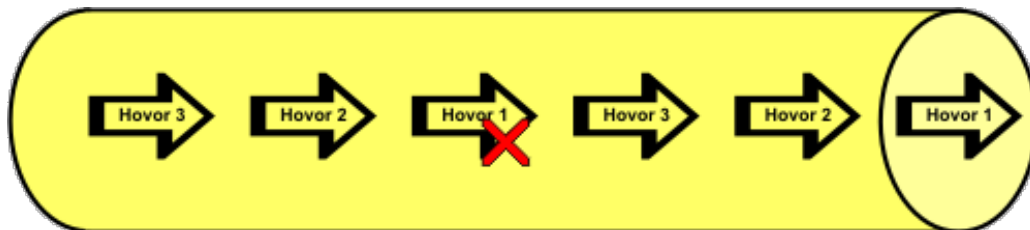
V prípade uzla s viacerými rozhraniami a IP adresami SCTP podporuje vyššie spomínaný **multi-homing**. Každá IP adresa je považovaná za cestu (*path*). Každý SCTP koncový bod si zvolí jednu cestu ako primárnu, ktorou sa pokúša vyslať správy na prvý pokus. V prípade opätovného vyslania správy sa automaticky využije alternatívna cesta, ak je dostupná. Dohľad nad cestami je vykonávaný prostredníctvom potvrdzovaných *heartbeat* správ, na základe ktorých koncový bod vie, či je linka aktívna, alebo neaktívna (podobný princíp ako FISU jednotky v MTP).

Dobre navrhnutá SS7 sieť poskytuje najmenej dve fyzicky oddelené cesty na prenos signalizačných informácií. Rovnakú úroveň redundancie v prípade IP riešení môžeme dosiahnuť práve *multi-homingom*. Každý SCTP koncový bod by mal mať najmenej dve IP adresy a rozhrania pripojené k dvom rôznym smerovačom. Smerovanie v IP sieti by malo byť navrhnuté tak, aby pakety posielané rôznymi cestami (v zmysle SCTP) neprechádzali v IP sieti spoločnými prostriedkami. *Multi-homing* poskytuje redundanciu sieťových prostriedkov, čím umožňuje predchádzať zlyhaniam siete.

Multi-streaming je ďalšia z hlavných výhod protokolu SCTP pre prenos signalizačných správ.

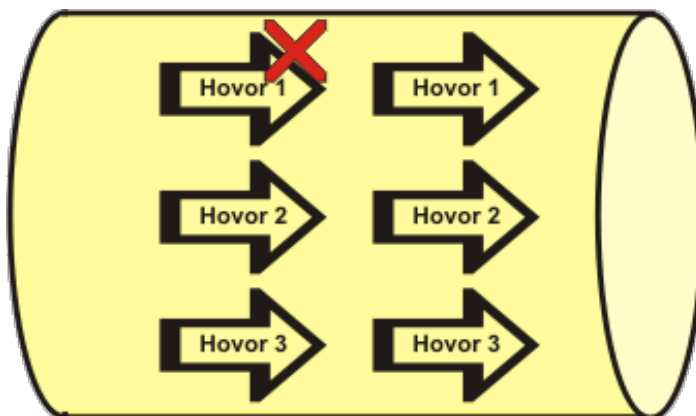
Táto vlastnosť umožňuje rozdeliť jednu SCTP asociáciu medzi dvoma koncovými bodmi do logicky oddelených tokov dát (*streams*) a priradiť každý z týchto tokov konkrétnej aplikácii. Zároveň je garantované poradie doručenia správ v rámci každého toku. Na uvedený účel sa využívajú parametre *Stream Identifier* a *Stream Sequence Number*.

Výhodou je, že chyby alebo oneskorenia v jednom toku nemajú vplyv na prenos dát v ostatných tokoch. Príkladom je protokol ISUP, ktorý nesie signalizačné správy pre rôzne telefónne hovory. Nezávislé SS7 správy (napr. s odlišnými hodnotami SLS) tak môžu byť prenášané odlišnými logickými tokmi. Počet tokov je dohadovaný počas fázy vytvárania asociácie.



Obr. 3. Prenos signalizačných správ pre 3 rôzne hovory cez jednu TCP „rúru“

V prípade TCP protokolu chyba, strata, alebo nesprávne poradie správy pre jeden hovor spôsobí oneskorenie pre ostatné hovory rádovo v sekundách, čo je neprijateľné pre PSTN sieť. TCP protokol totiž pri výskyte chyby pozastaví všetky ďalšie dáta v rámci jedného toku do doby, kým príde k náprave.



Obr. 4. Prenos správ pre 3 rôzne hovory cez tri logicky oddelené toky v jednom SCTP spojení

V prípade SCTP môžu byť signalizačné správy prenášané v rámci spojenia logicky oddelenými tokmi, takže strata dát v jednom hovore nespôsobí oneskorenie pri prenose správ pre ostatné hovory.

Tab.: Porovnanie vlastností protokolov SCTP, TCP, UDP z hľadiska ich vhodnosti pre prenos signalizácie.

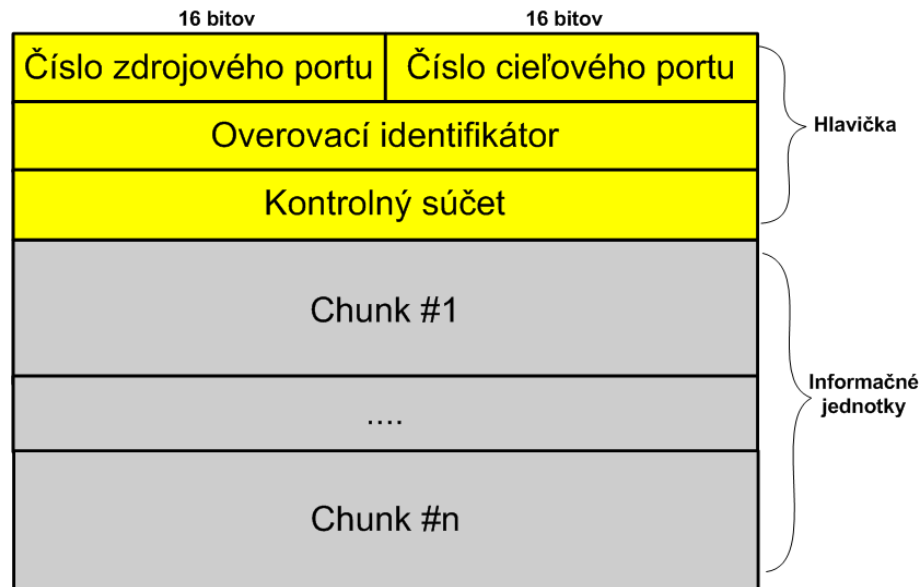
Vlastnosti	SCTP	TCP	UDP
Spojovo-orientovaný	Áno	Áno	Nie
Plný duplex	Áno	Áno	Áno
Spol'ahlivý prenos dát	Áno	Áno	Nie
Zachovanie poradia dát	Áno	Áno	Nie
Neusporiadané doručenie dát	Áno (voliteľne)	Nie	Áno
Riadenie toku	Áno	Áno	Nie
Riadenie zahĺtenia	Áno	Áno	Nie
Zachovanie hraníc správ	Áno	Nie	Áno
Fragmentácia aplikačných	Áno	Áno	Nie

PDU			
Združovanie aplikačných PDU (<i>chunk bundling</i>)	Áno	Áno	Nie
Multi-streaming	Áno	Nie	Nie
Multi-homing	Áno	Nie	Nie

V súčasnosti existujú implementácie SCTP pre väčšinu operačných systémov, niektoré ako súčasť jadra systému, iné ako rozširujúce balíky. Prehľad implementácií je k dispozícii na stránke <http://www.sctp.org/implementations.html>.

Formát SCTP paketu

SCTP paket pozostáva zo spoločnej hlavičky a jednej, alebo viacerých informačných jednotiek, tzv. *chunks*. Štruktúra paketu je znázornená na nasledujúcom obrázku.



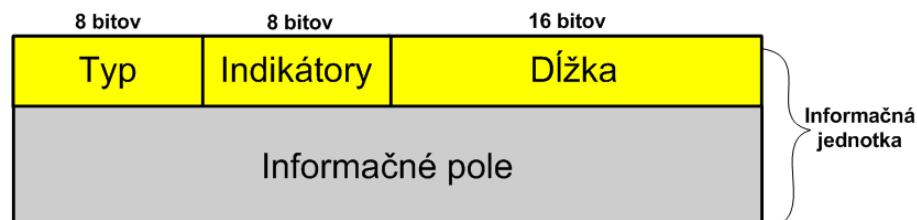
Obr. Štruktúra SCTP paketu.

Spoločná hlavička SCTP paketu obsahuje:

- **Číslo zdrojového portu** - číslo portu odosielateľa SCTP paketu.
- **Číslo cieľového portu** - číslo portu príjemcu SCTP paketu.
- **Overovací identifikátor** (*Verification Tag*) - nastavený na hodnotu dohodnutú počas vytvárania asociácie.
- **Kontrolný súčet** - algoritmus Adler-32.

Každá informačná jednotka obsahuje svoju hlavičku a samotnú prenášanú informáciu. Viacero informačných jednotiek môže byť prenášaných spolu v jednom SCTP pakete (tzv. **chunk bundling**). Existuje viacero typov informačných jednotiek (*chunks*), napr.:

- **DATA** - obsahuje používateľskú informáciu, jednotlivé jednotky sú číslované pomocou poľa TSN (*Transmission Sequence Number*). Obsahuje aj hodnoty SI (*Stream Identifier*) a SSN (*Stream Sequence Number*), ktoré určujú príslušnosť danej jednotky ku konkrétnemu toku a poradové číslo jednotky v rámci daného toku.
- **SACK** (*Selective Acknowledgement*) - potvrdzuje prijatie dátových jednotiek od druhej strany a zároveň informuje o prípadných chýbajúcich dátových jednotkách.
- **HEARTBEAT** - používa sa na testovanie dostupnosti konkrétnej transportnej adresy v rámci asociácie.
- **HEARTBEAT ACK** - posiela sa ako odpoveď na HEARTBEAT.
- INIT, INIT ACK, ABORT, SHUTDOWN, SHUTDOWN ACK, ...



Obr. Všeobecná štruktúra informačnej jednotky (*chunk*).

Úloha: Pozrite si ukážky SCTP paketov v adresári **Plocha->SS7_Wireshark/SCTP**.

Aké *chunk*-y obsahujú SCTP pakety v jednotlivých ukázkach?

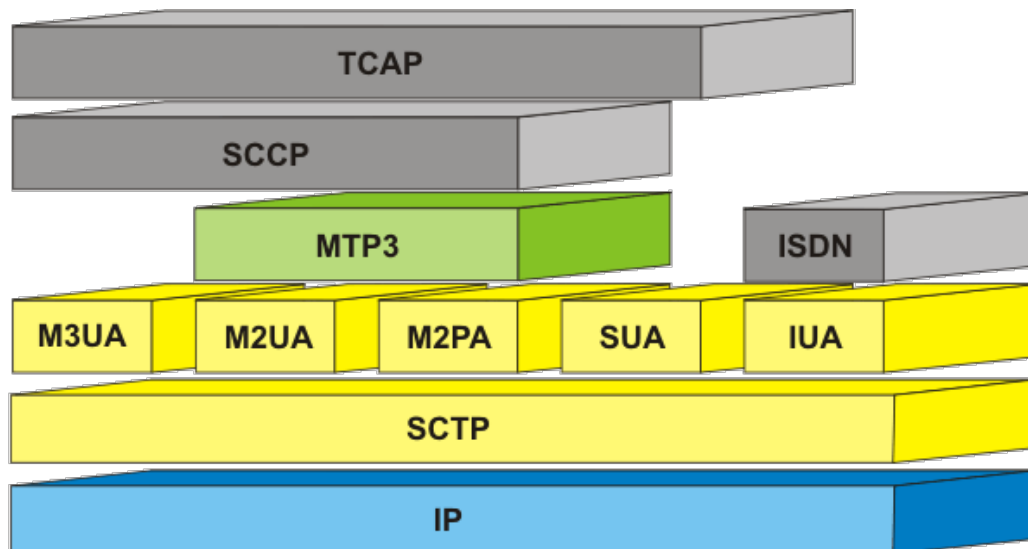
Využil sa v niektorom prípade aj *chunk bundling*?

Aké indikátory (*Flags*) obsahuje DATA *chunk*?

Pozrite si aj obsah SACK, HEARTBEAT a HEARTBAT ACK *chunk*-ov.

Adaptačné protokoly SIGTRAN

V nasledujúcich podkapitolách si priblížime hlavné vlastnosti jednotlivých protokolov adaptačnej podvrstvy, ich využitie a rozdiely medzi nimi. S výnimkou *peer-to-peer* protokolu M2PA sú všetky ostatné protokoly typu klient-server.



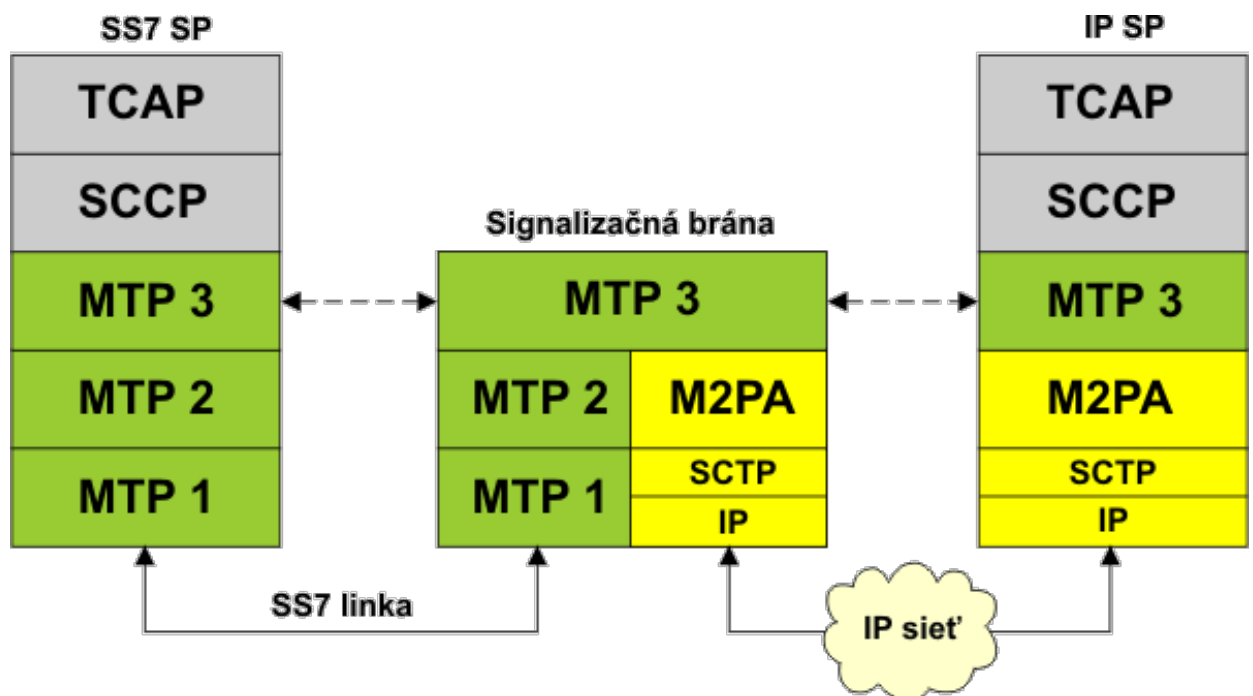
Obr. Protokoly adaptačnej podvrstvy architektúry SIGTRAN.

Protokoly M3UA a M2PA boli vybrané združením 3GPP na prenos SS7 signalizácie v 3GPP *core* sieťach ([3GPP TS 29.202](#)).

M2PA – MTP2 User Peer-to-Peer Adaptation Layer

Protokol M2PA poskytuje prenos SS7 signalizačných správ z úrovne MTP3 cez IP sieť prostredníctvom služieb protokolu SCTP. M2PA poskytuje plnú podporu spracovania MTP3 správ a funkcie manažmentu siete medzi dvoma SS7 signalizačnými bodmi cez IP sieť. M2PA vykonáva podobné funkcie ako MTP2, pričom je zodpovedná najmä za:

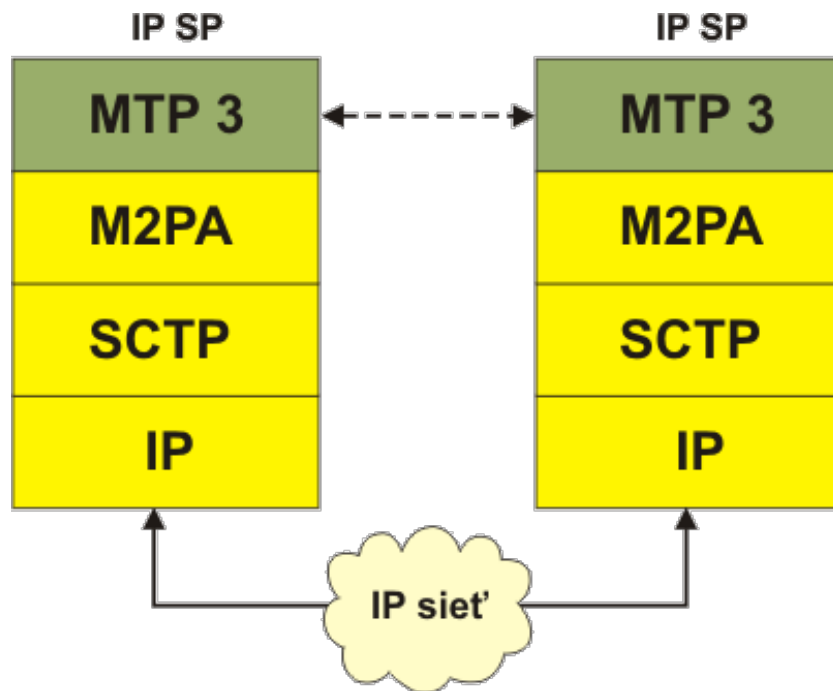
- aktiváciu a deaktiváciu liniek (SCTP asociácií) na základe požiadaviek MTP3,
- spravovanie informácií o stave liniek,
- spravovanie poradových čísiel (FSN) a pamäte pre retransmisiu.



Obr. 5. Ilustrácia použitia protokolu M2PA

Obr. 5 znázorňuje SS7 signalizačný bod pripojený k IP signalizačnému bodu cez signalizačnú bránu (SG) vybavenú tradičným SS7 aj IP pripojením. Komunikácia medzi úrovňami MTP3/M2PA je definovaná rovnakými primitívami ako komunikácia MTP3/MTP2. Signalizačná brána SG sa v tomto prípade chová ako STP.

Špecifikácia MTP vyžaduje, aby každý signalizačný bod s úrovňou MTP3 bol reprezentovaný svojím kódom signalizačného bodu (*Point Code*). Každý IP signalizačný bod s implementovanou úrovňou MTP3 musí preto okrem IP adresy priradený aj kód signalizačného bodu. Rovnako je to aj v prípade SG.



Obr. 6. Komunikácia dvoch IP SP prostredníctvom M2PA v all-IP architektúre

Na obr. 6 je príklad prepojenia dvoch signalizačných bodov prostredníctvom adaptačnej vrstvy M2PA v tzv. all-IP architektúre. V tomto prípade úrovne MTP3 signalizačných bodov využívajú M2PA ako rovnocennú náhradu za MTP2. M2PA teda umožňuje nahradiť sieť SS7 línií kapacitnejšou IP sieťou.

Použitie M2PA na prenos SS7 signalizácie v *3GPP Core sieťach* je definované v špecifikácii TS 29.202. Protokol M2PA je možné využiť na komunikáciu medzi dvoma signalizačnými bránami navzájom (rozhranie B).

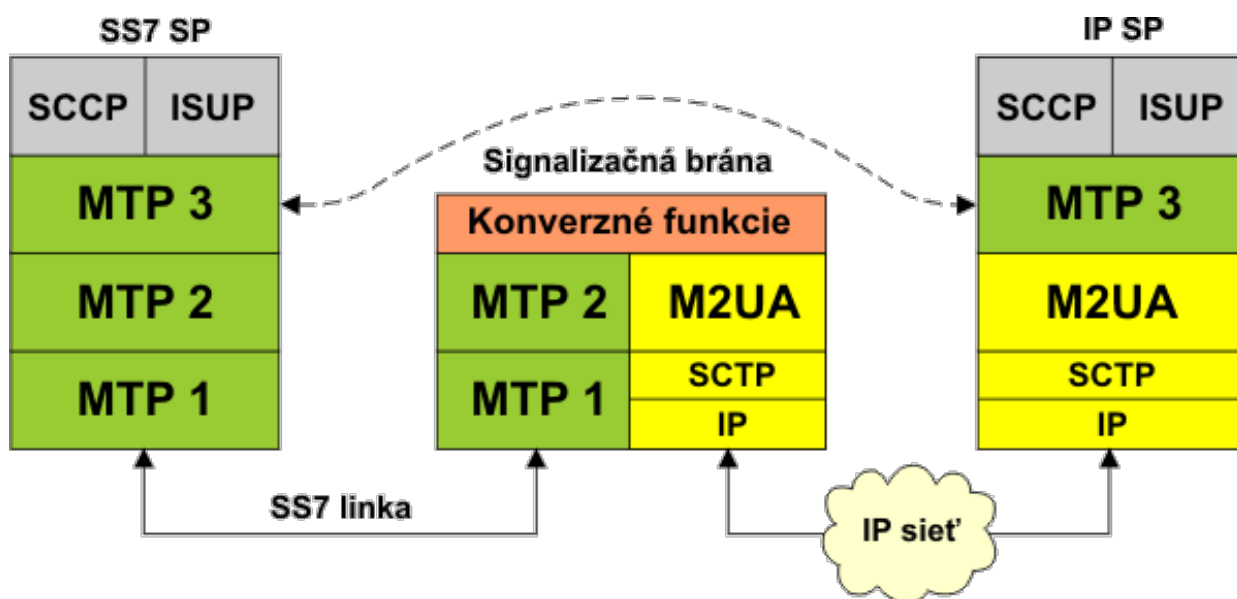
M2UA – MTP2 User Adaptation Layer

Protokol M2UA je určený pre prenos SS7 signalizačných správ MTP2 používateľa (ktorým je MTP3) cez IP sieť prostredníctvom protokolu SCTP. M2UA poskytuje:

- rozhranie MTP2/MTP3
- podporu manažmentu aktívnych asociácií (SCTP spojení).

Príklad využitia M2UA je na obrázku 7. Tento protokol môže byť použitý na komunikáciu medzi SG a blokom riadenia sieťového prechodu médií (*Media Gateway Controller* - MGC). SG prijíma SS7 signalizáciu cez štandardné SS7 rozhranie prostredníctvom MTP, pričom poskytuje funkcie na prenos signalizačných správ do úrovne MTP3, ktorá sa nachádza v IPSP. MTP3 v IP signalizačnom bode tak využíva MTP2 v SG ako svoju nižšiu SS7 vrstvu. MTP3/MTP2 komunikácia je definovaná prostredníctvom M2UA správ prenášaných cez IP sieť. V tomto prípade signalizačná brána predstavuje ukončenie signalizačnej SS7 linky.

M2UA umožňuje pripojiť jeden IPSP ku klasickej TDM signalizačnej sieti prostredníctvom SG. Využitie brán s M2UA je možné len v prípade lokálneho nahradenia TDM linky IP linkou, nakoľko na druhej strane signalizačnej brány musí byť naďalej TDM linka. SG poskytuje len spoluprácu medzi jednou TDM linkou a jednou IP linkou, čo znamená v prípade nahradenia celej množiny SS7 liniek (*link set*) rovnakým počtom SG ako je počet SS7 liniek.



Obr. 7. Ilustrácia použitia protokolu M2UA

Tab. 1. Porovnanie M2PA a M2UA

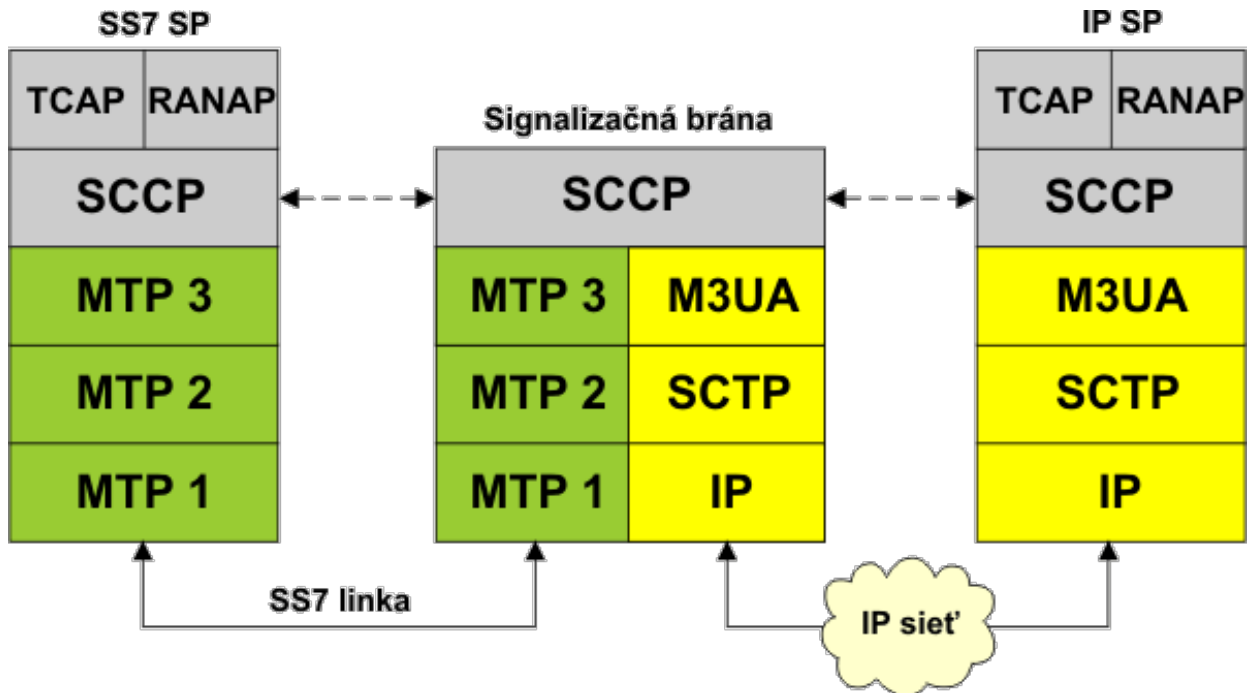
	M2PA	M2UA
MTP3 správy	Prenáša MTP3 správy	Prenáša MTP3 správy
Rozhranie k MTP3	Poskytuje rozhranie MTP2/MTP3	Poskytuje rozhranie MTP2/MTP3
Služby (primitívy) MTP3-to-MTP2	IPSP spracováva primitívy MTP3-to-MTP2	IPSP prenáša primitívy MTP3-to-MTP2 na spracovanie do MTP2 v SG

Typy liniek	Spojenie medzi SG a IPSP je z pohľadu MTP3 SS7 linka	Spojenie medzi SG a IPSP nie je SS7 linka. Ide o vysunutie MTP2 do vzdialeného uzla
Kód signalizačného bodu (Point Code)	SG je SS7 uzol s kódom bodu	SG nie je SS7 uzol keďže nemá priradený kód bodu
Používateľské časti SS7	SG môže mať vyššie vrstvy (napr. SCCP)	SG nemá vyššie vrstvy SS7, pretože nemá MTP3
Manažment	Spolieha sa na MTP3 funkcie manažmentu	Používa M2UA funkcie manažmentu

M3UA – MTP3 User Adaptation Layer

Protokol M3UA umožňuje prenos signalizácie MTP3 používateľa (napr. ISUP, SCCP, BICC) cez IP sieť prostredníctvom SCTP protokolu.

M3UA poskytuje ekvivalentnú množinu služieb MTP3 používateľom na svojej hornej vrstve ako poskytuje MTP3 svojim používateľom v klasickom SS7 koncovom bode. Vrstvy ISUP a SCCP tak nevedia, že očakávané MTP3 služby sú poskytované vzdialene z MTP3 v SG a nie lokálnou MTP3. Rovnako, vrstva MTP3 v SG nevie, že jej lokálni používatelia sú v skutočnosti vzdialení v IPSP.

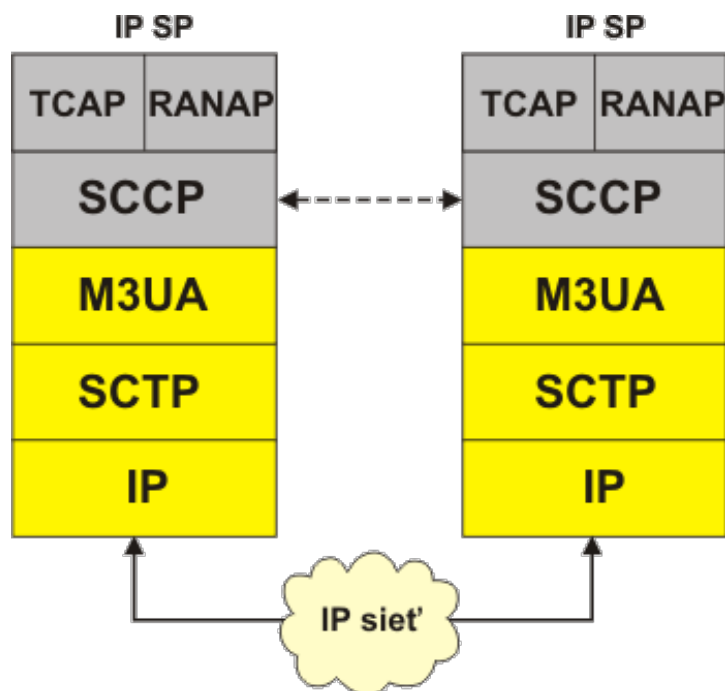


Obr. 8. Ilustrácia použitia protokolu M3UA

Na obr. 8 je príklad prepojenia IPSP (napr. MGC, IP SCP, IP HLR) k signalizačnej bráne. SG môže obsahovať aj vrstvu SCCP protokolu vykonávajúcu preklad globálnych názvov (GTT - ekvivalent IP smerovania) pre správy, ktoré sú určené pre SCCP v signalizačnej bráne (DPC = SG, SIO = SCCP).

Predkladom globálneho názvu získame kód signalizačného bodu, pre ktorý je správa určená. Ak sa tento signalizačný bod nachádza v IP doméne, správa je ďalej odoslaná cez lokálnu vrstvu M3UA na ďalšie smerovanie k cieľovému uzlu cez IP sieť (M3UA musí mať tabuľku umožňujúcu preklad DPC na IP adresu). Podobne to funguje aj v opačnom smere. Oproti M2PA nepotrebujeme pri M3UA udržiavať tabuľku Link set <-> IP adresa.

Použitie protokolov ako M3UA (MTP3 User Adaptation Layer) alebo SUA (SCCP User Adaptation Layer) umožňuje výrobcam aplikácií (SMS centrum - SMSC, IP-Home Location Register IP-HLR, ...) zamerať sa len na vývoj aplikačnej vrstvy bez nutnosti riešenia zložitých SS7 rozhraní.



Obr. 9. Komunikácia dvoch IP SP cez M3UA v all-IP architektúre

Obr. 9 predstavuje príklad, kedy sú SCCP správy vymieňané priamo medzi dvoma IPSP cez IP sieť.

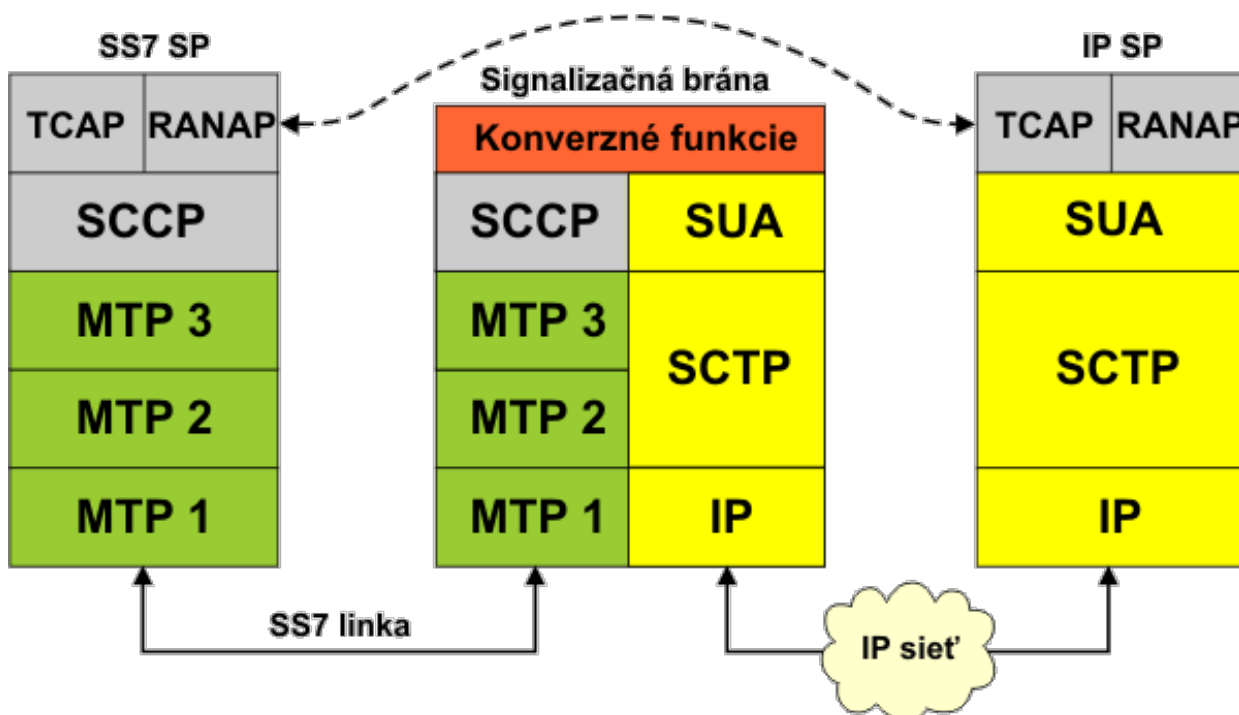
Protokol M3UA je najčastejšie používaný SIGTRAN protokol. Organizácia 3GPP štandardizovala použitie M3UA na prenos SS7 signalizácie v *3GPP Core sieťach* medzi dvoma IP signalizačnými bodmi (rozhranie A), alebo medzi IP signalizačným bodom a signalizačnou bránou (rozhranie C) v špecifikácii [TS 29.202](#).

Použitie protokolov ako M3UA (MTP3 User Adaptation Layer) alebo SUA (SCCP User Adaptation Layer) umožňuje výrobcovi aplikácií (SMS centrum - SMSC, IP-Home Location Register IP-HLR, ...) zamerať sa len na vývoj aplikačnej vrstvy bez nutnosti riešenia zložitých SS7 rozhraní.

SUA – SCCP User Adaptation Layer

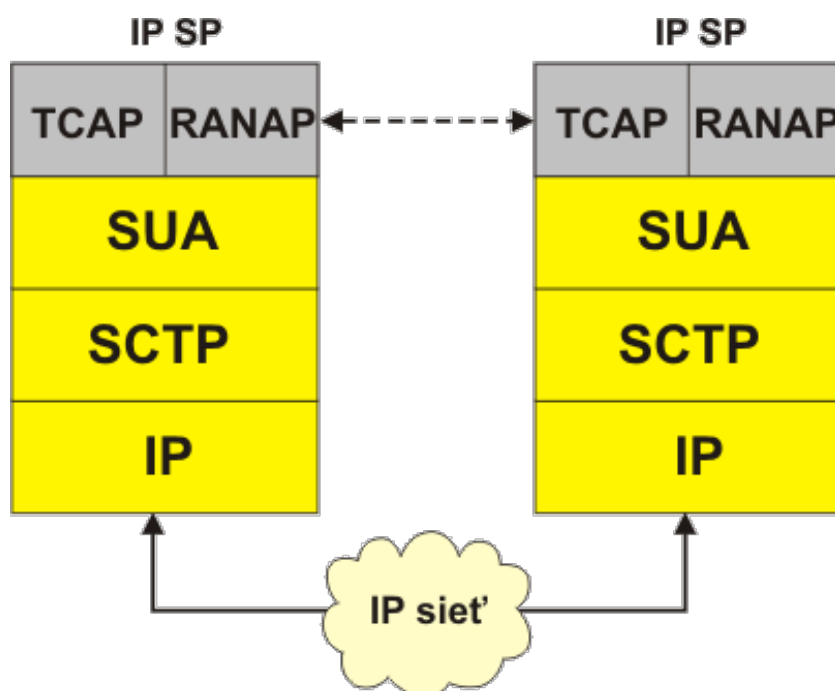
Protokol SUA umožňuje prenos správ SCCP používateľa (MAP cez TCAP, BSSAP, RANAP, a pod.) a správ nových 3G protokolov cez IP medzi dvoma koncovými signalizačnými bodmi. Môže ísť o prenos medzi signalizačnou bránou a IP koncovým signalizačným bodom (napr. databázou v IP sieti), alebo aj prenos správ medzi dvoma IP koncovými bodmi len v rámci IP siete. Protokol SUA umožňuje:

- prenos správ SCCP používateľa (TCAP, BSSAP, RANAP, ...),
- spojovo aj nespojovo orientovaný prenos,
- manažment SCTP asociácií medzi SG a jedným alebo viacerými IP SP.



Obr. 10. Ilustrácia použitia protokolu SUA

Obr. 10 znázorňuje príklad nespojovo orientovaného prenosu. Signalizačná brána obsahuje vrstvy SCCP aj SUA, ktoré navzájom spolupracujú prostredníctvom konverzných funkcií.



Obr. 11. Komunikácia dvoch IP SP cez SUA v all-IP architektúre

Na obr. 11 je znázornená all-IP architektúra vhodná na prenos protokolov využívajúcich prenosové služby SCCP, ale plne v rámci IP prostredia. Táto architektúra poskytuje značnú flexibilitu v tvorbe sietí, najmä ak nie je vyžadovaná spolupráca s tradičnou signalizačnou sieťou.

SUA protokol má modulárnu štruktúru, ktorá umožňuje rôzne implementácie v závislosti od prostredia, ktoré má podporovať. V závislosti od podporovaného protokolu vyššej vrstvy môže podporovať SCCP služby so spojovou orientáciou, bez spojovej orientácie, prípadne obe.

Smerovanie pre nespojovo orientovanú službu môže byť na základe:

- **IP adresy a čísla podsystému (SSN)** - na ich základe je správa smerovaná na príslušnú *SCTP asociáciu* smerom k cieľovej IP adrese.
- **Kódu signalizačného bodu (DPC) a čísla podsystému (SSN)** - podobne ako predchádzajúci prípad.
- **Globálneho názvu (GT) a čísla podsystému (SSN)** - *SCTP asociácia* k cieľovej IP adrese sa vyberie na základe prekladu globálneho názvu (GTT).

Tab. 2. Porovnanie M3UA a SUA

	M3UA	SUA
Verzie SCCP (ANSI, ITU-T)	Signalizačný bod musí podporovať rôzne verzie SCCP v prípade, že bude spolupracovať s rôznymi národnými systémami	Použitím SUA tento problém odpadá, nakoľko vrstva SCCP je eliminovaná
Implementácia	M3UA vyžaduje služby SCCP - potreba manažmentu dvoch vrstiev (M3UA, SCCP)	Elimináciou SCCP vrstvy znížime zložitosť sieťového uzla (z hľadiska implementácie aj manažmentu), čím šetríme náklady
Otázky smerovania	Správa je smerovaná na základe kódov signalizačných bodov	SUA umožňuje smerovať správy v IP sieti aj na základe Globálneho názvu (GT), IP adresy či hostname
Otázky adresovania	Každý IP bod musí mať priradenú IP adresu aj kód bodu (PC)	IP uzol nemusí mať priradený kód bodu (PC)
ISUP služby	Sú podporované	Nie sú podporované

Vo všeobecnosti je protokolový model založený na SUA menej zložitý a viac efektívnejší v porovnaní s modelom SCCP + M3UA. Protokol SUA poskytuje lepšiu škálovateľnosť a flexibilitu v implementácii signalizačnej siete v all-IP prostredí. Výkonné adresovacie a smerovacie vlastnosti protokolu SUA umožňujú značne redukovať oneskorenie pri prenose signalizácie. V prípade plne IP prostredia nie je potrebné používanie kódov signalizačných bodov, nakoľko smerovanie v IP sieti je možné na základe IP adres. Nevýhodou však je nepodporovanie ISUP či BICC protokolov.

Použitie protokolov ako M3UA (MTP3 User Adaptation Layer) alebo SUA (SCCP User Adaptation Layer) umožňuje výrobcovi aplikácií (SMS centrum - SMSC, IP-Home Location Register IP-HLR, ...) zamerať sa len na vývoj aplikačnej vrstvy bez nutnosti riešenia zložitých SS7 rozhraní. Menšia zložitosť sietí a jednoduchá integrácia umožňuje redukovať čas potrebný na uvedenie nových aplikácií a služieb. SS7 cez IP tiež rieši problém s limitovanou priepustnosťou klasickej SS7 siete. Zariadenia ako SMSC, HLR a iné s veľkými požiadavkami na SS7 prevádzku, tak nie sú limitované priepustnosťou klasickej SS7 signalizačných liniek.

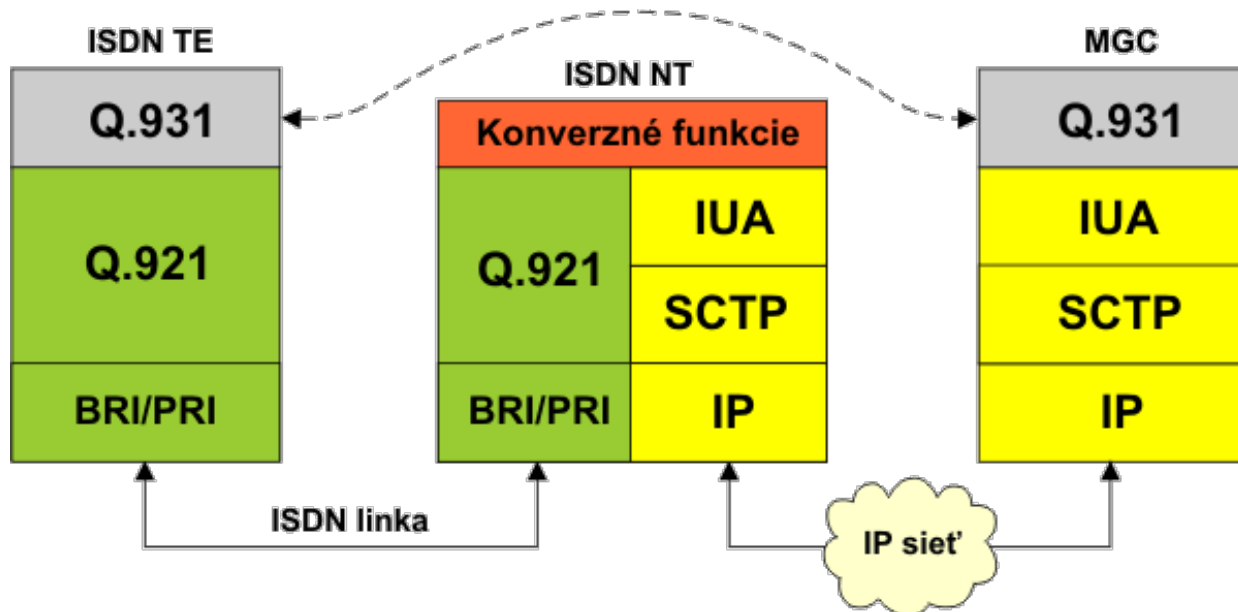
Na záver treba ešte spomenúť, že aj organizácia ITU-T poskytuje štandardy pre prenos správ

SCCP používateľov cez IP siete a to prostredníctvom **Transport Independent SCCP (TI-SCCP)**, odporúčanie [Q.2220](#)).

Použitie protokolov ako M3UA (MTP3 User Adaptation Layer) alebo SUA (SCCP User Adaptation Layer) umožňuje výrobcom aplikácií (SMS centrum - SMSC, IP-Home Location Register IP-HLR, ...) zamerať sa len na vývoj aplikačnej vrstvy bez nutnosti riešenia zložitých SS7 rozhraní.

IUA – ISDN Q.921 User Adaptation Layer

SIGTRAN poskytuje aj adaptačný protokol pre ISDN signalizácie. Protokol IUA bol navrhnutý na prenos ISDN signalizácie Q.921 používateľa (napr. Q.931, Q-SIG) cez IP sieť. Príklad použitia je na obrázku č. 12. V tomto prípade signalizačná brána predstavuje štandardné sieťové ISDN zakončenie (NT). V SG prebieha konverzia transportných funkcií LAPD protokolu za účelom prenosu Q.931 signalizačných správ cez IP sieť prostredníctvom SCTP protokolu do vrstvy Q.931 v MGC (*Softswitch*).



Obr. 12. Príklad využitia protokolu IUA

IUA podporuje základný aj primárny prístup ISDN, rovnako aj komunikáciu bod-bod a bod-multibod. Využitie protokolu SCTP pri použití IUA nie je povinné, je možné využiť aj protokol RTP. Použitie protokolu SCTP má však v tomto prípade niekoľko výhod:

- prenáša štruktúrované rámce (správy),
- každý D kanál môže byť prenášaný nezávislým tokom v rámci SCTP asociácie (*multi-streaming*, obr. 4),
- efektívna sieťová redundancia prostredníctvom *multi-homingu*,
- zachovanie poradia správ v rámci tokov.

The Bearer-Independent Call Control (BICC) is a signaling protocol based on N-ISUP that is used for supporting narrowband Integrated Services Digital Network

The Signalling Connection Control Part (SCCP) is a network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, ...

The M3UA layer enables MTP 3-like functionality to be performed over IP. .

The Transaction Capabilities Application Part (TCAP) is the primary SCCP User in ... the transport layer for air interface protocols such as BSSAP and RANAP.

RANAP (Radio Access Network Application Part)

BSSAP. ... Base Station System Application Protocol (BSSAP).

The ISDN (Integrated Services Digital Network) User Part or ISUP is part of the Signaling System No. 7 (SS7) which is used to set up telephone calls in the public .

The Bearer-Independent Call Control (BICC) is a signaling protocol based on N-ISUP that is used for supporting narrowband Integrated Services Digital Network