VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

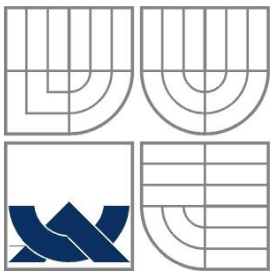
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

EMULÁTOR MOBILNÍ TELEFONNÍ ÚSTŘEDNY

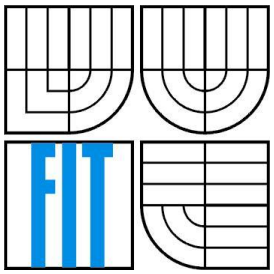
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE Bc. Jan Králíček
AUTHOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

EMULÁTOR MOBILNÍ TELEFONNÍ ÚSTŘEDNY

MOBILE SWITCHING CENTRE EMULATOR

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Jan Králíček
AUTHOR

VEDOUCÍ PRÁCE — Ing. František Ščuglík Ph.D.
SUPERVISOR

BRNO 2012

Abstrakt

Tato práce se snaží poskytnout základní přehled v tématice GSM systému. Dále se snaží navrhnout Emulátor mobilní telefonní ústředny, který by dokázal provést operaci Location Update. První část práce popisuje principy a specifika GSM sítě (strukturu sítě, operace nutné pro podporu mobility uživatelů, entity sítě atd.). Druhá část popisuje signalizační protokoly rodiny SS7, SIGTRAN a MAP protokol. Závěrečná část se věnuje návrhu Emulátoru.

Abstract

This thesis attempts to provide basic overview of the topic of the GSM system and tries to design Mobile Switching Centre Emulator that could perform the operation Location Update. The first part of this thesis describes the principles and specifics of the GSM network (network structure, the operations required to support user mobility, network entities, etc.). The second part of this thesis describes the SS7 signaling protocols, SIGTRAN and MAP protocol. The final part deals with design of the emulator.

Klíčová slova

GSM, SS7, SIGTRAN, TCAP, ISUP, TUP, TCAP, MAP, MTP, SCTP, MSC, Emulátor mobilní telefonní stanice, signalizace

Keywords

GSM, SS7, SIGTRAN, TCAP, ISUP, TUP, TCAP, MAP, MTP, SCTP, MSC, Mobile switching centre emulator, signaling

Citace

Králíček Jan: Emulátor mobilní telefonní ústředny, diplomová práce, Brno, FIT VUT v Brně, 2012

Emulátor mobilní telefonní ústředny

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením Ing. Františka Ščuglíka Ph.D.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Jan Králíček
23. května 2012

Poděkování

Chtěl bych poděkovat svému vedoucímu práce za pomoc a rady při tvorbě této práce.

Obsah

1 Úvod

Komunikace prostřednictvím mobilních telefonů je již neoddělitelnou součástí našeho života. Původně sloužila pouze pro přenos hlasu – poskytovala pouze podporu pro telefonní hovory. S postupem času, jak vzrůstala obliba internetu, stále více zákazníků projevovalo zájem o poskytnutí možnosti, připojit se k internetu mobilně – tedy za pomoci jejich mobilního telefonu. A tento trend pokračuje, GSM se stalo celosvětově nejúspěšnější mobilní sítí a nic nenaznačuje tomu, že by se to mělo v nejbližších několika letech změnit.

Tato práce pojednává o GSM síti a možnostech signalizace, které používá. Nabízí hrubý pohled na prvky GSM sítě, jejich organizaci a použití. Také představuje nejdůležitější ze signalizačních protokolů, poskytuje pohled na jejich funkci, pozici v hierarchii signalizačních protokolů atd.

Druhá část se zabývá návrhem *Emulátoru Mobilní telefonní stanice* a GSM operacemi, které jsou nutné pro vykonání operace *Location Update*. Ta slouží k aktualizaci lokačních dat v GSM databázích (VLR a HLR). Také je zde popsán navržený protokol pro komunikaci mezi *Emulátorem Mobilní telefonní stanice* a *Emulátorem mobilní stanice*.

První kapitola ***Úvod*** nastiňuje cíle diplomové práce a popisuje obsah jednotlivých kapitol.

Druhá kapitola ***Historický vývoj*** popisuje historický vývoj GSM systému. Ten lze rozdělit do několika generací, které se vyznačují použitou technologií a podporou služeb uživatelům.

Třetí kapitola ***Struktura GSM systému*** popisuje strukturu GSM systému, jeho jednotlivé části a funkčnost entit, které se v nich nacházejí. Jedná se o Base Station Subsystem (BSS), Network Switching Subsystem (NSS) a Operation Subsystem (OSS).

Tato kapitola také poskytuje popis důležitých entit, se kterými se v této práci budeme dále často setkávat, zejména tak Mobile Switching Centre (MSC), Visitor Location Registry (VLR) a Mobile Station (MS).

Čtvrtá kapitola ***Číslování v GSM*** shrnuje přehled důležitých identifikátorů, které lze v GSM systému nalézt. Popisuje jejich význam, použití a také jejich elementy, ze kterých se skládá jejich struktura. Popsány jsou identifikátory International Mobile Subscriber Identity (IMSI), Temporary Mobile Subscriber Identity (TMSI), Mobile Station International ISDN Number (MSISDN), Location Area Identity (LAI), International Mobile Equipment Identity (IMEI), Local Mobile Subscriber Identity (LMSI) a Cell Identifier (CI).

Pátá kapitola ***Vlastnosti GSM*** *sítě* popisuje důležité specifika GSM sítě. První část je věnována popisu kmitočtového plánování a hierarchie oblastí sítě, které ji formují. Následuje obecný popis významných činností sítě, jako je handover, šifrování komunikace a autentizace mobilní stanice.

Šestá kapitola ***Typy GSM kanálů a jejich použití*** se zabývá logickými kanály, které jsou v GSM systémech formovány v přístupové síti. Popisuje jejich význam a způsob použití.

Sedmá kapitola ***Signalizace*** se zabývá obecným popisem signalizace a jejím rozdělením podle způsobu přenosu signalizačních dat vůči vlastním datům.

Osmá kapitola ***Signalizace v přístupové sítí*** popisuje signalizační protokoly a rozhraní, která se vyskytují v přístupové síti GSM systému. Zaměřuje se zejména na popis *Um* protokolu, který slouží ke komunikaci mezi mobilní stanicí a BTS stanicí.

Devátá kapitola ***Protokoly v tradiční SS7*** popisuje signalizační protokoly, které jsou definovány v tradičním SS7 stacku. Jedná se o protokoly definované pro drátové sítě, tedy bez protokolů souvisejících s mobilitou uživatelů.

V úvodní části jsou popsány základní principy adresování v těchto protokolech a je ukázána hierarchická struktura, kterou jsou tyto protokoly provázány.

Následuje popis protokolů Message Transfer Part (MTP), Telephone User Part (TUP), Transaction Capabilities Application Part (TCAP), ISDN User Part (ISUP) a BSS Application Part (BSSAP).

Desátá kapitola ***Mobile Application Part (MAP)*** se zabývá popisem tohoto protokolu jakožto nejdůležitějšího nositele mobility v GSM signalizaci. Tento protokol byl definován později a rozšiřuje SS7 signalizaci o podporu celulárních sítí, přidává funkcionalitu související s mobilitou uživatelů sítě a také přináší podporu pro tzv. inteligentní sítě)

První část je věnována popisu obecné struktury MAP rámce, dále následuje popis MAP služeb s jejich rozdělením do kategorií. Konec kapitoly je věnován popisu některým důležitým MAP službám, které souvisejí s operací *Location Update*.

Jedenáctá kapitola ***SIGTRAN*** popisuje rodinu protokolů, které umožňují přenos SS7 signalizace skrze IP síť. Popsán je zde protokol Stream Control Transmission Protocol (SCTP), MTP3 User Adaptation (M3UA) a SCCP User Adaptation (SUA).

Dvanáctá kapitola ***Důležité procedury v GSM*** popisuje vybrané procedury GSM systému, které souvisejí s provedením operace *Location Update*. V první části jsou popsány obecné činnosti, které jsou společné pro všechny operace, jejichž iniciátorem je MS. Jedná se o Channel Request operaci (požadavek na přidělení komunikačního kanálů), Autentizace MS a Šifrování komunikace.

Druhá část se věnuje procedurám souvisejícím s provedením operace *Location Update*. Jedná se o operace IMSI attach, Explicitní IMSI detach, Implicitní IMSI detach a Location Update operaci.

Třináctá kapitola ***Emulátor*** se věnuje popisu *Emulátoru Mobilní telefonní ústředny* (dále jen *Emulátor*). První část popisuje zprávy, které souvisejí s činnosti *Emulátoru*. Následuje popis navrženého komunikačního protokolu, který slouží pro spojení *Emulátoru mobilní stanice* a *Emulátoru.* Jsou zde popsány definované typy zpráv, princip jejich tvorby a definované parametry.

Další část je věnována popisu konfiguračního souboru, který slouží k předání parametrů *Emulátoru*.

Následuje popis vlastní činnosti *Emulátoru*. Tu lze rozdělit na dvě části – komunikaci v přístupové síti (kde je použit navržený komunikační protokol) a komunikaci v páteřní síti (kde se využívá protokol MAP).

Na závěr jsou uvedeny definované chybové stavy, ke kterým může v průběhu činnosti *Emulátoru dojít*.

2 Historický vývoj

První generace (1G) mobilních služeb se v 80. letech, kdy vznikl mobilní (celulární) telefon, realizovala analogově a soustředila se na přenos hlasu. Do první generace patřily následující analogové služby a systémy:

- **NMT** (Nordic Mobile Telephone) – první komerční analogový mobilní systém zahájil práci v Norsku a Švédsku v roce 1979
- **AMPS** (Analog Mobile Phone System) – systém používaný od roku 1982 v USA
- **TACS** (Total Access Communications System) – původně specifikován pro Velkou Británii, později našel uplatnění v Asii a oblasti Pacifiku

Druhá generace (2G), působící od poloviny 90. let, již využívá digitální způsob přenosu, ale opět se soustřeďuje na hlasové služby. Proto propustnost sítě nepřesahuje 20 kbit/s. Mezi technologie 2G patří:

- **GSM** (Global System for Mobile Communications) – nejúspěšnější mobilní technologie vůbec
- **CDPD** (Cellular Digital Packet Data)
- **TDMA** (Time Division Multiple Access)
- **CDMA** (Code Division Multiple Access)

Kolem roku 2001 se objevuje **přechodová generace** (tzv. 2.5G). Ta reaguje na zvyšující se poptávku po mobilních datových přenosech, které úzce souvisí s internetovým boomem. Pro přenos dat ale není stávající přístup (přepínání okruhů) příliš vhodný, proto systém této generace používají přepínání paketů. Mezi technologie této generace patří:

- **GPRS** (General Packet Radio Service) je paketová služba a jako nadstavba GSM umožňuje uživateli používat najednou až 8 GSM kanálů, s výslednou kapacitou do 115 kbit/s.
- **EDGE** (Enhanced Data for GSM Evolution) je další stupeň modernizace sítí GSM/GPRS, který se již podobá třetí generaci.

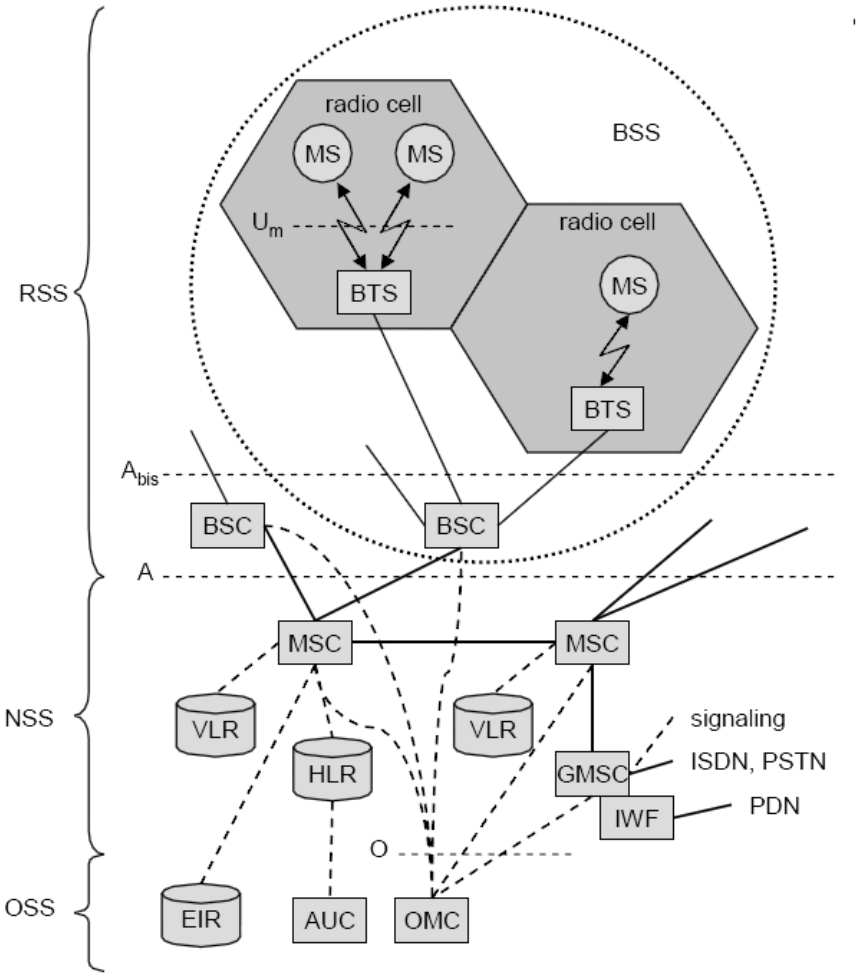
Třetí generace (3G) se již soustředí na poskytnutí širokopásmového datového připojení. Nejedná se o jedinou technologii, ale celou plejádu různorodých radiových technologií:

- **UMTS** (Universal Mobile Telecommunication System) – založeno na CDMA principu
- **HSDPA** (High-Speed Dedicated Shared Channel)
- **HSUPA** (High-Speed Uplink Packet Access)

Čtvrtá generace (4G) nepřináší žádný nový systém, naopak, kombinuje dohromady techniky 2.G a 3G spolu s WiFi, Bluetooth atd. Například ve škole je možné připojit se za pomoci WiFi, při cestování domů za pomoci UMTS, doma za pomoci ADSL a u babičky na vesnici za pomoci GPRS.

Informace pro tuto kapitolu byly čerpány z [1], [2].

3 Struktura GSM systému



Obrázek 3.1 - Struktura GSM systému, převzato z [3]

3.1 Base Station Subsystem (BSS)

Přístupovou část sítě tvoří RSS subsystém, který se skládá z mnoha BSS sekcí. Tyto sekce zajišťují zeměpisné členění sítě – reprezentují oblast, která je pod správou právě jednoho BSC kontroléru (tedy obsahuje právě jedno BSC, k němu přidružených několik BTS a MS, která se aktuálně nacházejí v této oblasti). Zajišťuje všechny potřebné funkce pro bezdrátovou komunikaci s MS, kódování a dekódování hlasu atd.

Funkčnost BSS je distribuována mezi BSC kontrolér a příslušné BTS stanice. BTS zajišťuje všechny funkce specifické pro rádiovou komunikaci. Oproti tomu BSC obsluhuje rádiové kanály BTS stanic a představuje centrum přepínání rádiových kanálů. Tabulka 3.1 shrnuje funkčnost BSS subsystému, kterou poskytují BTS stanice a BSC kontrolér.

Funkce	BTS	BSC
Správa rádiových kanálů		X
Frequency hopping	X	X
Správa pozemních kanálů		X
Mapování pozemních kanálů na rádiové		X
Kódování a dekódování kanálu	X	
Změna rychlosti přenosu	X	
Šifrování a dešifrování	X	X
Výzva (paging)	X	X
Měření kvality signálu	X	
Měření intensity hustoty provozu		X
Autentizace		X
Komunikace s registry lokality (HLR a VLR)		X
Handover management		X

Tabulka 3.1 - Distribuce funkčnosti BSS mezi BTS a BSC

3.1.1 Mobile Station (MS)

Pod pojem MS zahrnujeme veškeré uživatelské vybavení a software, který je potřebný pro komunikaci s GSM sítí. Mobilní stanice se skládá z několika oddělených funkčních jednotek, kde každá jednotka odpovídá za jednu oblast činnosti (Obrázek 3.2, část A ukazuje vztahy mezi těmito jednotkami). Tento koncept umožňuje oddělit problematiku přístupu do sítě, který je specifikován GSM systémem (rádiový přenos, synchronizace atd.), možných odlišností v implementacích jednotlivých poskytovatelů GSM připojení (použití odlišných algoritmů od A3 a A8, dodatečná funkcionalita poskytovaná sítí – např. internetové bankovnictví) a funkcionality mobilní stanice (různé implementace obsluhy telefonních hovorů, adresáře, hry atd.). Díky tomu existuje na trhu celá plejáda nejrůznějších řešení mobilních stanic, které se liší poskytovaným uživatelským komfortem i svým zaměřením (od smartphonů přes mobilní telefony se základní funkcionalitou až po specifická zařízení, jako jsou například GSM zásuvky).

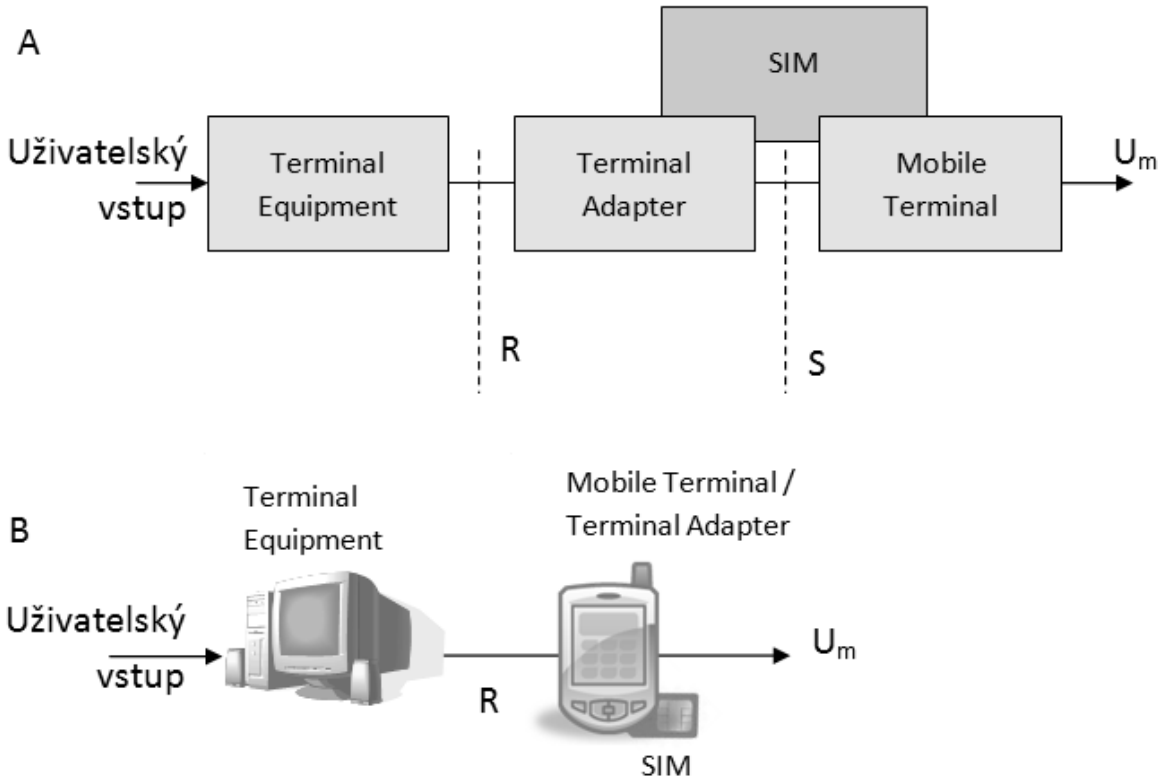
TE (Terminal Equipment) je periferní zařízení, které nabízí uživatelské služby (neobsahuje funkce specifické pro GSM). Dochází k oddělení GSM funkcionality, kterou musí implementovat každé zařízení, které chce přistupovat do GSM sítě, od uživatelského prostředí. Obrázek 3.2, část B schematický ukazuje, že TE může realizovat jakoukoliv uživatelskou funkcionalitu (standardně realizuje uživatelské ovládání SMS, hovorů…), zatímco TA+MT představuje pouze přístupové prostředí do GSM sítě.

MT (Mobile Terminal) je ekvivalentem ukončení ISDN adresy v digitálních pevných sítích. MT poskytuje všechny funkce, které musí každé MS povinně implementovat. Jedná se o bezdrátový přenos (radiovou komunikaci za pomoci Um rozhraní), implementaci handoveru, kódování a dekódování hlasu, detekce a korekce chyb v přenosu a přístup ke kartě SIM. V této části MS je také uloženo IMEI číslo.

TA (Terminal Adapter) reprezentuje jednotné rozhraní, které zpřístupňuje služby MT tak, jako by se jednalo o ukončující bod ISDN sítě. Pro jeho ovládání se používají tzv. AT příkazy (jedná se o podmnožinu sady příkazů Hayes).

SIM (Subscriber Identity Module) uchovává všechna uživatelská data relevantní pro GSM síť, zejména IMSI číslo a klíč Ki, které jsou nutné pro autentizaci (viz kapitola 5.4). Zatímco MS je identifikováno za pomoci IMEI, uživatel se identifikuje právě pomocí SIM karty (vůči SIM kartě se uživatel verifikuje znalostí PIN kódu). Protože je SIM karta oddělitelná od MS, je jednoduché

personifikovat jakékoliv MS a využívat tak výrobky třetích stran (nezávisle na poskytovateli GSM připojení).



Obrázek 3.2 - Schéma mobilní stanice (MS), část A ukazuje vztahy mezi jednotlivými entitami MS, část B zdůrazňuje odlišnosti v zaměření entit

3.1.2 Base Transceiver Station (BTS)

Celá GSM síť je složena z velkého počtu buněk (cell) a každá tato buňka je řízena základnovou stanicí (BTS). Jedná se o zařízení, jehož hlavním účelem je bezdrátové propojení mobilních stanic se zbytkem sítě. Pod pojem BTS stanice se tedy zahrnuje veškeré potřebné technické vybavení nutné k bezdrátové komunikaci (antény, zesilovače, zpracování signálu).

Kromě přenosu dat zajišťují základnové stanice také šifrování komunikace s mobilní stanicí (musejí tedy znát šifrovací klíč *Kc* pro každou MS, kterou obsluhují, viz kapitola 5.4) a mohou provádět měření pro potřeby řízení handoveru (viz kapitola 5.3).

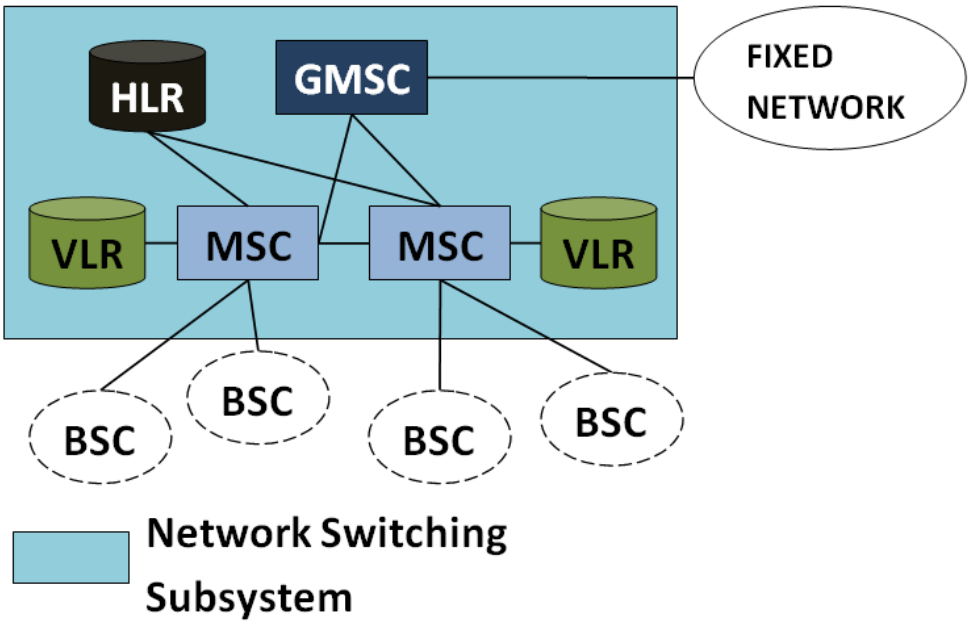
3.1.3 Base Station Controller (BSC)

BSC v podstatě řídí a kontroluje BTS stanice. Rezervuje rádiové frekvence, obsluhuje handovery z jedné BTS stanice na jinou v rámci BSS, zajišťuje paging (výzvu MS) atd.

3.2 Network Switching Subsystem (NSS)

Propojuje bezdrátovou přístupovou síť (RSS) s běžnou veřejnou sítí, zajišťuje handovery mezi různými BSS systémy a poskytuje funkce pro lokalizaci uživatelů.

Obrázek 3.3 ukazuje schéma NSS subsystému. Základ tvoří síť telefonních ústředen (MSC), které propojují jednotlivé BSC subsystémy navzájem a připojují ostatní sítě skrze bránové ústředny (GMSC). Také sem spadají GSM databáze, které zajišťují mobilitu sítě (HLR a VLR databáze).



Obrázek 3.3 - Schéma NSS

3.2.1 Mobile Service Switching Center (MSC)

Jedná se o vysoce výkonný digitální ISDN přepínač, je nejdůležitější částí páteční sítě. Nejdůležitější funkcí MSC je řízení hovoru a jeho přepínání. Vytváří spojení s ostatními MSC a s přidruženými BSC kontroléry. Také zajišťují propojení s ostatními sítěmi, jako jsou například PSTN a ISDN (v tomto případě mluvíme o tzv. gateway MSC – GMSC).

Další funkcí, kterou MSC zastává je komunikaci s GSM databázemi (HLR, VLR, EIR). Zajišťuje tak získání aktuální pozice mobilní stanice (zjištění jeho aktuální lokační oblasti), získání informací o službách, které může mobilní stanice využívat a zda není mobilní stanice evidována jako nefunkční či ukradená (EIR databáze).

MSC je také zapojeno do procesu účtování (platby za poskytnuté služby). Zajišťuje vytváření tzv. CDR záznamů (**Call Detail Records**), které potom zasílá do účtovacího centra. Zde jsou na základě takto získaných dat vytvářeny účty pro uživatele mobilní stanice. V případě zahraničních hovorů jsou tyto údaje poskytnuty i druhému zainteresovanému poskytovateli GSM připojení.

Jako centrální propojovací prvek zajišťuje MSC propojení s dalšími entitami, jako je hlasová schránka na straně sítě (služba poskytovaná provozovatelem GSM sítě, hlasová schránka v případě, že je mobilní stanice nedosažitelná či vypnutá), nebo SMSC (centrum pro zpracování SMS zpráv).

3.2.2 Visitor Location Register (VLR)

Každá mobilní ústředna (MSC) má svou vlastní VLR databází, která slouží k uložení všech potřebných údajů o MS, která se nacházejí v oblasti pod správou ústředny. Každá mobilní stanice (MS) může být v jednu chvíli pouze v jediné VLR databází.

Ukládaná data jsou získána přímo od HLR (povolené služby, informace pro přihlášení atd.) databáze nebo od MS (stav mobilního zařízení, lokační oblast atd.) Mezi ukládaná data patří tyto položky:

- TMSI (Temporary IMSI) – náhrada za neměnné IMSI, které se z důvodu bezpečnosti po síti přenáší co nejméně
- MSISDN – telefonní číslo MS
- Stav mobilního zařízení – zapnuto, vypnuto, mimo dosah
- Lokační oblast (Location Area) – skupina buněk, ve které se MS aktuálně nachází, viz kapitola 5.2
- Přístupový bod pro GPRS
- Adresa domovské HLR databáze mobilního zařízení
- Autentizační data – pro šifrování komunikace mezi MS a BTS, viz kapitola 5.4
- Seznam GSM služeb, které může MS využívat

3.2.3 Home Location Register (HLR)

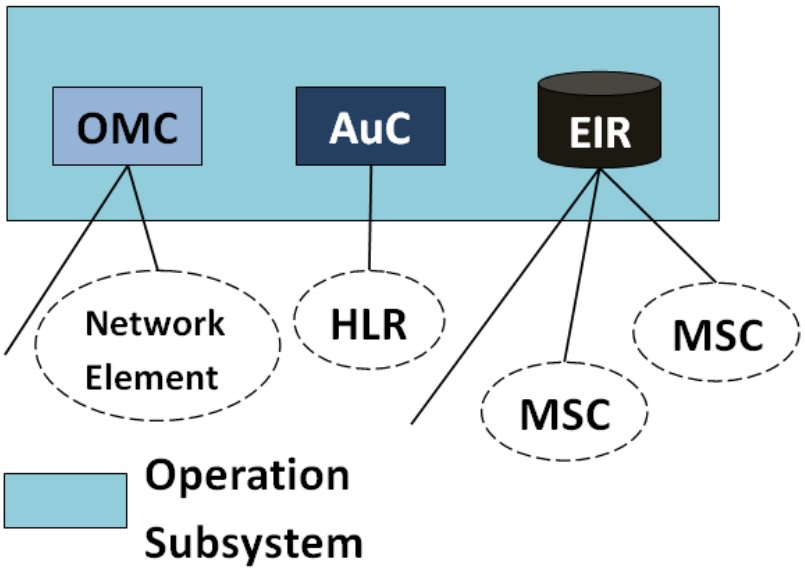
Jedná se o nejdůležitější databázi GSM systému, která obsahuje všechny podstatné údaje o vlastních uživatelích GSM sítě. To zahrnuje jak statické údaje (MSISDN, roaming restrictions, GPRS, IMSI, aktivované služby zákazníka), tak i dynamické údaje (identifikace současné lokalizační oblasti – location area, MSRN – Mobile Subscriber Roaming Number, aktuální využívanou VLR databázi a MSC).

3.2.4 Gateway Mobile Switching Center (GMSC)

GMSC slouží jako přístupový bod pro spolupráci s dalšími sítěmi. Například, pokud mluvíme o příchozím hovoru z pevné telefonní sítě, není v tomto případě poloha účastníka známa (protože pevná síť nemůže získat potřebné informace o poloze z HLR databáze). Potom bude hovor směrován skrz GMSC centrum (jako přístupový bod GSM sítě), které musí samo kontaktovat HLR databází (založeno na MSISDN), a získat tak pozici volané stanice přesměruje hovor k příslušné MSC/VLR. [4]

3.3 Operation Subsystem (OSS)

OSS se skládá z nezbytných funkcí pro síťové operace a údržbu. Zahrnuje několik síťových entit a ostatní zpřístupňuje za pomoci SS7 signalizace. Obrázek 3.4 jej schematický zobrazuje. Do této skupiny patří entity, které se přímo nepodílejí na funkčnosti GSM sítě, ale přidávají dodatečnou funkcionalitu. Mezi ně patří autentizační centrum (AuC), které se stará o bezpečnost v GSM síti, Equipment Identification Register (EIR), která spravuje IMEI čísla a OMC centrum.



Obrázek 3.4 - Schéma OSS

3.3.1 Equipment Identification Register (EIR)

EIR představuje databázi mobilních zařízení (reprezentována svými IMEI čísli), která nemají dovoleno připojit se do sítě nebo jsou sledována. Většinou je EIR součástí HLR databáze. Na rozdíl od ní však EIR může být více centralizované, protože jeho údaje nejsou aktualizována okamžitě. EIR se skládá ze tří částí:

- White List – obsahuje zařízení, která se mohou připojit do sítě
- Grey List – obsahuje seznam zařízení, u kterých je předpoklad, že jsou nefunkční. Umístěním do tohoto seznamu začne být aktivita mobilní stanice monitorována.
- Black List – obsahuje seznam zařízení, která nemohou síť využívat (tedy se do ní připojit), např. ukradené MS

3.3.2 Authentication center (AuC)

Autentizační centrum představuje databázi, nesoucí údaje o všech uživatelích, které náleží do dané GSM sítě. Obsahuje algoritmus pro autentizaci, algoritmus pro generování šifrovacího klíče, soukromé klíče uživatelů (*Ki*) a jejich IMSI. Samotné AuC bývá situováno do zvlášť chráněné části HLR.

Hlavní úlohou AuC je autentizace uživatelů GSM sítě. Tohoto procesu se centrum však přímo neúčastní, místo toho pro MSC generuje autentizační data, tzv. *triplet*.

Bezpečnost autentnizační procedury je založena na existenci sdíleného klíče *Ki*. Ten je do SIM karty napevno vypálen během její výroby a stejně tak je i napevno uložen v autentizačním centru. Tento klíč se nikdy v síti nepřenáší, pracuje se s ním pouze v rámci AuC a SIM karty, kde slouží jako jeden ze vstupů pro algoritmy A3 (autentizace) a A8 (generování šifrovacího klíče). Proces autentizace uživatelů je popsán v kapitole 5.4 - Autentizace v GSM sítidole.

Typicky používanými algoritmy v GSM sítích jsou algoritmus A3, který slouží ke generování odpovědí prokazující znalost klíče *Ki* , dále algoritmus A8 sloužící ke generování šifrovacího klíček *Kc* a algoritmus A5, kterým se šifruje komunikace. Použití algoritmů A3 a A8 ale není povinné, každý provozovatel GSM sítě může zvolit vlastní sadu algoritmů. Je to umožněno tím, že jejich použití je lokalizováno do té části sítě, která je plně pod kontrolou provozovatele (AuC a SIM).

3.3.3 Operation and Maintenance Center (OMC)

Provozní a řídící centrum, které monitoruje a kontroluje všechny ostatní síťové entity, komunikující skrze O rozhraní (SS7 s X. 25). Typickými funkcemi jsou monitorování provozu, správa bezpečnosti atd.

3.4 Ostatní entity

V GSM sítích mohou existovat i další entity, které přidávají další funkcionalitu. V předchozí části kapitoly byly zmíněny pouze základní entity, které se nacházejí v každé GSM síti a jsou nutné k její bezproblémové funkčnosti. Informace o pro tuto část kapitoly byly převzaty z [4].

Short Messaging Service Center (SMS-C)
Jednou z nejčastěji využívané služby v GSM je přenos *Short Messaging Service* (SMS). Tuto službu zajišťuje SMS-C, která rozhoduje o směrování SMS zpráv (které se liší od směrování v případě telefonního hovoru). Doručení SMS se skládá z několika kroků. Nejprve SMS-C zjistí cílovou adresu, kam SMS směruje, potom s využitím svých vlastních interních směrovacích tabulek zjistí informace o směrování a nakonec pošle SMS zprávu k přidružené MSC (která obsluhuje cílovou stanici), která zajistí její následný přenos mobilní stanici.

Také uchovává SMS zprávy, které nelze aktuálně doručit kvůli nedostupnosti MS (telefon je vypnutý nebo se nachází mimo dosah sítě).

Number Portability Location Register (NPLR)
Tato databáze poskytuje podporu pro sítě, kde je implementována přenositelnost telefonního čísla. Poskytuje směrovací informace uživatele s „přeneseným číslem“ podobně jako databáze používané pro portabilitu čísel v pevných sítích.

GSM Service Control Function (gsmSCF)
Obsahuje CAMEL (Customized Applications for Mobile network Enhanced Logic) pro implementaci služeb OSS.

CAMEL byl vyvinut jako standart pro distribuci inteligence GSM sítích skrze různé výrobce zařízení. Tím je míněno, že koncový uživatel je schopen pohybovat se mezi různými sítěmi (i v různých zemích) a být stále dostupný na stejném telefonním čísle a obdrží pouze jeden účet od svého původního poskytovatele služeb (tzv. *Home Operator*). [5]

Před zavedením CAMEL standardu byl pro zajištění inteligence v GSM sítích používán protokol INAP (*Intelligent Network Application Part*). Omezením INAPu bylo, že nepodporovalo správu mobility. CAMEL tento problém vyřešil a poskytl mnoho další funkcionality (která se s postupem vývoje 3G standardů rozšiřovala).

Voice Broadcast Service (VBS)/Voice Group Call Service (VGCS) relay MSC
Zajišťují získání potřebných atributů a ostatních dat z přidružených MSC pro skupinový hovor. Také řídí VBS/VGCS všechny buňky ve své oblasti, které patří do skupinového hovoru.

Group Call Register (GCR)
Jedná se o databázi, která má na starost atributy týkajících se řízení založení skupinových hovoru a broadcastových hovorů.

Serving Mobile Location Center (SMLC)
Databáze funkcí, které řídí procesy používané pro určení umístění mobilní stanice.

Gateway Mobile Location Center (GMLC)
Komunikuje s ostatními bezdrátovými sítěmi s cílem určení umístění mobilních stanic.

Location Measurement Unit (LMU)
Provádí poziční měření, které jsou dále použitý SMLC a GMLC s cílem získat pozici cílové mobilní stanice.

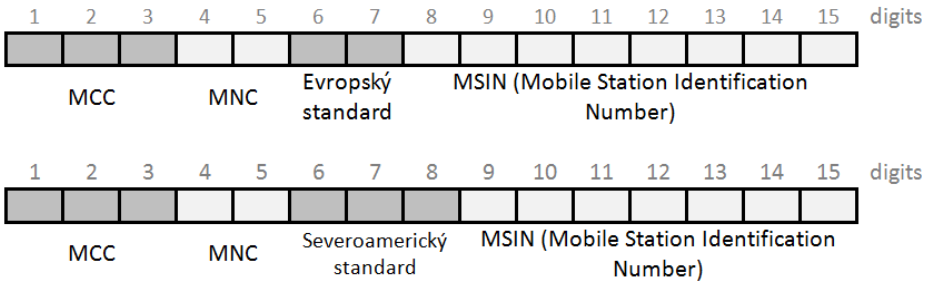
4 Číslování v GSM

4.1 IMSI (International Mobile Subscriber Identity)

Jedná se o celosvětově unikátní číslo, které je přiděleno mobilním operátorem každé SIM kartě v mobilní síti GSM a UMTS. Je uloženo jako 64bitové pole uvnitř SIM karty (každá číslice je uložena na čtyřech bitech). S ohledem na bezpečnost je použití IMSI co nejvíce minimalizováno a místo něj se používá TMSI.

IMSI číslo se nejčastěji reprezentuje jako číslo o 15 číslicích, ale může být i kratší. Jeho struktura se skládá ze čtyř částí (viz Obrázek 4.1):

1. ***Mobile Country Code*** (*MCC*) představuje celosvětově unikátní identifikátor státu (země) o pevné délce tří číslic. Jsou definovány v rámci specifikace `ITU E.212` (Land Mobile Numbering Plan). [6]
2. ***Mobile Network Code*** (*MNC*) – identifikátor, který v kombinaci s *MCC* slouží k jedinečné identifikaci mobilního operátora (v sítích GSM, CDMA, IDEN, TETRA a UMTS). V rámci dané země (v rámci dané *MCC*) je unikátní a identifikuje místního operátora a jeho délka závisí na *MCC* (typicky 2 číslice, ve velkých zemích má ale více číslic – např. Kanada má *MNC* dlouhé tři číslice). [7]
3. Následuje jedna ze dvou možností
    a. Dvoubitový evropský standard
    b. Tříbitový severoamerický standard
4. ***Mobile Station Identification Number*** (*MSIN*) – identifikace mobilní stanice v rámci mobilního operátora.



Obrázek 4.1 - Schéma IMSI, reprezentováno 15 číslicemi

4.2 TMSI (Temporary Mobile Subscriber Identity)

Jedná se o dočasnou identifikaci uživatele, která se používá ke zvýšení bezpečnosti GSM systému a nahrazuje použití *IMSI* čísla. Jedná se o unikátně zvolený identifikátor, který je však platný pouze v aktuální lokační oblasti. Proto musí docházet k aktualizaci tohoto identifikátoru nejpozději při

každé změně lokalizační oblasti (Location Update, LU). O to se stará VLR databáze, kde je TMSI identita také uložena.

TMSI hraje klíčovou roli během tzv. paging akce. Jedná se o komunikaci mezi mobilním zařízením a BTS stanicí. Nejdůležitějším využitím je nastavení kanálů pro paging. Každý mobilní buňkový systém má svůj mechanizmus distribuce takovýchto informací pro více mobilních zařízení [8].

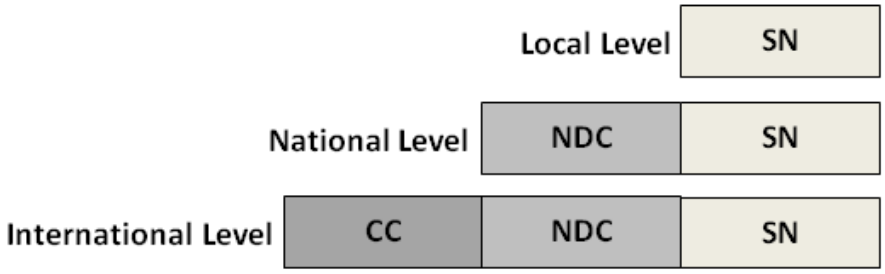
TMSI číslo je dlouhé čtyři oktety (32 bitů) a spolu s identifikátorem aktuální lokační oblasti (LAI, viz kapitola 4.4) jednoznačně identifikuje mobilní stanici.

4.3 MSISDN (Mobile Station International ISDN Number)

Jedná se o celosvětově unikátní číslo, které identifikuje SIM kartu v mobilních sítích GSM a UMTS. Pro uživatele mobilních sítí se jedná o tzv. **telefonní číslo** jejich mobilního telefonu.

MSISDN číslo je většinou uváděno v mezinárodním tvaru kde začátek tvoří tzv. *mezinárodní přestupový znak.* Jedná se o posloupnost znaků (nejčastěji se jedná o znak křížku + nebo dvojici nul *00*), které se musejí zadat před zadáním vlastního volaného čísla, aby se tak vyjádřil požadavek, že se jedná o mezinárodní hovor. Jeho délka se nezapočítává do celkové délky *MSISDN* čísla. Maximální délka *MSISDN* čísla je stanovena na hodnotu 15 číslic, které tvoří tři části (viz Obrázek 4.2) [9]:

1. *Country Code* (CC) představuje unikátní kód země o délce jedné až tří číslic.
2. *National Destination Code* (NDC) reprezentuje národní směrové číslo, které určuje mobilní síť v příslušné zemi (v rámci dané CC).
3. *Subscriber Number* (SN) představuje účastnické číslo, které určuje konkrétní SIM kartu. V rámci dvojce CC/NDC je unikátní a přiděluje jej provozovatel GSM sítě.



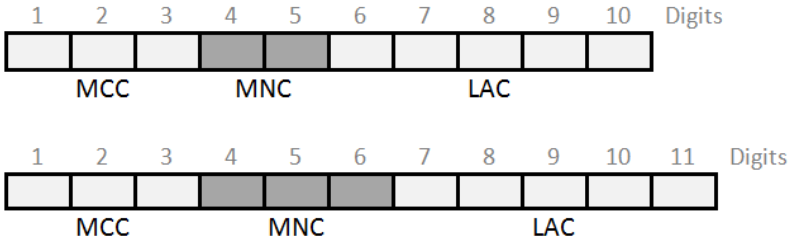
Obrázek 4.2 - Formát MSISDN, převzato z [10]

4.4 LAI (Location Area Identity)

Každá oblast, na které je dělena GSM síť, je identifikována celosvětově unikátním identifikátorem. Ten slouží k jednoznačnému určení polohy, ve které se mobilní stanice nachází. Skládá se ze tří po sobě jsoucích částí (viz Obrázek 4.3) [11]:

1. **Mobile Country Code** (*MCC*) představuje celosvětově unikátní identifikátor státu (země) o pevné délce tří číslic. Jsou definovány v rámci specifikace `ITU E.212` (Land Mobile Numbering Plan). [6]

2. ***Mobile Network Code*** (*MNC*) – identifikátor, který v kombinaci s *MCC* slouží k jedinečné identifikaci mobilního operátora (v sítích GSM, CDMA, IDEN, TETRA a UMTS). V rámci dané země (v rámci dané *MCC*) je unikátní a identifikuje místního operátora a jeho délka závisí na *MCC* (typicky 2 číslice, ve velkých zemích má ale více číslic – např. Kanada má *MNC* dlouhé tři číslice). [7]
3. *Location Area Code* (LAC) představuje číslo, které identifikuje lokační oblast v rámci daného poskytovatele GSM připojeni. Jeho maximální délka je pět decimálních číslic nebo dvojce hexadecimálních číslic, které jsou kódovány na osmi bitech (LAC < FFFF) [12]. To znamená, že jeden poskytovatel GSM připojení může spravovat až 65536 (maximální hodnota, kterou lze uložit na 16 bitech) lokačních oblastí.



Obrázek 4.3 - Schéma LAI

4.5 IMEI (International Mobile Equipment Identity)

Jedná se o číslo, obvykle unikátní, které slouží k identifikaci mobilního zařízení. Skládá se ze 14 dekadických číslic a jedné kontrolní číslice. V těchto patnácti číslicích je uchována informace o původu, modelu a sériovém čísle mobilního zařízení.

Formát IMEI čísla je AA-BBBBBB-CCCCCC-D (v tomto formátu nemusí být vždy zobrazen, pomlčky mohou být vynechány), kde každé písmeno představuje jednu číslici. IMEI se skládá ze tří částí (viz Obrázek 4.4):

1. ***Type Allocation Code*** (TAC) – prvních osm číslic IMEI čísla (část formátu IMEI označená jako AA-BBBBBB), obsahují informace o modelu a původu mobilního zařízení.
2. **Sériové číslo** – dané výrobcem mobilního zařízení (část formátu IMEI označená jako -CCCCCC).
3. Poslední číslici (část formátu IMEI označená jako D) tvoří zabezpečující **checksum** (SPARE), který je vypočten za pomoci Luhnův algoritmu. Přítomnost této složky je volitelná a nikdy nedochází k jejímu přenosu.

Až do roku 2002 byl *Type Approval Code* (TAC) šest číslic dlouhý. Za ním následovaly dvě číslice, které reprezentovali tzv. *Final Assembly Code* (FAC) – hodnota, která odkazuje na oblast, kde bylo mobilní zařízení sestrojeno (viz Obrázek 4.4). Od prvního ledna 2003 až do prvního dubna 2004, vylo FAC pro všechny mobilní zařízení rovno hodnotě *00*. Po prvním dubnu 2004 přestal FAC existovat a délka TAC narostla právě o tyto dvě číslice. Převzato z [13].

První dvě číslice IMEI čísla (označené jako AA) představují tzv. ***Reporting Body Identifier***, který označuje, která GSMA organizace registrovala (před rokem 2002 schválila) dané mobilní zařízení a přidělila mu jeho unikátní kód. [13]

<table>
<tr><th></th><th colspan="2">AA</th><th>-</th><th colspan="2">BB</th><th>BB</th><th>-</th><th colspan="3">CC</th><th>D</th></tr>
<tr><td>Starý formát IMEI</td><td colspan="5">TAC</td><td>FAC</td><td colspan="3" rowspan="2">Sériové číslo</td><td rowspan="2">Checksum za pomoci Luhnův algoritmu (volitelné)</td></tr>
<tr><td>Nový formát IMEI</td><td colspan="6">TAC</td></tr>
</table>

Obrázek 4.4 - formát IMEI

4.6 LMSI (Local Mobile Subscriber Identity)

Pro zvýšení efektivity činnosti VLR databáze, může dojít k přidělení dalšího identifikátoru, nazývaný jako *Local Mobile Subscriber Identity*, který slouží jako vyhledávací klíč. Je přidělován VLR databází každé evidované mobilní stanici během její registrace do VLR databáze. Současně s jeho přidělením dojde i k jeho zaslání HLR databázi.

Vytvořením lokálního identifikátoru, který si každá VLR databáze vytváří a spravuje sama, umožňuje přihlédnout k dané implementaci VLR databáze a optimalizovat tak vyhledávání v jejích registrech. Jedinou pevně stanovenou podmínkou struktury *LMSI* je její délka – skládá se ze čtyř oktetů (celkem tedy 32bitů).

4.7 Cell Identifier (CI):

V rámci dané lokační oblasti (LA) je každá jednotlivá buňka, která danou LA tvoří, unikátně identifikovaná za pomoci čísla *Cell Identifier* (CI). Jeho délka je maximálně 16 bitů (2 oktety).

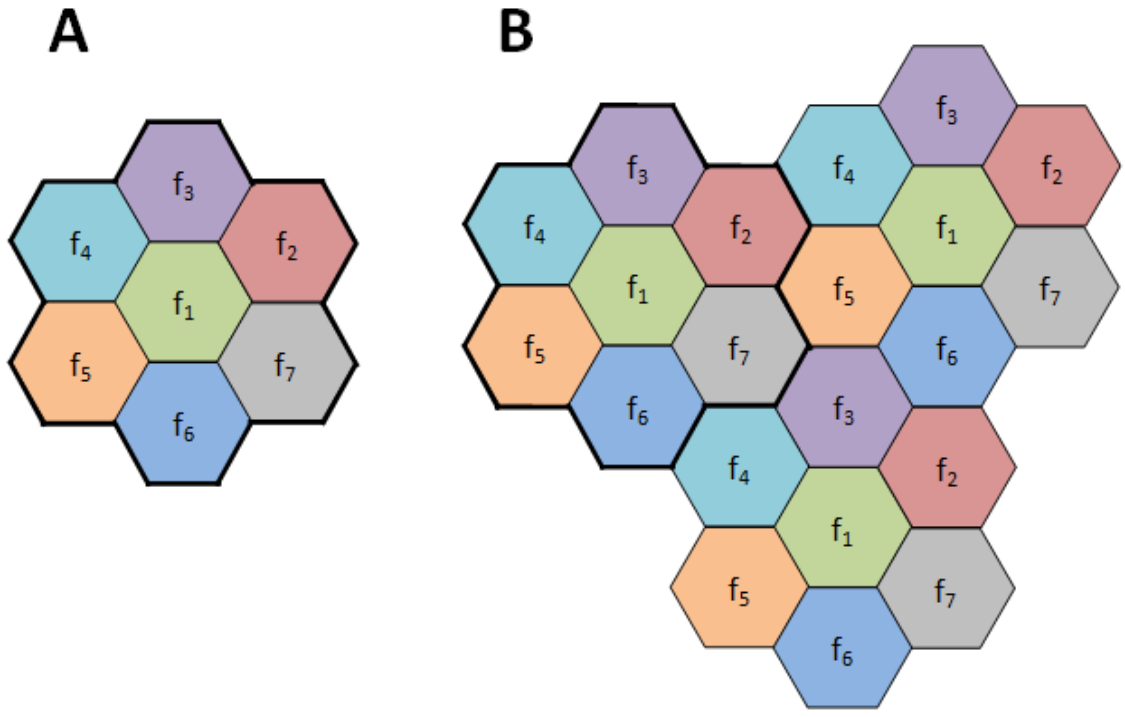
Každou buňku lze unikátním způsobem identifikovat i v globálním měřítku. Pro tyto účely je nutné využít kombinaci dvou hodnot – LAI (*Local Area Identifier*) a CI (*Cell Identifier*). LAI hodnota celosvětově jedinečně určuje lokační oblast, ve které se daná buňka nachází, oproti tomu CI hodnota určí v dané lokační oblasti vlastní buňku.

5 Vlastnosti GSM sítě

GSM síť spadá do kategorie **buňkových sítí** (cellular network). Jejich charakteristickou vlastností je distribuce rádiového signálu skrze malé geografické oblasti nazývané **buňka** (cell). Každá z nich je řízena nejméně jedním pevně umístěným transceiverem, známý jako základnová stanice. Spojení těchto buněk zajišťuje pokrytí signálem v rozlehlé oblasti za použití relativně nízkého počtu nosných frekvencí.

5.1 Kmitočtové plánování

Základní kámen pro **kmitočtové plánování** představuje takzvaný **svazek.** Jedná se o shluk buněk, které využívají vzájemně odlišné frekvence (viz Obrázek 5.1 A). Tento svazek se pak následně opakuje v celé sítí a díky tomu je možné omezeným počtem frekvencí (či setem frekvencí) pokrýt v podstatě nekonečně velké území. Kmitočtové plánování přestavuje činnost, během níž se podle předpokládaného zatížení sítě provede rozdělení dostupného frekvenčního pásma (přidělené nosné frekvence) do několika skupin (počet těchto skupin odpovídá počtu buněk ve svazku). Potom dojde k přidělení těchto skupin jednotlivým buňkám v rámci svazku tak, aby buňky s největším zatížením získaly skupinu s největším počtem nosných frekvencí.



Obrázek 5.1 - Schéma principu opakovaného použití frekvencí, A – svazek, B – příklad sítě využívající sedm frekvencí

V současnosti se používají dva způsoby přidělování frekvenčních kmitočtů buňkám:

1. **Pevné přidělení frekvencí** (Fixed Channel Allocation – FCA)
2. **Dynamické přidělení frekvencí** (Dynamic Channel Allocation – DCA)

FCA princip rozdělí dostupné kmitočtové pásmo do několika skupin, jejichž počet odpovídá počtu buněk, které v dané síti tvoří svazek. Každá skupina je potom s ohledem na kmitočtové plánování přidělena jedné buňce svazku.

Výhodou je jednoduchost implementace, kdy se na začátku nastaví parametry sítě a ta s nimi pak pracuje. Nevýhodou je nepřizpůsobivost sítě dynamice uživatelů, ve vytížených buňkách není možné využít volné kanály, které okolní buňky nepoužívají.

Druhým používaným způsobem je **dynamické přidělování frekvencí.** V tomto případě je každý rádiový kanál dostupný každé buňce ve svazku, pokud to dovolují interference s okolními buňkami. Díky tomu síť sama vyvažuje zátěž, kdy aktuálně vytížené buňky získávají více kanálů než buňky s nízkým počtem uživatelů.

Nevýhodou toho řešení je nutnost použít složitější a dražší základnové stanice, které musejí být schopny pracovat na všech dostupných frekvencích.

Oproti jiným typům řešení poskytují buňkové sítě díky své koncepci dělení do buněk několik významných výhod:

1. Dosahují značné kapacity uživatelů sítě.
2. Je redukován nutný vysílací výkon jak na straně mobilní stanice, tak na straně vysílače (díky dělení do buněk je komunikováno na vzdálenost maximálně poloviny velikosti buňky).
3. Pokrývají signálem rozsáhlé oblasti, které jsou snadno rozšiřitelné přidáním nových buněk.
4. Redukují interference mezi ostatními používanými signály. Pokud existuje v oblasti nějaký druh rušení, který by ovlivňoval komunikační kanály, jsou v zasažených buňkách použity ty frekvence, které jsou zasaženy nejméně.

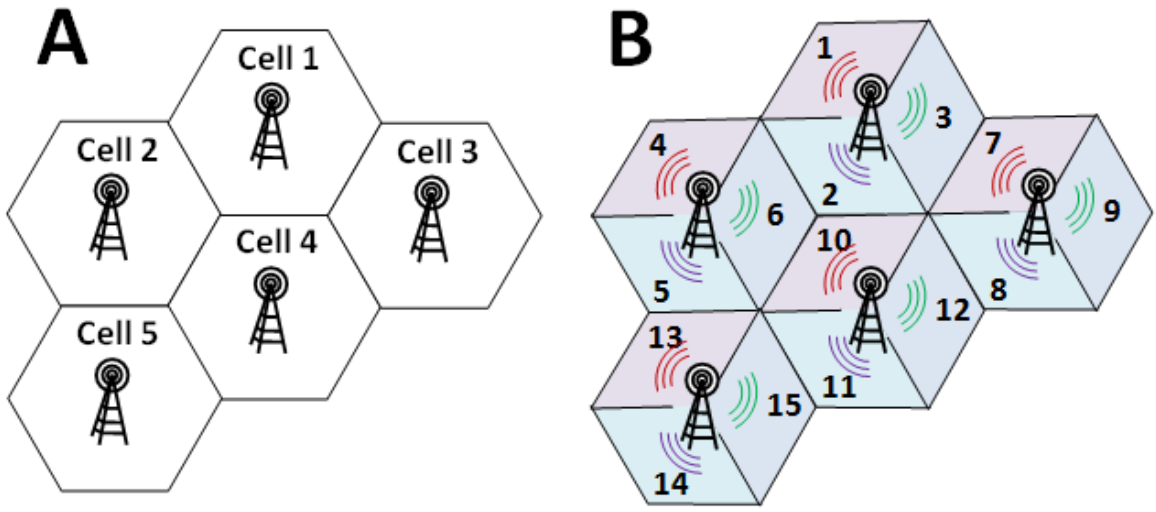
Buňkový přístup sebou však přináší i několik problémů:

1. Nutnost implementovat přechod aktivního uživatele od jedné buňky k druhé – tzv. handover.
2. Vznik interferencí mezi buňkami. Tento problém se snaží řešit kmitočtové plánování, přesto k nim dochází.
3. Nutnost propojení základnových stanic pevnou sítí.

Budování základnových stanic je nákladné a v některých případech i složité (zakomponování stanice do již existující městské zástavby). Zavedením systému sektorových antén je dosaženo redukce ceny infrastruktury sítě, protože některé základnové stanice (ty, které řídí sektorové buňky) sdílejí část hardwarového vybavení a přidrženou infrastrukturu – stožár, pevnou propojující síť atd. (viz Obrázek 5.2, kde je porovnána síť s a bez sektorových buněk. Část B schematický naznačuje, sdílení základnových stanic pro trojice buněk – např. buňky 1, 2 a 3).

Výhodou použití směrových antén je možnost soustředit signál určitým směrem a tak v daném směru navýšit kapacitu sítě. Toho je využíváno například v případě dálnic, kdy jsou buňky budovány tak, aby se za pomoci sektorizace oddělilo pokrytí dálnice a území okolo nich. Tím lze navýšit kapacitu pro dálniční buňky na úkor jejich okolí (kde je koncentrace mobilních stanic řádově nižší než na dálnicích).

Obrázek 5.2 popisuje vznik nových buněk za použití **sektorizace buněk.** Toho je docíleno použitím sektorových antén, které stávající buňky rozdělí na sektory – nové buňky. Část A ukazuje část sítě, která nepoužívá sektorové antény. V tomto případě je nutné pro každou buňku vybudovat jednu základnovou stanici (na obrázku se síť skládá z pěti buněk a proto má i pět BTS stanic). Část B zvyšuje kapacitu sítě zavedením nových buněk, které vzniknou sektorizací buněk stávajících.



Obrázek 5.2 - Redukce počtu fyzických BTS stanic za pomoci sektorových antén, A – schéma sítě bez sektorových antén, B – schéma sítě se sektorovými anténami

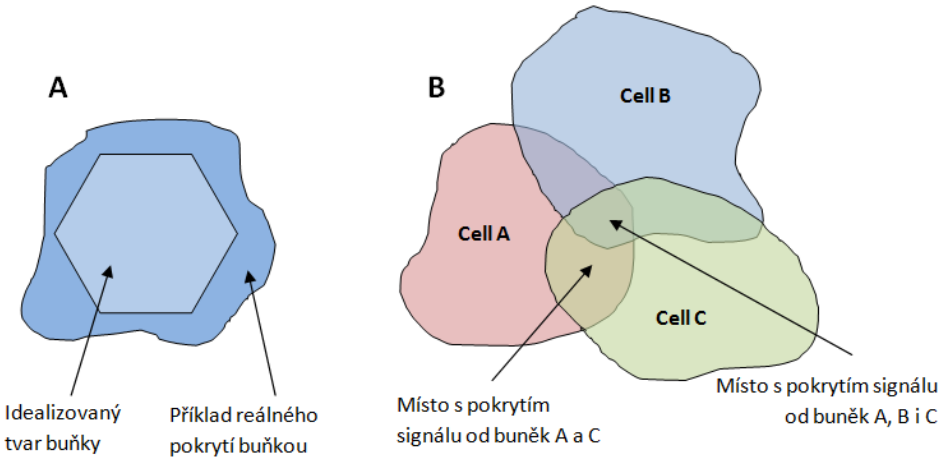
5.2 Oblasti sítě

Buňka (cell) představuje zeměpisnou oblast pokrytou signálem, která spadá pod správu jedné BTS stanice (nebo sektorové antény BTS stanice). Každá nosná frekvence, kterou buňka používá, definuje celkem osm *timeslotů*. To znamená, že na každé frekvenci může být ve stejné chvíli obslouženo až osm uživatelů. Tento počet je však příliš malý, proto většina buněk operuje s více nosnými frekvencemi.

Pro jednoduchost se tvar buňky modeluje jako idealizovaný šestiúhelník (či jiný pravidelný útvar). Ovšem skutečný tvar oblasti, kterou daná buňka pokrývá, je závislý na okolním terénu a je tak nepravidelný (viz Obrázek 5.3 A). Protože jsou hranice buněk nepravidelné, dochází k překrývání jejich působnosti (viz Obrázek 5.3 B). Pokud se mobilní stanice nachází v této oblasti, je připojena pouze k jediné BTS stanici. Ostatní stanice, které zde mají svůj signál, představují jednu z možných budoucích cílových buněk.

Velikost buňky není pevně daná, pohybuje se v rozsahu sta metrů až 35 kilometrů. Díky tomu je možné diferencovat buňky podle typu použití:

1. **Makro buňka** má největší dosah (až 35 kilometrů) a je určena do otevřených oblastí s nízkou hustotou obyvatel. Používá se mimo města (např. venkov), kde by budování husté sítě BTS stanic bylo příliš nákladné a neefektivní.
2. **Mikro buňka** se používá zejména ve městech. Jedná se o kompromis mezi kapacitou buňky a jejím vysílacím výkonem. Mají střední dosah, díky čemuž se jich může ve městě použít větší počet a zajistit tak vysokou obslužnost sítě.
3. **Piko buňky** mají nejmenší dosah a nalézají uplatnění uvnitř budov s vysokou koncentrací mobilních stanic (např. nákupní středisko, nemocnice).

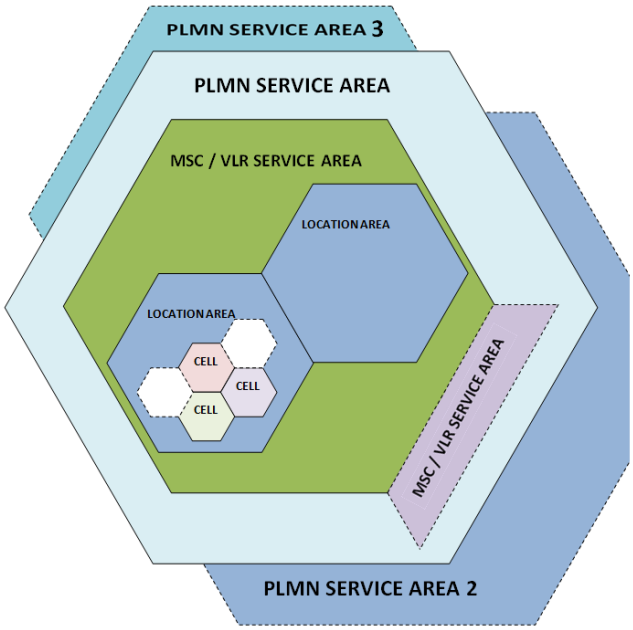


Obrázek 5.3 - Buňka, A - vzhled idealizované a reálné buňky, B - překrytí signálu jednotlivých buněk

Lokační oblast (Location Area) se skládá z několika buněk, které jsou řízeny jedním BSC kontrolérem. Každá lokační oblast má své označení LAI (Location Area Identity). Tento identifikátor je v rámci daného poskytovatele připojení unikátní.

MSC/VLR service area je zeměpisná oblast, která spadá pod správu jedné ústředny (MSC) a jí přidružené VLR databázi (obsahuje informace o všech aktivních MS, které se v dané oblasti nacházejí). Skládá se z několika lokačních oblastí.

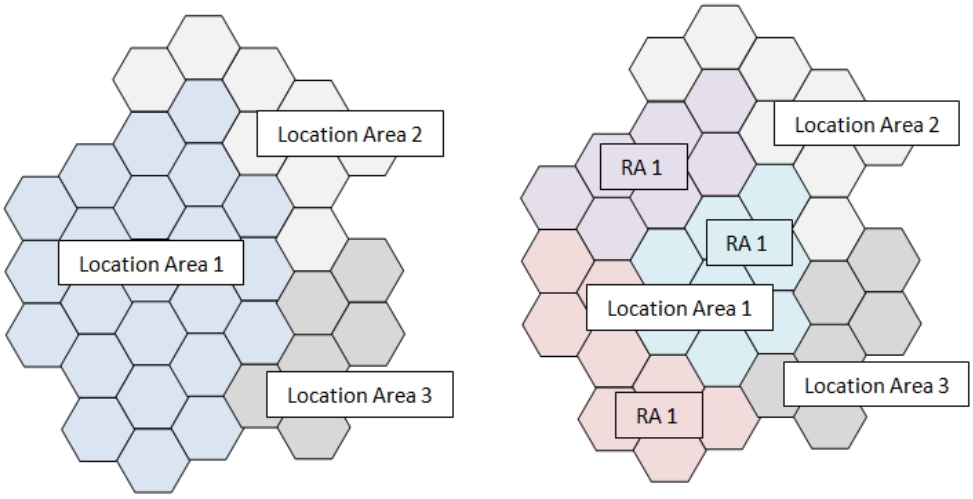
PLMN (Public land mobile network) je obecný název pro bezdrátovou síť, která je provozována a spravována jednou organizací za účelem poskytnutí mobilních služeb veřejnosti. **PLMN service area** je zeměpisná oblast, ve které PLMN nabízí své služby (např. oblast, kterou pokrývá svým signálem Vodafone CZ v České republice).



Obrázek 5.4 - Schéma hierarchie GSM zeměpisných oblastí

S příchodem GPRS datových přenosů nastal problém s dosud používanou velikostí lokačních oblastí – pro potřeby GPRS byly příliš velké a neúměrně tak zatěžovaly síť. Proto byla zavedena nová oblast

– **Routing Area (RA).** Ve své podstatě se jedná pouze o rozdělení lokačních oblastí na několik menších celků, ovšem s ohledem na hranice lokační oblasti (žádná z RA nepřesahuje hranice své LA, viz Obrázek 5.5).



Obrázek 5.5 – Vznik nové oblasti Routing Area, původní lokační oblast je rozděleno na několik menších oblastí – Routing Area

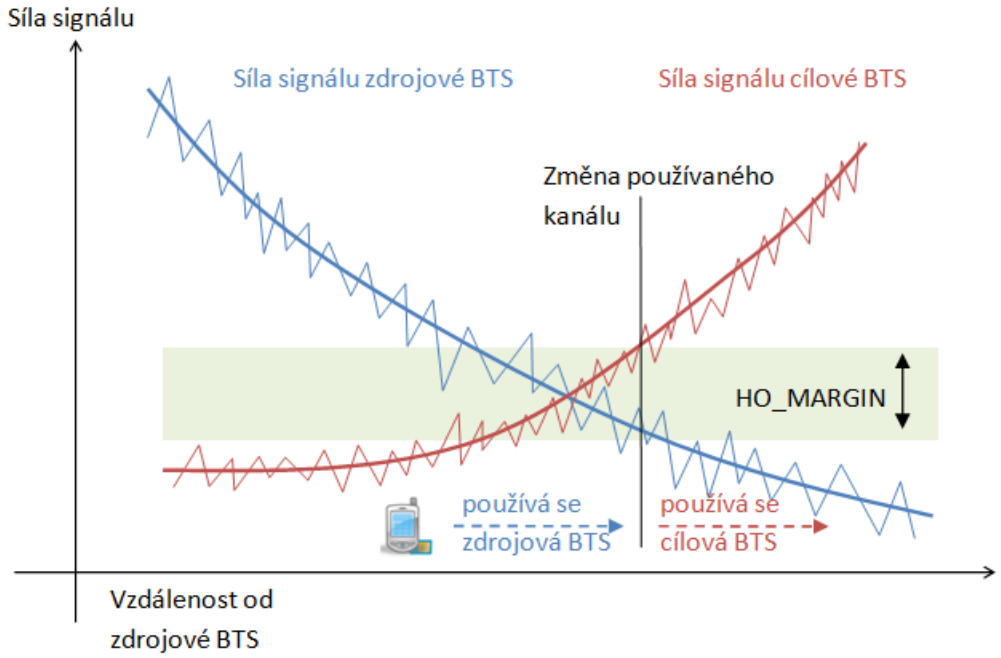
5.3 Handover

Tak jako každá buňková síť, i GSM muselo přijít s řešením problému, který nastává s pohybem uživatelů během hovoru. S tím, jak se uživatel pohybuje, může dojít k situaci, kdy opustí svou stávající buňku (nazývanou jako zdrojová buňka, source cell) a přejde do buňky nové (tzv. cílové buňky, destination cell). Protože sousedící buňky operují na rozdílných frekvencích (viz kapitola 5.1), je nutné, aby se mobilní stanice při přechodu přes hranice buněk přizpůsobila a začala operovat na nové frekvenci (na které operuje cílová buňka). K této změně musí dojít automaticky (bez zásahu uživatele mobilní stanice) a velmi rychle, aby nedošlo k ovlivnění probíhající komunikace.

Rozhodnutí o provedení handoveru je učiněno na základě kvalitativních parametrů aktuálně používaného kanálů (zdrojové buňky) a ostatních dostupných kanálů (na které je možné přejít). Používanými kvantifikátory kvality kanálů jsou:

1. Síla přijímaného signálu (RSS – Received Signal Strength)
2. Odstup signálů od šumu (SNR – Signal-to-Noise Ratio)
3. Bitová chybovost (BER – Bit Error Rate)

Protože kvalita kanálů kolísá, je nutné, aby měla síť určitou setrvačnost při rozhodování o provedení handoveru. Bez ní by docházelo k přepínání kanálů během každé lokální změny kvality používaného kanálu. Například pokud by se mobilní stanice pohybovala na hranici buněk A a B, neustále by docházelo k jejich vzájemnému handoveru. Tento problém řeší zavedení hodnoty *HO_MARGIN*, která určuje, o kolik musí být kvalita kanálu cílové BTS stanice lepší, než kvalita kanálu zdrojové BTS, aby bylo rozhodnuto o provedení handoveru (viz Obrázek 5.6).

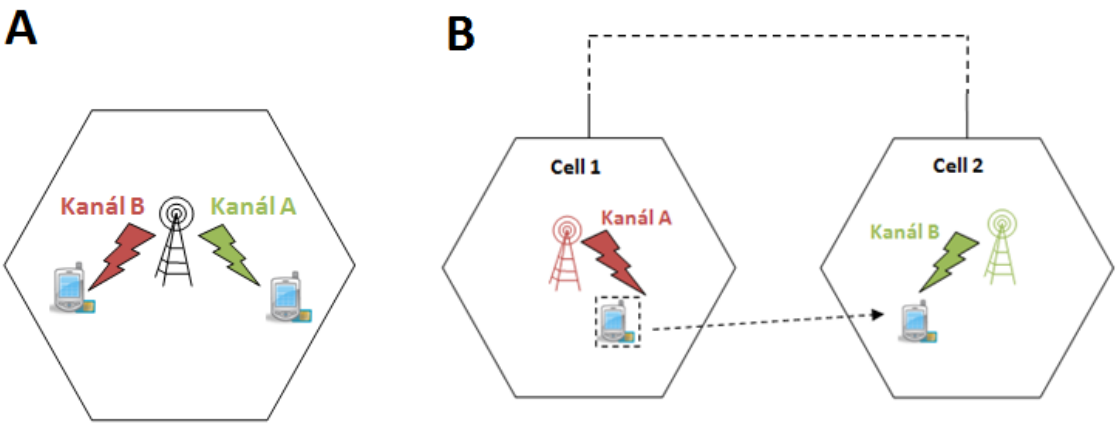


Obrázek 5.6 – Schéma setrvačnosti sítě v rozhodování o handoveru za použití hodnoty HO_MARGIN

5.3.1 Typy handoverů podle rozsahu

Podle rozsahu prováděného handoveru (zda se jedná o handover v rámci jedné buňky nebo zda dochází k její změně) se vyčleňují dvě základní skupiny (viz Obrázek 5.7):

1. Intra-cell handover (vnitrobuňkový handover)
2. Inter-cell handover (mezibuňkový handover)



Obrázek 5.7 - Typy handoveru, A - Intra-cell, B - Inter-cell

Pokud mobilní stanice změní používaný kanál v rámci jediné buňky (zdrojová buňka se shoduje s cílovou), potom se jedná o **intra-cell handover** (vnitrobuňkový). Typickým důvodem pro změnu kanálu v rámci jedné buňky je vznik rušení, které zhoršuje vlastnosti části používaných kanálů. Protože však nezasahuje do všech kanálů buňky, je žádoucí využívat zbývající nezarušené kanály. Pokud tedy nejsou aktuálně používány, provádí se na ně handover.

Obrázek 5.7 A schematicky popisuje tuto situaci. Mobilní stanice původně operuje na kanálu A. Časem se však na tomto kanále objeví rušení, díky čemuž klesne jeho kvalita. Protože v dané buňce existuje nevyužitý kanál B, kterého se rušení netýká, provede se handover a mobilní stanice začne komunikovat na tomto nerušeném kanále.

Ve většině případů však prováděný handover patří do kategorie **inter-cell (mezibuňkový).** Rozdílem oproti předcházejícímu typu je, že během handoveru dochází ke změně používané buňky (cílová buňka je odlišná od zdrojové). Typickým důvodem pro vznik požadavku na tento typ handoveru je pohyb mobilní stanice. Spolu se změnou polohy MS se mění i vzdálenosti od jednotlivých BTS stanic (a tím se mění kvalita jednotlivých kanálů). Až v jednu chvíli dojde k překročení hranic buněk a s tím i spojeného handoveru na novou BTS stanici.

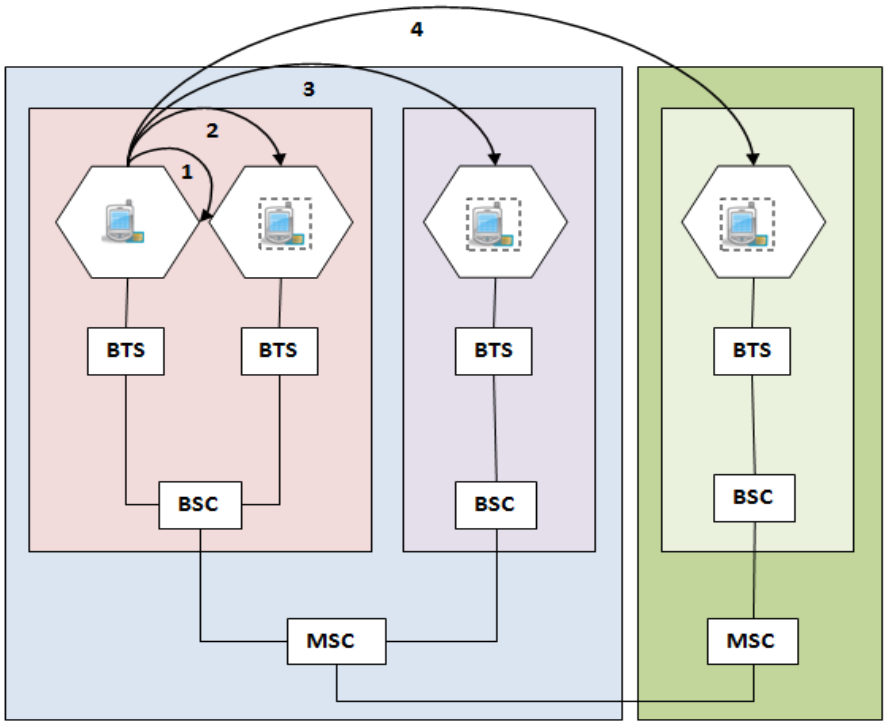
Důležitou vlastností, která je na provedení handoveru kladena, je rychlost jeho provedení. Proto se na jeho provedení podílí jen ty entity, které jsou nezbytně nutné (tedy ty, co leží v cestě od zdrojové buňky k cílové buňce). Proto rozlišujeme tři typy mezibuňkových handoverů (viz Obrázek 5.8, kde je ukázán i intra-cell handover – označen číslem 1):

1. Intra-BSC handover (handover v rámci jednoho BSC kontroléru)
2. Intra-MSC handover (handover v rámci jedné ústředny)
3. Inter-MSC handover (meziústřednový handover)

Intra-BSC handover nastává, pokud spadají zdrojová a cílová buňka do jedné lokační oblasti (jsou řízeny stejným BSC kontrolorem). V tomto případě se jeho provedení účastní BTS zdrojové a cílové buňky a také náležící BSC kontrolér (viz Obrázek 5.8 - 2).

Pokud se lokační oblast zdrojové a cílové buňky liší, ale stále spadají do stejné MSC/VLR oblasti, mluvíme o **intra-MSC handoveru** (handoveru v rámci stejné ústředny). V tomto případě se procesu účastní zdrojová a cílová BTS stanice, jejich příslušné BSC kontroléry a MSC, do jejíhož pole působnosti obě buňky spadají (viz Obrázek 5.8 - 3).

Posledním typem je **inter-MSC handover** (meziústřednový handover), který je z hlediska množství zúčastněných entit nejrozsáhlejší. V tomto případě zdrojová a cílová buňka spadají do odlišných MSC/VLR oblastí a provedení handoveru tedy nejsložitější a podílí se na něm nejvíce entit (viz Obrázek 5.8 - 4).



Obrázek 5.8 - Typy handoverů podle rozsahu, 1 – intra-cell handover, 2 – intra-BSC handover, 3 – intra-MSC handover, 4 – inter-MSC handover

5.3.2 Typy handoverů podle typu řízení

Existují tři možnosti, jak realizovat handover, které se liší toho, kdo se na rozhodnutí o provedení handoveru podílí:

1. Handover řízený systémem/sítí (tzv. NCHO – *Network Controlled Handover*)
2. Handover řízený mobilní stanicí (tzv. MCHO – *Mobile Controlled Handover*)
3. Handover řízený se spoluúčastí mobilní stanice (tzv. MAHO – *Mobile Assisted Handover*)

V případě, že o provedení handoveru rozhoduje pouze síť, mluvíme o **handoveru řízený systémem**. Mobilní stanice se rozhodování vůbec neúčastní. Jejím úkolem je pouze vysílat kontrolní signál, který přijímají všechny základnové stanice v jejím dosahu. Informace o přijetí toho signálu jsou předány odpovědnému rozhodovacímu procesu (který může být implementován jako část ústředny), který na základě porovnání síly signálu od všech stanic rozhodne, která stanice má nejvhodnější podmínky pro komunikaci s mobilní stanicí. Podle toho se podle potřeby provede handover.

Výhodou je, že se nikterak nezatěžují mobilní stanice, které nemusejí provádět žádná měření ani přenášet žádná data, která by sloužila k rozhodování. Výhodu lze také spatřovat v tom, že síť má absolutní kontrolu nad svými uživateli, ona sama rozhoduje, zda provést či neprovést handover.

Tento způsob řízení však klade vyšší požadavky na propustnost sítě (část přenosové kapacity datových linek mezi základnovými stanicemi a rozhodovacím procesem je neustále využívána pro přenos informací o naměřených kontrolních signálech). V případě vyšší koncentrace mobilních stanic v jedné oblasti dochází k plýtvání rádiovým pásmem, neboť každá stanice vysílá svůj kontrolní signál. S rostoucím počtem mobilních stanic tedy roste i počet vysílaných signálů, které je nutné od

sebe oddělit. Tento způsob řízení se uplatňoval zejména u starších analogových systémů (lze jej nalézt např. u systému NMT).

Pokud v předcházejícím případě náleželo rozhodování pouze síti, potom v případě **handover řízeného mobilní stanicí** je systém zodpovědný za rozhodování lokalizován na mobilní stanici. Měření síly signálu tentokrát provádějí obě entity – jak síť, tak i samotná mobilní stanice. Na základě těchto informací vybere mobilní stanice nejvhodnější BTS stanici. Pokud se vybraná stanice liší od stávající (dojde tedy k nutnosti provést handover), informuje o tom mobilní stanice přímo novou BTS stanici, které se o provedení handoveru již postará.

Tento způsob řízení je zdaleka nejrychlejší a také nejlépe využívá buňkový prostor. Cenou je změna koncepce mobilní stanice, která již není pouze koncovým uživatelem, ale stává se i rozhodovací entitou. Do popředí také vystupuje otázka bezpečnosti, kdy důležitý element řízení sítě je předán mimo kontrolu sítě. S tímto druhem řízení se lze setkat např. u bezdrátových telefonů typu DECT.

Pokud se na rozhodování podílí obě entity, mluvíme o **handoveru řízeném se spoluúčastí mobilní stanice.** V tomto případě provádí mobilní stanice neustálé měření kvality signálů dostupných BTS stanic a výsledek o měření předává stanici, ke které je aktuálně přiřazena (se kterou komunikuje). Tyto hodnoty jsou stejně, jako v případě handoveru řízeného sítí, předány odpovídající rozhodovací entitě (typicky ústředně), která v případě potřeby vybere novou BTS stanici. Kromě mobilní stanice může měření provádět i sama síť (základnové stanice). Ovšem rozhodující jsou právě hodnoty získané z MS.

Tento způsob řízení přihlíží k lokálním podmínkám, ve kterých se mobilní stanice nachází a distribuuje zátěž řízení (vyhodnocení kvality signálu na MS, rozhodování o handoveru v síti). Také se zde dosahuje kompromisu v bezpečnosti, kdy sice rozhodující vliv mají data získaná od mobilní stanice, ale poslední slovo má samotná sít. Oproti předcházejícím způsobům řízení dochází v rádiovém spektru k vyšší zátěži (oproti řízení mobilní stanicí) a roste komplikovanost komunikačního protokolu pro komunikaci s BTS stanicí (oproti řízení systémem, kdy se vysílá pouze kontrolní signál). Tento způsob řízení je implementován např. v GSM síti.

5.3.3 Typy handoverů podle realizace

Předcházející kapitola popisovala různé typy implementace rozhodovacího procesu. Pokud již tedy bylo o provedení handoveru rozhodnuto, je nutné jej ještě provést. Z hlediska existence komunikačního kanálu můžeme rozlišit tři různé přístupy:

1. Hard handover (tvrdý handover)
2. Seamless handover (bezešvý handover)
3. Soft handover (měkký handover)

Pokud mobilní stanice nejprve přeruší spojení s opouštěnou základnovou stanicí a teprve potom se připojí na stanici novou, mluvíme o **hard handoveru** (tzv. tvrdém handoveru). Důležité je co nejvíce minimalizovat dobu tohoto přepojování, protože od chvíle, kdy dojde ke zrušení kanálu, až do chvíle vytvoření kanálu nového neexistuje komunikační kanál a spojení je přerušeno. Tento výpadek může způsobovat problémy v případě datových přenosů.

Výhodou je jednoduchost realizace, kdy se v kterýkoliv okamžik komunikuje pouze na jediné frekvenci, což zjednodušuje úlohu mobilní stanici, která nemusí zvládat souběžnou komunikaci na více frekvencích. Tento princip se objevil jak u analogových sítí (např. NMT), tak i u sítí digitálních (např. GSM).

Pořadí operací můžeme zaměnit – v tom případě mluvíme o **seamless handover.** Nejprve tedy dojde k vytvoření kanálu nového a až potom dojde ke zrušení stávajícího. Na krátký okamžik je

mobilní stanice spojena se dvěma BTS stanicemi a komunikuje souběžně na dvou kanálech (po dobu mezi vytvořením nového kanálu a zrušením starého). Toto řešení nepřerušuje komunikační kanál, ovšem klade vyšší požadavky na mobilní stanici, která musí zvládat komunikaci na dvou různých frekvencích. Tento princip se uplatňuje zejména v případě řízení handoveru mobilní stanicí. Nalezneme jej tedy např. u systému DECT.

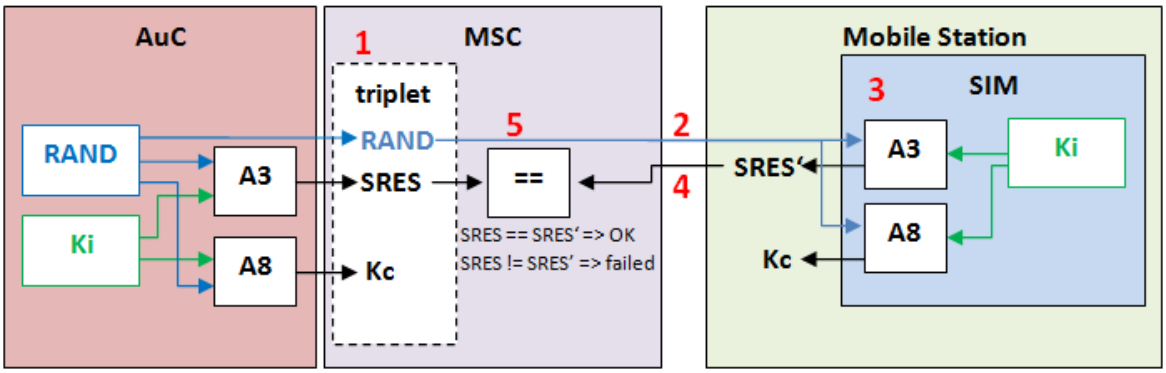
Oba výše zmíněné typy handoverů se aplikují v systémech, kdy je mobilní stanice připojena k jediné BTS stanici a rozlišuje se pouze pořadí, ve kterém se provádějí úkony připojit/odpojit. Existují ale i sítě, kdy je mobilní stanice již z principu systému vždy připojena k nejméně dvěma základnovým stanicím. V tomto případě mluvíme o tzv. **soft handoveru** (měkkém handoveru). Jak se mobilní stanice pohybuje, dochází k průběžnému připojování a odpojování k BTS stanicím. Spojení není nikdy přerušeno (vždy existuje spojení na některou další stanici), realizace rádiového spoje je však poměrně složitá. Příkladem může být systém UMTS.

5.4 Autentizace v GSM síti

Úspěšná autentizace je hlavní podmínkou úspěšného přihlášení do GSM sítě. Další důležitou podmínkou je, že se IMEI číslo mobilní stanice nenachází na *black* či *gray* listu EIR databáze.

V prvním kroku autentizačního procesu pošle ústředna (MSC) autentizačnímu centru IMSI číslo uživatele, který se snaží přihlásit do GSM sítě. Na jeho základě vygeneruje AuC autentizační hodnoty, tzv. ***triplet***. Jedná se o trojici hodnot – *RAND, SRES* a *Kc*. Hodnota *RAND* je náhodně vygenerované 128bitové číslo. Hodnota *SRES* vznikne aplikací algoritmu A3, jehož vstupem jsou hodnoty *RAND* a *Ki*. Poslední hodnotou je šifrovací klíč *Kc*, sloužící k šifrování komunikace pomocí algoritmu A5.

Takto vygenerovaný *triplet* je poslán zpět ústředně, která z něj zašle mobilní stanici pouze hodnotu *RAND*. Mobilní stanice získanou hodnotu předá SIM kartě, kde se na základě této hodnoty, znalosti sdíleného klíče *Ki* a znalosti algoritmu A3, vypočítá odpověď *SRES*. Ta je poslána zpět MSC, které ji porovná s hodnotou získanou od AuC. Pokud se obě hodnoty rovnají, proběhla autentizace úspěšně a příslušné BTS stanici (té, která řídí buňku, ve které se uživatel aktuálně nachází) je odeslán šifrovací klíč *Kc*. V opačném případě je spojení ukončeno (viz Obrázek 5.9).



Obrázek 5.9 - Princip autentizace v GSM síti

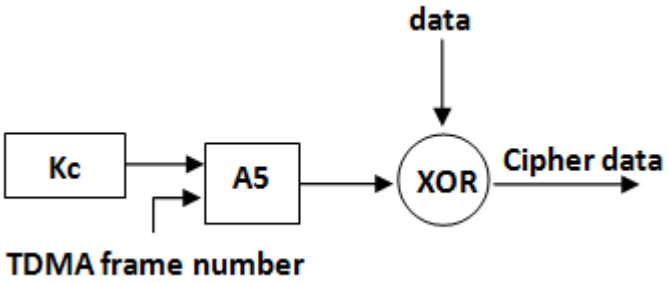
5.5 Šifrování komunikace

Kromě autentizace uživatele je také nutné zajistit zabezpečený přenos dat, tedy jejich **šifrování**. K tomuto účelu existuje v GSM algoritmus A5. Vstupem tohoto algoritmu je šifrovací klíč *Kc* a číslo rámce, ve kterém jsou data přenášena (TDMA frame number). Výstupem algoritmu je hodnota, se

kterou provádíme operaci *xor* nad odesílanými daty, díky čemuž provedeme jejich zašifrování pro přenos. Proces šifrování schematicky popisuje Obrázek 5.10.

Šifrovací klíč *Kc* není pevně stanovenou hodnotou. Naopak, během každého přihlášení uživatele do sítě je generován znovu. K jeho vygenerování se používá algoritmus A8, který jako vstup používá sdílený klíč *Ki* a náhodné číslo *RAND*. Obě tyto hodnoty jsou známy oběma účastníkům komunikace – klíč *Ki* je uložen na SIM kartě a v AuC, hodnota *RAND* je v průběhu procesu autentizace zaslána mobilní stanici (proces autentizace vždy předchází procesu šifrování, bez úspěšné autentizace není možné v GSM síti komunikovat, tudíž by nebylo co šifrovat). Díky tomu je možné vygenerovat šifrovací jak na straně sítě, tak na straně uživatele.

Důležitou vlastností GSM zabezpečení je, že jedinou hodnotou, která se přenáší po síti v otevřené podobě (nešifrovaně), je hodnota *RAND* – tedy náhodně vygenerované číslo. Jakmile dojde k jeho úspěšnému přenesení, je již veškerá komunikace šifrována (během autentizace klíčem *Ki*, během komunikace šifrovacím klíčem *Kc*). Veškeré zabezpečení tedy stojí na utajení společného klíče *Ki*.



Obrázek 5.10 - Princip šifrování komunikace v GSM síti

Podle specifikace GSM sítě existují celkem čtyři varianty A5 algoritmu, které se liší svou silou šifrování (viz Tabulka 5.1). Pokud mobilní stanice neimplementuje alespoň jedenu z variant, A5/1 nebo A5/2, potom jí musí každá GSM síť odmítnout poskytnutí svých služeb (GSM 02.09 Section 3.3.3). Původně bylo povinné implementovat obě tyto varianty a to až do roku 2006, kdy GSMA (GSM Association) prohlásilo variantu A5/2 jako zastaralou.

Varianta A5 algoritmu	Popis
A5/0	Žádná forma šifrování
A5/1	Silná forma šifrování, určeno pro použití v Severní Americe a Evropě
A5/2	Slabá forma šifrování, určeno pro požití v ostatních částech světa
A5/3	Nejsilnější forma šifrování (silnější než A5/1 varianta) s otevřeným dizajnem. Tato varianta není příliš používána.

Tabulka 5.1 - Varianty A5 algoritmu, převzato z [14]

6 Typy GSM kanálů a jejich použití

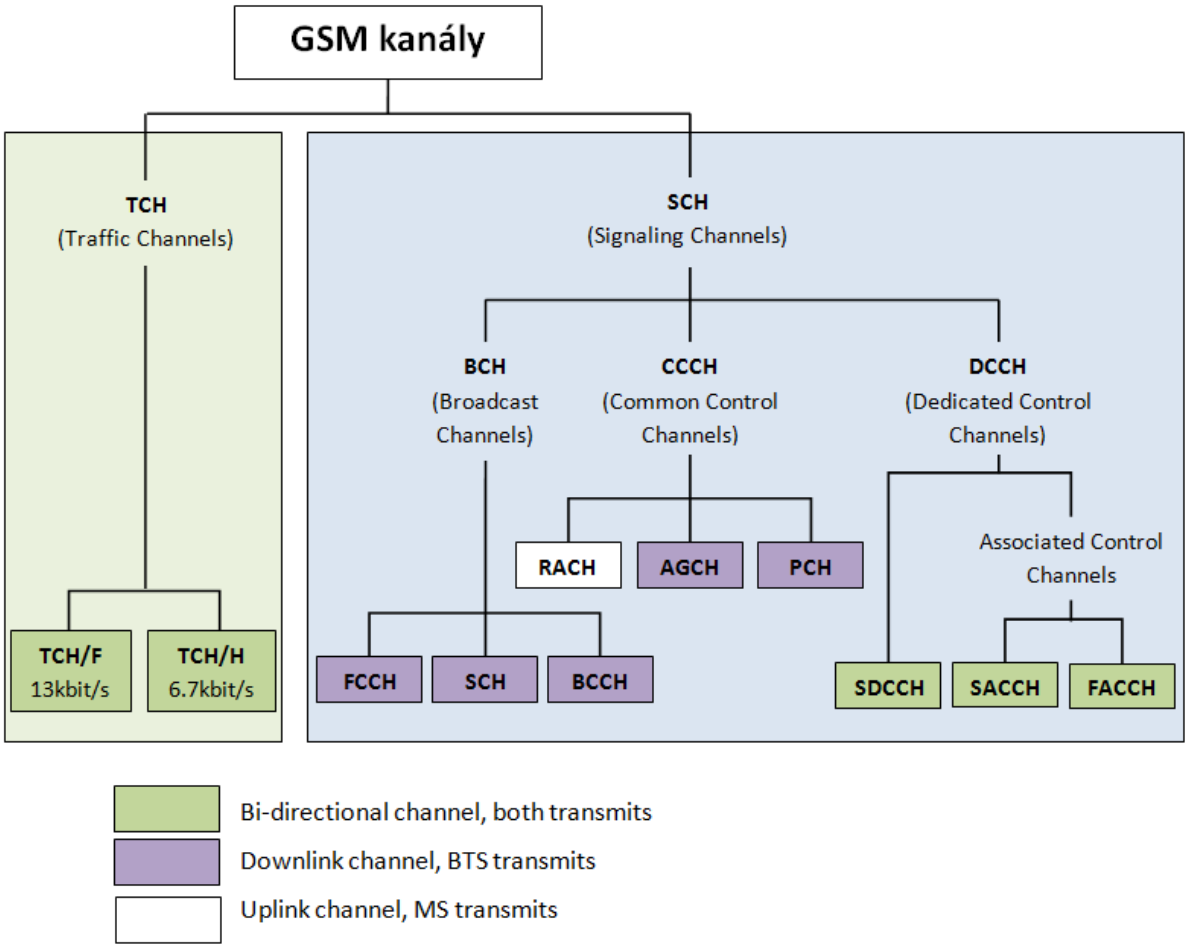
GMS systém využívá několik různých komunikačních kanálů, které se liší nejen svojí šířkou (přenosovou rychlostí), ale i svým určením (viz Obrázek 6.1). Tyto kanály existují pouze mezi mobilní stanicí a BTS stanicí, tedy v radiovém spektru. GSM kanály se podle využiti dělí na dvě skupiny:

1. Traffic Channels (TCH, přepravní kanály)

2. Signaling Channels (SCH, signalizační kanály)

Přenosové kanály (TCH) slouží k přenosu „užitečných dat“, tedy digitalizovaného hlasu v případě telefonního hovoru nebo dat při přenosu datových souborů (při využití připojení k internetu skrze GSM síť). S ohledem na původní účel jsou tyto kanály optimalizovány pro přenos digitalizovaného hlasu za pomoci PCM, proto mají relativně nízkou propustnost. Také nejsou oproti signalizačním kanálům nikterak výrazně členěny, existují pouze dva typy datového kanálu (TCH/F a TCH/H).

Signalizační kanály (SCH) jsou určeny pro přenos signalizace (řízení). Každý kanál má určený specifický význam, často mají svou existenci pevně danou v rámci vysílaného spektra (zejména přístupové kanály – RACH a kanály sloužící k nalezení a synchronizaci mobilní stanice s BTS stanicí).



Obrázek 6.1 - Přehled GSM kanálů

6.1 Traffic Channels (TCH)

Slouží k přenosu hlasu a dat. Existují dvě varianty lišící se svou rychlostí:

1. **Traffic Channel / Fullrate** (TCH/F) – jedná se o rychlejší kanál s rychlostí přenosu přibližně 13 kbit/s.
2. **Traffic Channel / Halfrate** (TCH/H) – rychlost přenosu je poloviční oproti TCH/F, přibližně 6,7 kbit/s.

6.2 Signaling Channels (SCH)

Signalizační kanály slouží k přenosu signalizace a synchronizačních dat. Podle způsobu, jak s daným typem kanálů nakládá mobilní stanice, rozlišujeme tři hlavní kategorie: *common*, *broadcast* a *dedicated*.

6.2.1 Broadcast Channels (BCH)

Kategorie *Broadcast Channels* se vyznačuje tím, že všechny její kanály jsou jednosměrné, mobilní stanice na nich může naslouchat, ale nemůže je použít k vysílání. Jsou dostupné ve stejnou chvíli všem MS a obsahují informace, které nejsou specificky určené pro konkrétní mobilní stanici.

Frequency Correction Channel (FCCH) – slouží k naladění mobilní stanice na správnou frekvenci. Na této frekvenci se vysílají samé logické nuly, což ve svém důsledku vytvoří ve frekvenčním spektru „zub“, na který se mohou MS po prvotním vstupu do dané buňky naladit.

Synchronization Channel (SCH) – slouží k synchronizaci a nastavení MS na správný *timeslot* a na správnou pozici v rámci multiframe. V průběhu času může dojít, stejně tak jako u každé synchronizované komunikace, k vzájemnému posunu mezi MS a BTS. Proto může MS využít tento kanál, který vysílá BTS ke korekcím a tak zabránit rozpadu komunikace.

Broadcast Control Channel (BCCH) - kanál je jednosměrný, propojuje BTS stanici se všemi MS, které aktuálně spadají pod danou BTS. Mezi vysílané informace patří identifikátor buňky (Cell-ID), typ Frequency Hopping, které daná BTS stanice používá, dostupné frekvence v buňce, frekvence sousedních buněk atd.

6.2.2 Common Control Channel (CCCH)

Tyto kanály může použít kterýkoliv účastník, nejsou dedikované pouze jedinému z nich. Z tohoto důvodu je nutné tyto kanály využívat co nejméně a po co nejkratší možnou dobu (kvůli problémům s vícenásobným přístupem k médiu). Proto tyto kanály slouží pouze k sestavení spojení, ve kterém až poté probíhá samotné předávání požadavků (např. pro odchozí hovor je za pomoci RACH/AGCH kanálů nejdříve zaslán jednoduchý požadavek na sestavení spojení a až v takto vytvořeném spojení je zaslán požadavek na samotné vytvoření hovoru. I když tedy nemá účastník právo hovor uskutečnit, je tato skutečnost ověřována až po sestavení spojení, aby nedocházelo k blokaci CCCH kanálů). Jedná se o jednosměrné kanály, s pevně určeným směrem komunikace (BTS komunikuje směrem k MS nebo naopak).

Paging Channel (PCH) – slouží pro vyvolávání MS (např. během příchozího hovoru je pomocí tohoto kanálu MS informováno o této skutečnosti). Na tomto kanálu naslouchají všechna MS, díky čemuž je zajištěna informovanost v celém dosahu signálu. PCH je logicky formován jako společný pro všechny BTS stanice, které leží ve stejné lokační oblasti (jedná se nejmenší oblast, ve které

Random Access Channel (RACH) slouží pro zaslání požadavku mobilní stanice BTS stanici s požadavkem na přiřazení signalizačního kanálu. Tento kanál je společný pro všechny mobilní stanice, které spadají do dané buňky. Aby se co nejvíce minimalizovala možnost kolize (kdy se o komunikaci ve stejnou chvíli pokouší více než jedna MS), slouží RACH kanál pouze k jednoduchému oznámení, že mobilní stanice „něco chce“. Veškerá další komunikace se odehrává až následně, na dedikovaném kanálu, který síť pro potřeby MS vyčlení.

Access Grand Channel (AGCH) používá BTS stanice k zaslání zprávy, která potvrdí přiřazení signalizačního kanálu. Obsahuje také informace, které MS potřebuje ke správnému přepnutí na komunikační kanál (nejčastěji se jedná o SDCCH kanál).

6.2.3 Dedicated Control Channel (DCCH)

Kanály v této kategorii jsou obousměrné (slouží jak pro upload, tak i pro download) a jsou dedikovány vždy jedinému účastníkovi (jediné MS).

Slow Associated Control Channel (SACCH) – každých TCH má přiřazený jeden SACCH kanál. Ten je velmi pomalý a slouží jako signalizace během hovoru. Mezi přenášená data, která posílá základnová stanice mobilní stanici, patří časový předstih, s kterým má MS začít vysílat, aby se trefila do svého timeslotu (Timing Advance) a síla vysílaného signálu (souvisí s aktuální vzdáleností od aktuálně používané BTS, mění se s pohybem MS). Naopak MS zasílá BSC (skrze BTS) informace o naměřených hodnotách z okolních BTS stanic. Tyto informace slouží pro rozhodnutí o provedení handoveru.

Fast Associated Control Channel (FACCH) se používá v případě, že je rychlost SACCH kanálu nedostatečná. FACCH kanál používá timesloty běžného TCH a slouží např. k provedení operace handover.

Stand-Alone Dedicated Control Channel (SDCCH) představuje hlavní signalizační kanál v GSM sítích. Slouží k sestavování hovoru, Location Area Update akci, přenesení SMS zprávy v případě, že uživatel netelefonuje (nemá přidělen TCH, jinak je přenesena za pomoci SACCH). Pokud další činnost MS vyžaduje přidělení TCH (např. v případě telefonního hovoru), musí být SDCCH kanál uvolněn současně s přidělením TCH kanálu.

7 Signalizace

Signalizace slouží k řízení a údržbě datových kanálů.

Signalizaci můžeme rozdělit na tři kategorie:

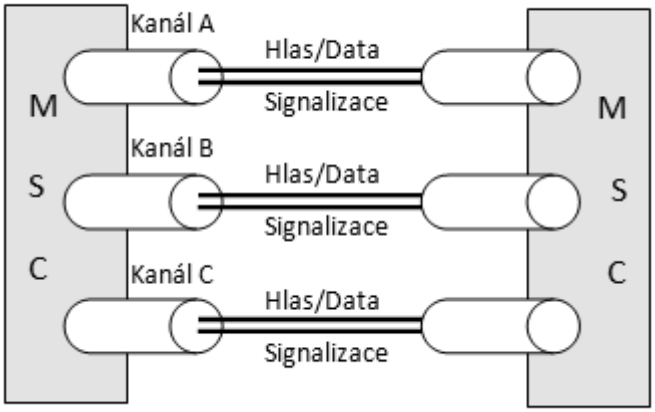
1. Mezi účastníky a ústřednami (přístupová síť)
2. Uvnitř ústředen
3. Mezi ústřednami (páteřní síť)

Existují dva přístupy ve vedení signalizace. Rozdíl mezi těmito dvěma přístupy je popsán dále:

1. Channel Associated Signaling (CAS)
2. Common Channel Signaling (CCS)

7.1 Channel Associated Signaling (CAS)

Signalizace putuje po hovorových nebo přidružených kanálech. Značnou nevýhodou je, že pro každý hovorový kanál musí existovat jeden signalizační kanál (viz Obrázek 7.1). To vede ke značnému plýtvání. Tento přístup byl používán zejména dříve a v dnešní době se od něj ustupuje (vede ke zbytečnému plýtvání prostředky, které by jinak mohli být využity pro „užitečná data“).



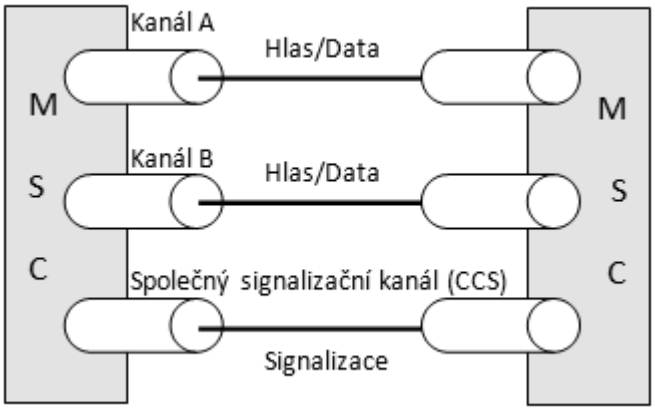
Obrázek 7.1 - CAS signalizace

7.2 Common Channel Signaling (CCS)

CCS je digitální typ signalizace, který přenášená signalizační data ukládá do podoby *timeslotů* nebo kanálu oddělených od hovorových kanálů. Tento způsob umožňuje spojit signalizaci různých kanálů do jednoho společného kanálu (viz Obrázek 7.2) a pro přenos použít síť oddělenou od přenosové sítě užívané pro hlas.

Funkci společného signalizační kanálu může zastávat libovolný kanál v PCM, původně se však k tomuto účelu používá *timeslot* 16. V podstatě dochází ke sdružování signalizačních kanálů do jednoho, kdy signalizace pro více hovorových kanálů vede pouze jediným (jeden kanál dokáže obhospodařovat až 1000 hovorů).

Mezi výhody CCS přístupu patří již zmíněná úspora signalizačních kanálů, kdy takto ušetřené kanály mohou být použity pro přenos hlasu (tím se navýší dostupná kapacita). Mezi další výhody patří možnost přenášet signalizaci jinudy, než kudy vede hlas, a také možnost přenosu i informace, která se netýká datových kanálů (doplňkové služby atd.).

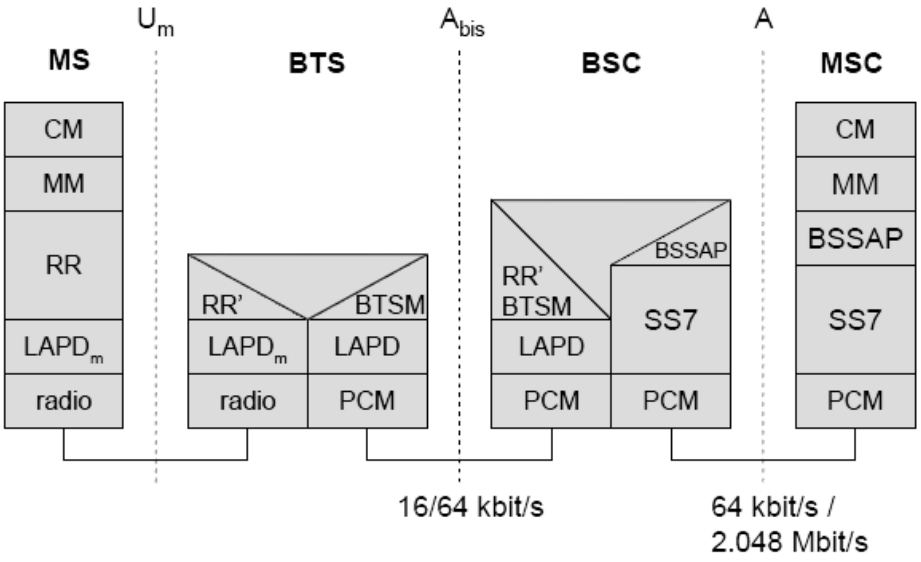


Obrázek 7.2 - Signalizace CCS

8 Signalizace v přístupové síti

V přístupové části GSM sítě existuje několik různých signalizačních rozhraní (viz Obrázek 8.1):

- **Um rozhraní** – mezi mobilní stanicí (MS) a základnovou stanicí (BTS)
- **Abis** – mezi základnovými stanicemi (BTS) a jejich kontroléry (BSC)
- **A** – mezi ústřednami (MSC) a kontroléry (BSC)



Obrázek 8.1 - Architektura protokolů pro signalizaci GSM, převzato z [3]

8.1 U_m rozhraní

U_m rozhraní je přístupové rozhraní, které používá GSM standart pro propojení Mobilní Stanice (MS) a základové stanice (BTS). Jeho název je odvozen jako analogie k U rozhraní, které existuje v ISDN (zde písmeno m reprezentuje mobile). U_m je definováno pouze na prvních třech vrstvách ISO/OSI modelu (fyzické, spojové a síťové) a jeho specifikaci nalezneme GSM 04.xx a 05.xx specifikacích.

Fyzická vrstva (vrstva1)
Protože Um rozhraní spojuje mobilní stanice (MS) se základovými stanicemi (BTS), je fyzickým médiem pro přenos vzduch. Fyzická vrstva definuje tři podvrstvy, které se starají o jednotlivé aspekty bezdrátového přenosu:

- Radiomodem – stará se o řízení a nastavování rádiového rozhraní
- Multiplex a časování – GSM používá TDMA (Time Division Multiple Access)
- Kódování – stará se o dodržení kódovacího schématu přenášených dat

Spojová vrstva (vrstva 2)
Na spojové vrstvě je použit protokol $LDAP_m$. Jeho název je odvozen do protokolu Link Access Procedure pro signalizační D-kanál v ISDN. Stejně jako v případě názvu Um, i zde písmeno m indikuje, že se jedná o mobilní verzi (LDAP mobile).

Síťová vrstva (vrstva 3)

Síťová vrstva U_m rozhraní je definována v GSM 04.07 a 04.08 specifikacích a má tři podvrstvy. Pro úspěšné navázání komunikace musí terminál vytvořit spojení v každé podvrstvě předtím, než může přistoupit k další vyšší vrstvě.

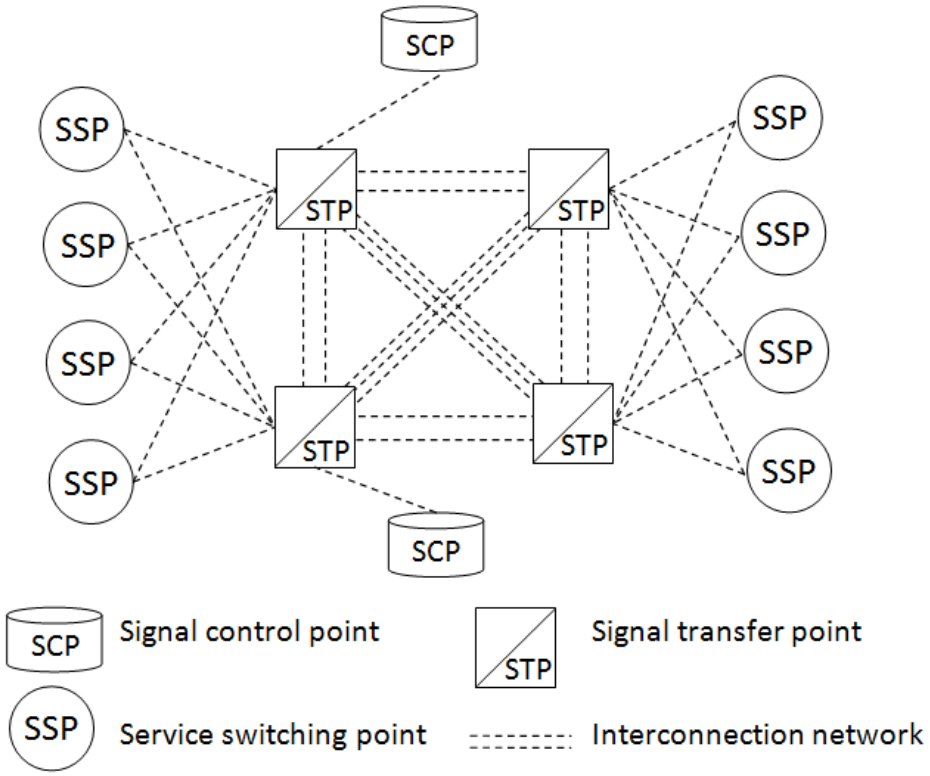
- **Radio Resource Management** (RR) – řídí využití rádiových kanálů, poskytuje spolehlivou službu pro přenos dat pro vyšší vrstvy. Běžně bývá ukončen na BSC.
- **Mobility Management** (MM) – obsahuje funkce pro registraci účastníka, jeho autentizaci, identifikaci zařízení, aktualizaci aktuálního umístění MS (location update), správu TMSI… Běžně bývá ukončen v HLR nebo VLR databázi.
- **Call Management** (CM) – obsahuje funkce pro vrstvy Call Control (CC), Short Message Service (SMS) a Supplementary Service (SS). SMS využívá řídící kanály SDCCH a SACCH v době, kdy jsou volná (není nutné přenášet jiná signalizační data). Běžně bývá ukončen v MSC.

9 Protokoly v tradiční SS7

Signaling System 7 (SS7) síť je paketově přepínaná síť (oddělená od sítě přenášející hlas), která je použita výhradně pro účely propojení telefonních hovorů. SS7 poskytuje dva typy služby: *circuit-related* a *non-circuit-related*. Circuit-related signalizace je použita pro založení a ukončení hlasových spojení v obou používaných sítích, jak v TDM (time division multiplexing) tak i v paketově přepínaných sítích (voice-over-IP). *Non-circuit-related* služby zajišťují všechny ostatní služby poskytované sítí, jako je přístup k databázi pro překlad a informací o odběrateli a správu sítě. [4]

Všechny uzly v SS7 síti jsou nazývány jako **signaling points**. Každý signalizační bod má schopnost *diskriminaci zprávy* (přečíst její cílovou adresu a rozhodnout se, zda je zpráva určena pro něj) a přeposlat zprávu k jinému signalizačnímu bodu. Každý SP má přiřazenou unikátní adresu nazývanou **point code.** Existují tři různé typy signalizačních bodů (SP, viz Obrázek 9.1):

- Service Switching Point (SSP)
- Signal Transfer Point (STP)
- Service Control Point (SCP)



Obrázek 9.1 - Struktura SS7 sítě, převzato z[4]

Service Switching Point (SSP) představují místní ústředny, které zajišťují propojení signalizační sítě SS7 s hlasovou přenosovou sítí. SPP může být realizováno jako kombinace hlasové ústředny a signalizační ústředny (pro přenos SS7 zpráv) nebo jako pomocný počítač připojený k hlasové ústředně. Tento přístup umožňuje telefonním společnostem provést vylepšení jejich stávající signalizační sítě (signalizačních bodů) bez nutnosti výměny drahých ústředen.

Všechny SS7 pakety, které procházejí skrze SS7 síť, jsou přenášeny za pomoci STP uzlů (**Signal Transfer Point**). STP obvykle nejsou cílem ani zdrojem SS7 zpráv, zajišťují jenom jejich přenos

(slouží jakou routery v SS7 síti). Proto na nich neoperují vyšší vrstvy (jako např. ISUP nebo TCAP), nacházejí se zde pouze vrstvy zajišťující přenos (MTP v případě klasické SS7 sítě, TCP/IP + SIGTRAN v případě IP sítích).

K zajištění redundance a různorodosti sítě jsou STP uzly vždy nasazeny ve dvojicích. Pokud by došlo k selhání jednoho STP uzlu, druhý převezme veškerý provoz. V běžném provozu pracují oba uzly a rozdělují si tak zátěž mezi sebe. [4]

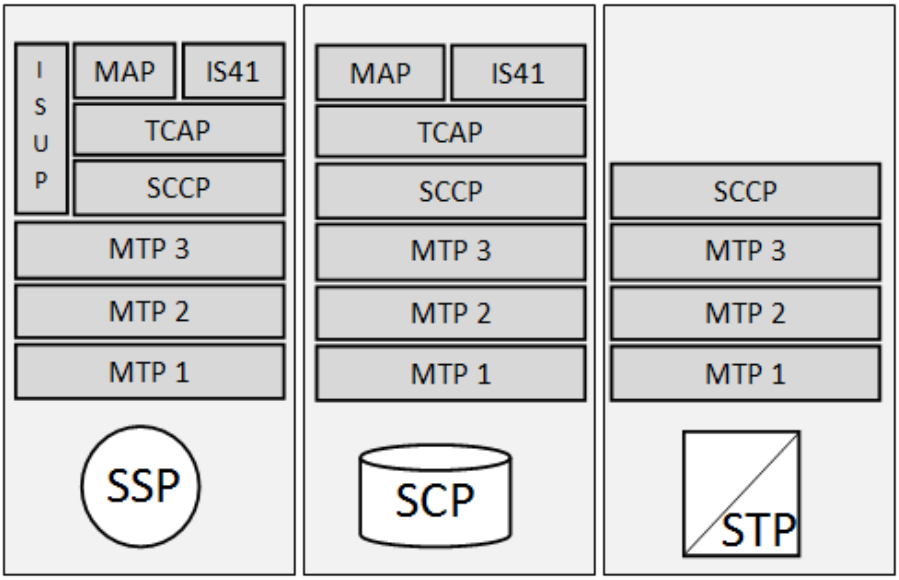
V případě rozlehlých sítí je požita hierarchická struktura STP uzlů, skládající se ze třech úrovní:

1. Národní STP (National STP)
2. Mezinárodní STP (International STP)
3. Gateway STP

Service Control Point (SCP) slouží jako přístupové rozhraní k databázím telefonní společnosti.

Obrázek 9.2 ukazuje protokoly, které operují na jednotlivých typech SP jednotek. Všechny typy SP podporují přenosovou část SS7 signalizace (MTP protokoly) a navíc i SCCP protokol. Pro jednotky typu STP je tento set protokolů dostačující, protože pouze zajišťuje přenos signalizace mezi ostatními typy jednotek, nezabývá se jejich zpracováním.

Oproti tomu se SCP a SSP typy jednotek již zabývají i zpracováním SS7 zpráv, proto musejí rozumět protokolům vyšších vrstev. Sety protokolu obou jednotek se liší pouze v podpoře protokolu ISUP jednotkami typu SSP.



Obrázek 9.2 - Protokoly operující na daných typech SP

9.1 Adresování v SS7

Každá signalizační jednotka (SP) má přiřazenou adresu nazývanou **Signaling Point Code** (SPC). Jedná se o 14-ti bitovou hodnotu, která je v rámci dané SS7 sítě unikátní a slouží k identifikaci (adresaci) dané SP jednotky. Velikost SPC hodnoty tvoří limit pro velikost SS7 sítě, kdy maximální počet SP v jedné SS7 je omezen na 16384.

Kromě SPC kódu se používá i dvoubitová hodnota nazývaná jako **Network Identifier** (NI). Ta vyčleňuje čtyři různé kategorie SS7 sítí, které se liší jak podle svého rozsahu (národní/mezinárodní), tak podle svého využití (viz Tabulka 9.1).

Označení	Název	Popis
NAT0	National 0	Tato síť je tvořena pouze jediným operátorem v rámci země (každý operátor formuje svou vlastní). Je tvořena až cca 16 tisíci ústřednami.
NAT1	National 1	V každé zemi by měla existovat jedna síť typu NAT1. Skládá se z ústředen typu *Gateway STP* všech operátorů v dané zemi. Díky této síti je možné přistupovat do sítí jednotlivých operátorů.
INAT0	International 0	Jedná se o mezinárodní síť, která se skládá z mezinárodních ústředen všech operátorů. Jejich čísla a adresy jsou určeny mezinárodními organizacemi.
INAT1	International 1	Síť tohoto typu se používá pouze zřídka a slouží zejména jako záloha.

Tabulka 9.1 - Kategorie SS7 sítí vyčleněné pomocí NI čísla

9.2 Hierarchie protokolů SS7

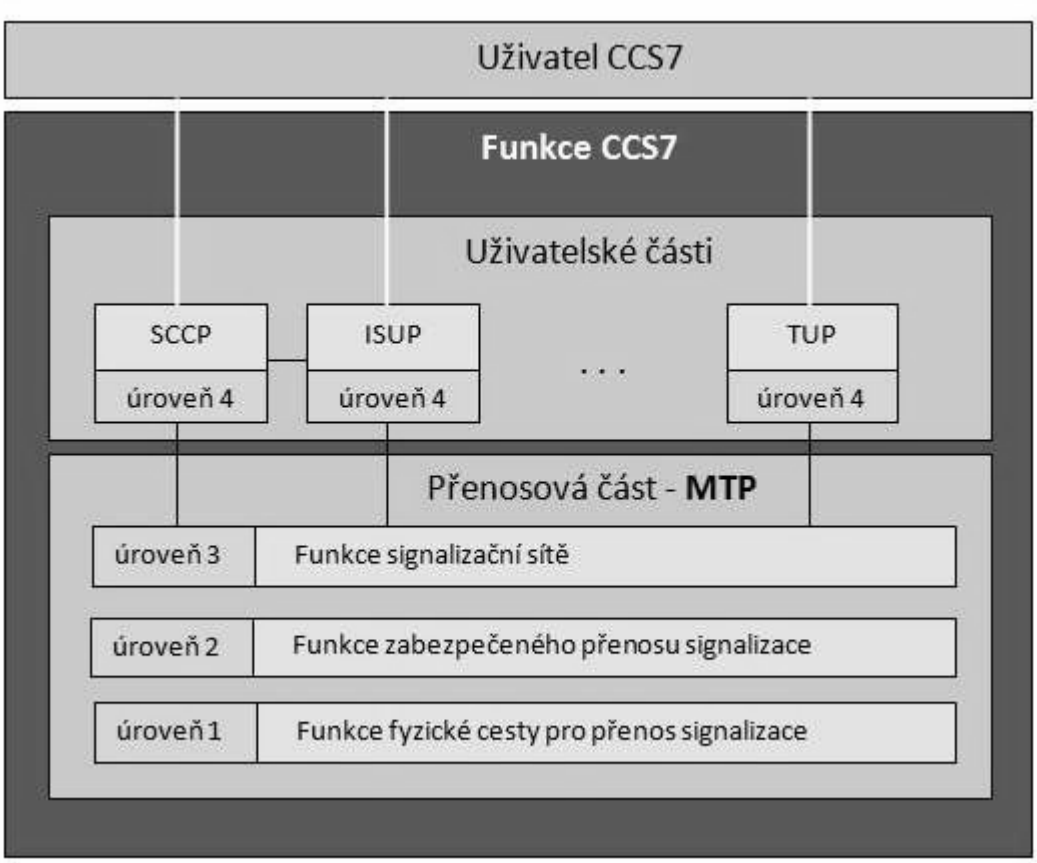
Protokoly SS7 signalizace se dělí na dvě skupiny (viz Obrázek 9.3) – **přenosovou část**, která je společná pro všechny SS7 protokoly a **uživatelkou část**, která zajišťuje požadovanou funkcionalitu.

Přenosová část – zajišťuje bezpečný přenos informace a řízení signalizační sítě

- **MTP 1**
- **MTP 2**
- **MTP 3**

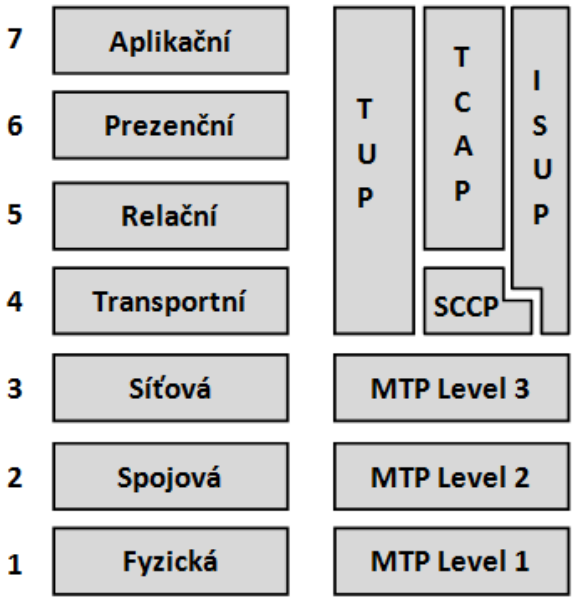
Uživatelská část má modulární povahu, což umožňuje do budoucna přidávat nové protokoly uživatelské části.

- **Transaction Capabilities Application Part** (TCAP)
- **Telephone user Part** (TUP)
- **ISDN User Part** (ISUP)
- **Signaling Connection Control Part** (SCCP)



Obrázek 9.3 - Logické celky CCS7, převzato z [15]

Obrázek 9.4 ukazuje SS7 protokoly v porovnání s modelem ISO/OSI. Přenosová část (MTP protokoly) přesně odpovídá protokolům první až třetí vrstvy. Protokoly vyšších vrstev se ale již překrývají.



Obrázek 9.4 - SS7 signalizace versus ISO/OSI model

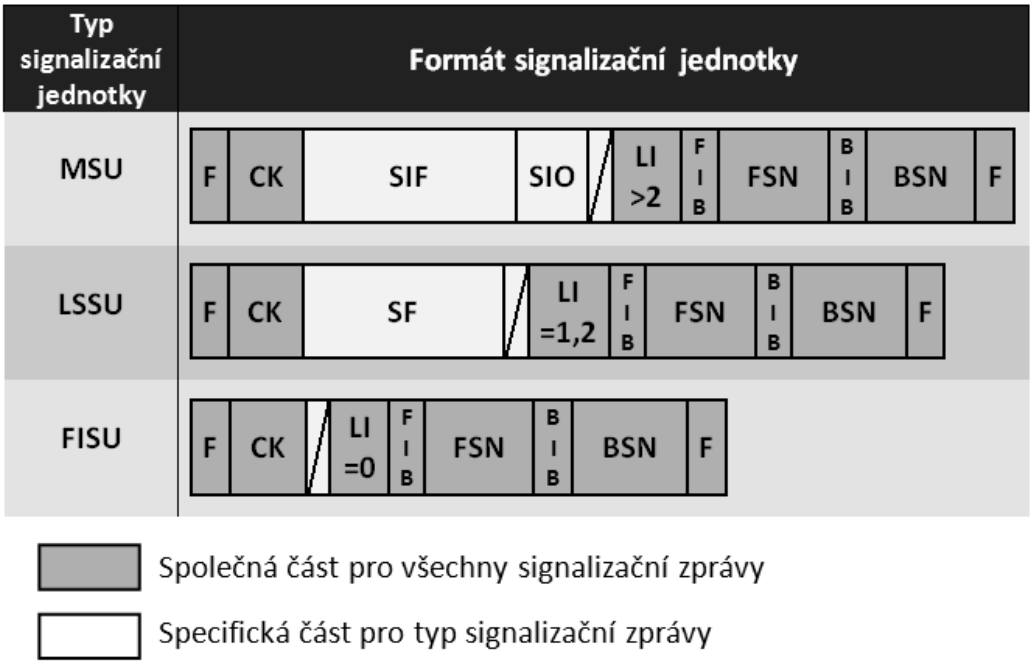
9.3 Message Transfer Part (MTP)

Protokoly rodiny MTP zajišťují přenos SS7 uživatelských protokolů skrze SS7 síť. Skládá se ze tří podvrstev:

1. Fyzickou vrstvu ISO/OSI modelu představuje **MTP 1**. Slouží pro přenos po signalizačním spoji.
2. Funkci spojové vrstvy zajišťuje **MTP 2**. Stará se o sestavení přenášeného rámce, detekci chyb a sledování dostupnosti signalizačního kanálu.
3. Poslední podvrstva **MTP 3** odpovídá síťové vrstvě a zajišťuje řízení signalizační sítě a manipulaci se zprávou (směrování zpráv, rozpoznání zpráv a distribuci zpráv). Každá entita v SS7 síti má jedinečnou adresu – **Signaling Point Code** (SPC), podle které se provádí směrování.

MTP protokol se skládá ze tří signalizačních jednotek (SU – Signaling Unit):

1. **Message Signaling Unit** (MSU) – vytvářena ve druhé vrstvě uživatelských zpráv řízení sítě třetí vrstvy
2. **Link Status Signaling Unit** (LSSU) – informace týkající se řízení signalizačního vedení, pouze mezi druhou úrovní dvou sousedních bodů (vedení není připraveno pro přenos MSU, vedení již nemůže být použito pro přenos MSU)
3. **Fill-In Signaling Unit** (FISU) – slouží pro detekci přenosových chyb během přenosu MSU



Obrázek 9.5 - formát signalizačních jednotek, převzato z [15], přepracováno

Obrázek 9.5 ukazuje formát jednotlivých signalizačních jednotek (zpráv). Většina polí je ve všech třech typech zpráv stejná, jejich význam je následující:

- **Flag** (F, návěstí) – statická bitová sekvence, která označuje začátek a konec rámce. Hodnota tohoto pole je vždy rovna hodnotě *0111 1110* (bitově).
- **Check Bits** (CK, kontrolní bity) – kontrolní součet pro detekci chyby při přenosu.

- **Length Indicator** (LI, indikátor délky, viz Tabulka 9.2) – slouží k rozlišení jednotlivých typů signalizačních jednotek (SU).

Hodnota	Význam
0	**FISU** - výplňová signalizační jednotka
1 nebo 2	**LSSU** - signalizační jednotka stavu spojů
Větší než 2	**MSU** - signalizační jednotka zprávy

Tabulka 9.2 - Možné hodnoty pole Length Indicator (LI)

- **Forward Indicator Bit** (FIB) – slouží pro opravu chyb, indikuje, zda byla SU poslána poprvé nebo se jedná již o opakovaný přenos.
- **Forward Sequence Number** (FSN) – tato sekvence provádí číslování signalizační jednotky (tato hodnota je oříznuta funkcí modulo 128).
- **Backward Indicator Bit** (BIB) – slouží pro opravu chyb, reprezentuje požadavek pro znovuzaslání SU.
- **Backward Sequence Number** (BSN) – slouží k potvrzování úspěšně přijatých SU.

Signalizační jednotka zprávy (MSU) obsahuje navíc pole **Signaling Information Filed** (SIF, Signalizační informační pole), které nese vlastní uživatelskou zprávu (maximálně 272 bytů dlouhou) a pole **Service Information Octet** (SIO, oktet služební informace), který slouží k identifikaci uživatelské části SS7 signalizace, které přenášená zpráva patří (obdoba čísla portu v TCP/IP).

Signalizační jednotka stavu spoje (LSSU) navíc obsahuje pole **Status Field** (SF), které slouží k přenesení informace o stavu pro synchronizaci.

9.4 Telephone User Part (TUP)

Protokol Telephone User Part poskytuje konvenční PSTN síti (Public Switched Telephone Network) telefonní služby napříč SS7 sítí. TUP byl prvním protokolem čtvrté vrstvy, které standardizační organizace definovali, a proto jako takový neposkytuje žádnou podporu pro ISDN služby. Dnes nahrazen ISUP protokolem. Stále se ale v některých částech světa používá (např. v Číně). Převzato z [16].

9.5 Transaction Capabilities Application Part (TCAP)

TCAP slouží k přenosu INAP zpráv v inteligentních sítích a MAP zpráv v mobilních sítích. Protokol TCAP existuje ve dvou verzích:

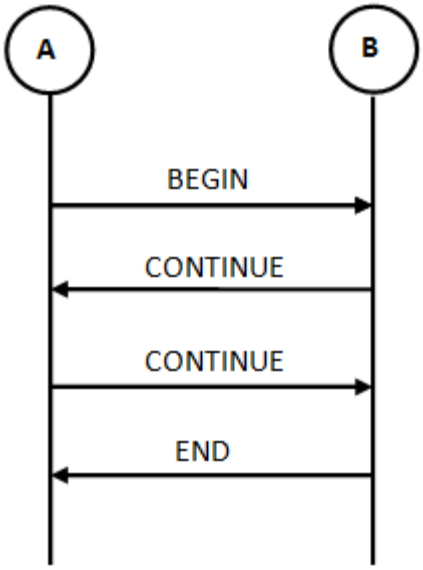
1. **ITU TCAP** (představen v Q.700 series) – jedná se o mezinárodní verzi protokolu
2. **ANSI TCAP** (představen v ANSI T1.114) – jedná se o verzi protokolu, která je používána v USA

ITU TCAP definuje pět zpráv, které slouží k vyjednání transakcí – jejich založení, ukončení, zrušení a pro přenos informací, pro které není nutné zakládat transakci. Tabulka 9.3 shrnuje a popisuje tyto zprávy (v příloze 3 jsou uvedeny typy zpráv pro ANSI i ITU verzi protokolu).

Typ ITU-TCAP zprávy	Její význam
Unidirectional	Slouží pro odeslání komponenty jinému uživateli TCAP, aniž by bylo nutné založit transakci (díky tomu nedochází k přidělení transakčního ID). Není očekávána žádná odpověď na přijetí této zprávy.
Begin	Zakládá transakci. Dojde k přidělení transakčního ID, které je obsaženo ve všech zprávách, které souvisí s aktuální transakcí. TCAP uživatel může na přijetí této zprávy odpovědět buď zprávou *End* nebo zprávou *Continue*.
Continue	Tato zpráva je zaslaná, pokud byla úspěšně založena transakce a je nutné ji použít k budoucí výměně informací. Je vytvořeno transaction ID, které dále slouží pro identifikaci přidružených zpráv této transakci (je součástí hlavičky každé zprávy). Kromě tohoto identifikátoru obsahují zprávy typu *Continue* i transaction ID přijaté od zprávy *Begin* – tedy obsahuje jak Origination Transaction ID, tak i Destination Transaction ID. TCAP uživatel může po přijetí této zprávy odpovědět buď zprávou *End* nebo *Continue*.
End	Ukončuje existující transakci. Okamžitě po přijetí této zprávy dojde k uvolnění Transaction ID.
Abort	Tato zpráva indikuje, že došlo k nepředvídatelné abnormální události, která ve svém důsledku znemožňuje další použití transakce – musí tedy dojít k ukončení transakce (spolu s tím i uvolnění všech přidělených transakčních identifikátorů). Takovéto násilné ukončení transakce může nastat v důsledku požadavku TCAP uživatele (typ *U-Abort*) nebo z požadavku protokolu samotného (*P-Abort*).

Tabulka 9.3 - ITU-TAP zprávy

Obrázek 9.6 ukazuje příklad komunikace za pomoci protokolu ITU-ISUP. První zprávou, kterou posílá zakladatel komunikace (tedy ten, který chce komunikovat), je zpráva *BEGIN*. Nyní záleží na druhé straně, zda s komunikací souhlasí (zpráva *CONTINUE*) nebo zda odmítne navázat spojení (zpráva *END*). V našem případě si druhá strana přeje komunikovat, proto zasílá zprávu *CONTINUE*. Od této chvíle dochází k výměně dat (nyní si komunikující strany zasílají zprávy *CONTINUE*, aby vyjádřili souhlas s pokračováním v komunikaci). Pro ukončení slouží zpráva *END*, která ukončí transakci a tím i celou komunikaci. Jedná se o poslední zasílanou zprávu, po níž již nenásleduje žádná další, která by patřila do této transakce.



Obrázek 9.6 - Příklad komunikace protokolem ITU-ISUP

9.6 ISDN User Part (ISUP)

Základní úlohou ISUP protokolu je založení a uvolnění hovorů. Protokol definuje velké množství postupů a zpráv, mnoho z nich je určeno pro doplňkové služby a údržbu. Ač standart definuje téměř padesát zpráv, jádro ISUP protokolu je tvořeno množinou pěti či šesti zpráv (ty tvoří většinu zpráv, které se běžně vyskytují na SS7 sítích).

Obrázek 9.4 ukazuje, že ISUP protokol je propojen jak s SCCP protokolem, tak i přímo s MTP3 protokolem. Služby druhého zmíněného využívá jako přenosovou službu pro výměnu síťových zpráv, jako např. vytvoření hovoru nebo zrušení hovoru. Pro přenos signalizace typu end-to-end je možné použit služeb SCCP, přesto však v dnešní době používá ISUP protokol přímo MTP3. Zprávy ISUP protokolu jsou obecně přenášeny za pomoci Message Signaling Unit (MSU) zprávy.

Základní hovor je rozdělen do tří fází:

1. **Založení hovoru** (set-up fáze)
2. **Konverzace** (případně přenos dat)
3. **Ukončení hovoru** (release fáze)

ISUP signalizace se váže hlavně na první a poslední fázi (v případě doplňkových služeb se ISUP signalizace zapojuje i do druhé fáze). Obrázek 9.7 ukazuje, jak probíhá vytvoření základního hovoru (v tomto případě se opravdu jedná pouze o základní hovor, neboť se v něm nevyužívá žádná z doplňkových služeb).

9.6.1 Call Setup (založení hovoru)

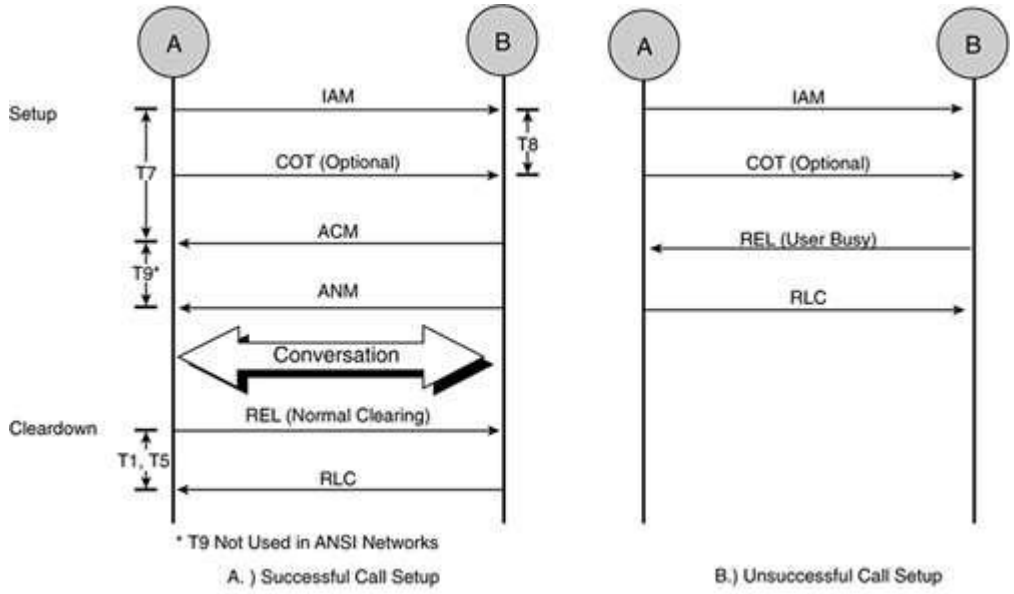
Obrázek 9.7 ukazuje schéma založení telefonního hovoru za pomoci ISUP protokolu. V části A (Successful Call Setup) je popsáno úspěšné založení telefonního hovoru. Kromě toho případu může dojít i ke stavu, kdy hovor nemůže být založen (volaná strana není dostupná, potřebná linka pro hovor

je nedostupná…), proto musí existovat mechanizmus, který volající stranu o této skutečnosti informuje. Tento mechanizmus je zachycen v části B (Unsuccessful Call Setup).

Základní telefonní hovor může být založen a uvolněn pouze za pomoci pěti ISUP zpráv. První zaslanou zprávou je **Initial Address Message** (IAM), která upozorňuje na pokus o sestavení hovoru pro určitý okruh. IAM zpráva obsahuje informace, které jsou nezbytné pro sestavení hovorového spojení, jako např. typ hovoru, číslo volané strany či informace o nosném okruhu. Reakce na přijetí IAM zprávy je odeslání **Address Complete Message** (ACM). Tato zpráva říká, že hovor pro danou oblast (kam hovor směřuje) může být uskutečněn - existuje linka pro spojení a je volná pro použití. Další zpráva, která byla odeslána je volitelná **Continuity Message** (COT), která slouží pro průběžné testování hlasové cesty před tím, než je kontaktován uživatel.

Jakmile je odeslána zpráva **ACM**, je na volaném zařízení spuštěno zvukové vyzvánění a informační tón je odeslán zpět volajícímu. Jakmile volaný příjme hovor, je zaslána zpráva **Answer Message** (ANM) zpět volanému. Hovor je nyní založen a dochází k výměně hovorových zpráv s hlasem [10].

Obrázek 9.7 ve své druhé části (b. Unsuccessful Call Setup) ukazuje **neúspěšný pokus o založení hovoru**. Poté, co je přijata zpráva IAM, zkontroluje B stav cílové linky a zjistí, že je obsazená. Proto namísto odeslání zprávy ACM, je poslána zpráva REL, která obsahuje důvod odmítnutí spojení User Busy hodnotu. Tato zpráva říká, že nemůže dojít k úspěšnému sestavení hovoru [10].



Obrázek 9.7 - Schéma zaslání signalizačních zpráv pro hovor, převzato z [10]

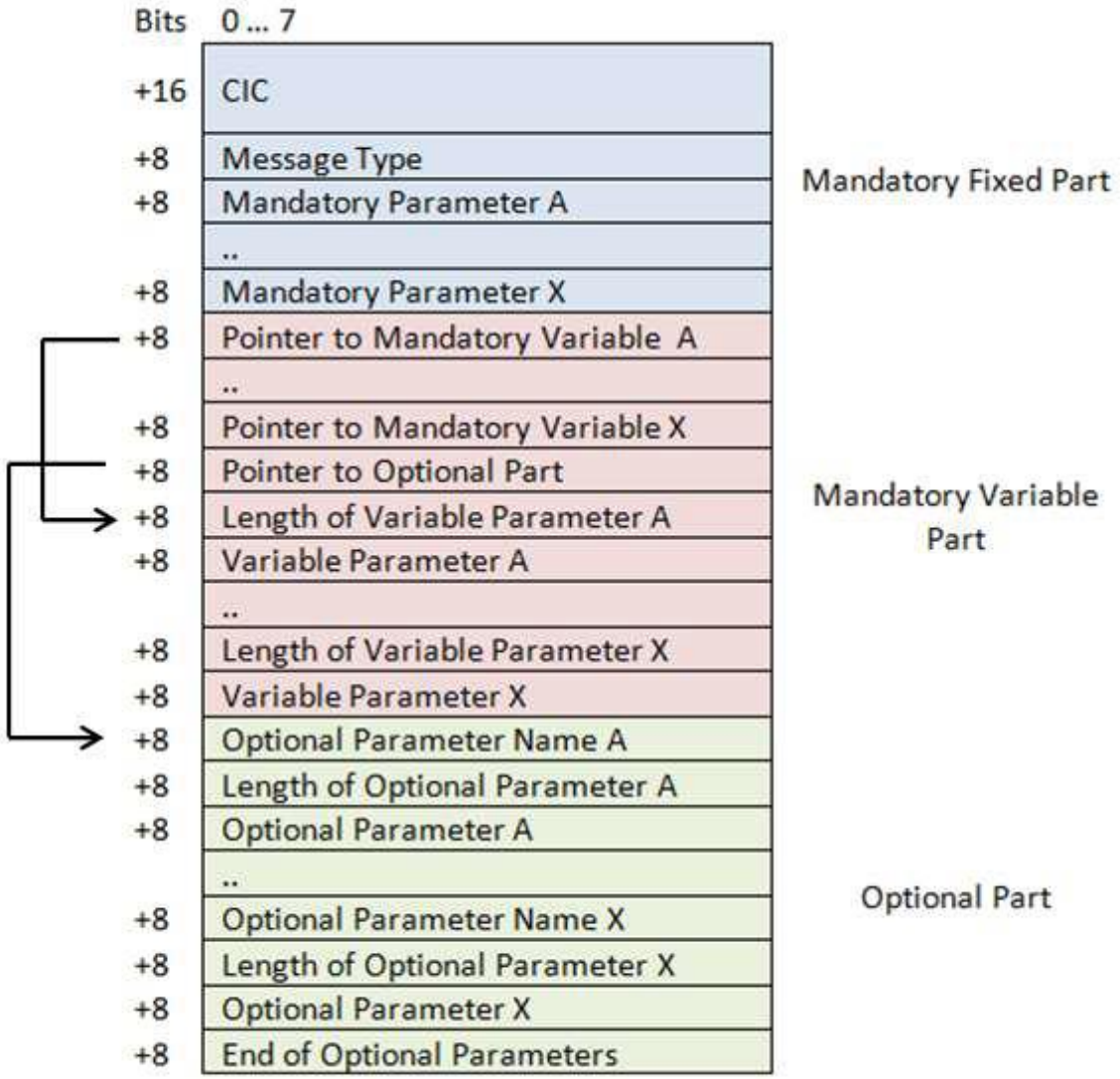
9.6.2 Call Release (ukončení hovoru)

Pokud existuje hovor, musí byt nějakým způsobem možné jej ukončit. K tomuto slouží **Release Message** (REL), kterou zašle zařízení, které se rozhodlo hovor ukončit, své protistraně. Tato zpráva způsobí uvolnění nosného kanálu. Protistrana na tuto zprávu odpoví **Release Complete Message** (RLC), kterou svou protistranu informuje o přijetí REL zprávy a říká tak, že došlo k uvolnění okruhu [10].

9.6.3 Struktura rámce

Struktura ISUP rámce je velmi flexibilní a umožňuje tak konstrukci nových ISUP zpráv (viz Obrázek 9.8). Každý typ zprávy definuje **povinné parametry**, které jsou nezbytné ke konstrukci zprávy. Tyto parametry neobsahují identifikátor své délky, protože ISUP standart definuje, že mají pevnou délku (bez výjimky). Protože ne všechny parametry mohou mít pevnou délku, a protože neobsahují identifikátor své délky, slouží k jejich přístupu ukazatele pevné velikosti. Tyto ukazatele odkazují na začátky každého proměnného parametru (ke každému ukazateli je přiřazena jedna proměnná). Hodnota ukazatele je v podstatě počet oktetů, které leží mezi ukazatelem a začátkem proměnné, na kterou odkazuje.

Kromě povinných parametrů, může každá zpráva obsahovat i **volitelné pole**. K tomuto poli se přistupuje za pomoci posledního ukazatele z povinné části, který odkazuje na volitelnou část. Toto pole slouží k přenosu dodatečných informací pro již definované zprávy. Pokud operátor začne nabízet novou doplňkovou službu, je možné k její realizaci využít toto pole – např. *Calling Party Number* je jedním z volitelných polí IAM zprávy, ale je obvykle přenášena, protože slouží k realizaci doplňkových služeb jako je číslo volajícího (Caller ID).



Obrázek 9.8 - Schéma obecné struktury rámce ISUP protokolu

Informace k této kapitole byly čerpány (a některé části převzaty) z [10].

9.7 BSS Application Part (BSSAP)

Tento protokol se používá pro komunikaci mezi MSC a BSC. Dělí se na dvě části:

1. **Base Station Subsystem Management Application Part** (BSSMAP) – podporuje všechny procedury mezi MSC a BSS, které vyžadují interpretaci a zpracování nesených informací i mimo svůj cíl a také pro spravování zdrojů.
2. **Direct Transfer Application Part** (DTAP) – tento protokol slouží k přenosu signalizace pro řízení hovorů a řízení mobility mezi MSC a MS. Zprávy DTAP protokolu nejsou interpretovány BSS subsystémem, slouží pouze pro přenos mezi zdrojem a cílem.

10 Mobile Application Part (MAP)

MAP protokol je rozšířením rodiny protokolů SS7/C7 o podporu buňkových sítí. Definuje operace, které probíhají mezi MSC, HLR,VLR, EIR a mezi pevnými telefonními sítěmi.

Nicméně MAP protokol existuje ve dvou verzích, které se liší jak v použitých typech zasílaných zpráv, tak i poskytovaných službách. To znemožňuje jejich vzájemnou spolupráci.

1. **GSM-MAP** – podporuje pouze GSM, jedná se o mezinárodní standard.
2. **ANSI-MAP** – kromě GSM poskytuje podporu i pro AMPS, NAMPS, D-AMPS/TDMA, CDMA (jak pro dma One, tak pro dma 2000), jedná se o standard požívaný Spojenými státy.

Map protokol se liší oproti ostatním signalizačním protokolům rodiny SS7 v tom, že se nejedná o bitový protokol ale textový.

MAP signalizace umožňuje realizovat operace pro aktualizaci polohy (LU), handover, roaming, autentizaci, směrovací příchozího hovoru a SMS. Map specifikuje množinu služeb a informační tok mezi jednotlivými GSM komponentami, aby byly tyto služby implementovány.

Pro přenos MAP signalizačních zpráv je použit protokol TCAP, přenášeny skrze SCCP a následně MTP vrstvy. V případě SIGTRAN signalizace je možné využít služeb TCAP, který je přenášen buď protokolem SUA, nebo dvojicí protokolů SCCP/M3UA nebo trojicí SCCP/MTP3/M2PA.

10.1 Struktura rámce

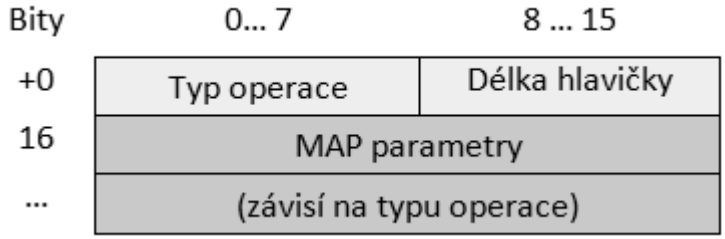
Struktura MAP rámce je velmi jednoduchá, skládá se ze tří částí (viz Obrázek 10.1):

1. Identifikátor typu operace
2. Celková délka hlavičky
3. Vlastní přenášená data

MAP protokol definuje několik desítek různých operací, které se týkají řízení mobility, vyřizování hovorů, provozu a údržby atd. Pro identifikaci typu MAP operace, která je aktuálně v rámci přenášena, slouží **identifikátoru typu operace.** Jedná se o 8bitové pole, umístěné v prvním oktetu rámce.

I když máme jednotný formát rámce pro všechny operace, je samozřejmé, že každá z nich vyžaduje své specifické hodnoty, které je nutné přenést. Proto je (jako i v jiných protokolech) důležitou součástí přenášených informací i **délka hlavičky**. Podle této hodnoty je možné rozeznat, jak velkou datovou část sebou zpráva nese.

Ve třetí části rámce jsou přenášeny samotné **parametry MAP operace**. Počet parametrů je závislý na typu přenášené operace, v rámci jedné zprávy mohou být přeneseny až 4 parametry.



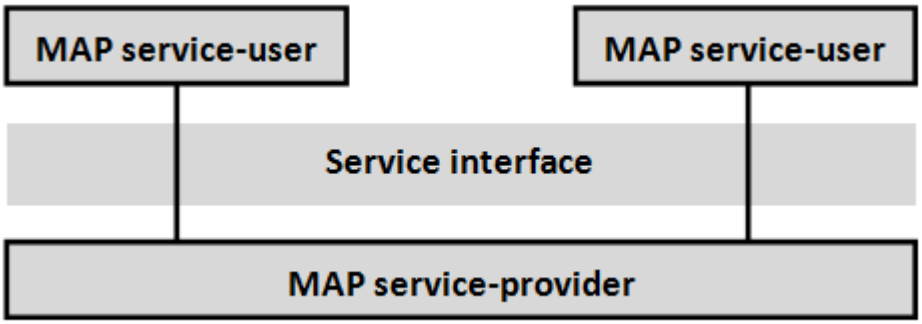
Obrázek 10.1 - Obecná struktura MAP hlavičky

10.2 MAP služby

Funkcionalita MAP protokolu je jeho uživatelům poskytována skrze specifikované sady služeb. Uživatele jej tak mohou chápat jako „černou skříňku“ (*black box*) nebo abstraktní stroj, který reprezentuje poskytovatele MAP služby. Obrázek 10.2 zachycuje tento pohled.

V komunikaci za pomoci MAP protokolu vystupují dvě entity – *MAP service-user* (uživatel služby) a *MAP service-provider* (poskytovatel služby).

Uživatelé služby interagují s *poskytovatelem služby* za pomoci zasílání nebo přijímání MAP primitiv skrze rozhraní služby. Uživatel služby může přijímat služby z několika instancí poskytovatele služby ve stejnou dobu. V tomto případě leží nutnost provádět časovou synchronizaci na uživateli služby. [17]



Obrázek 10.2 - Model komunikace MAP protokolem

Každá MAP služba je tvořena několika primitivy, které jsou zasílány mezi komunikujícími uzly – uživatelem služby a poskytovatelem služby. Primitiva jsou pojmenovány pomocí *MAP_Service_Primitive_Name type* konvence, kde *type* může být jednou z následujících čtyř hodnot:

1. *Request* (req)
2. *Indication* (ind)
3. *Response* (rsp)
4. *Confirm* (cnf)

Služby MAP protokolu se dělí do tří skupin:

1. *Confirmed-service* – jedná se o skupinu služeb, které jsou potvrzovány poskytovatelem služby.
2. *Unconfirmed-service* – skupina služeb, které nejsou potvrzovány poskytovatelem služby.
3. *Provider-initiated-service*

Každé použití služeb MAP protokolu vyžaduje založení tzv. ***MAP dialogu*.** Ten je definován jako výměna informací mezi dvěma MAP uživateli za účelem vykonat nějakou činnost. *Dialog* se může skládat jak z jediné služby, tak i z několika odlišných služeb.

MAP protokol definuje velké množství parametrů, které mohou být obsaženy v primitivech. Tabulka 10.1 shrnuje použité zkratky, které jsou použity pro indikaci požadavků kladených na daný parametr, a jejich význam.

Zkratka	Význam
M	Povinný (mandatory). Kategorie povinný parametr může být použita na jakýkoliv typ primitiva a znamená, že daný parametr musí být přítomen v daném primitivu.
O	Volitelný (optional). Používá se pouze pro primitiva typu *indication* a *confirm* a slouží pro označení parametrů, které mohou být dodatečně zaslány poskytovatelem služby.
U	Možnost uživatele služby (service-user option). Používá se pouze pro primitiva typu *request* a *response*. Zahrnutí tohoto parametru do zprávy je volbou uživatele služby.
C	Přítomnost parametrů této kategorie ve zprávách jsou podmíněná (conditional). Používají se k vyjádření několika skutečností, které ovlivňují přítomnost parametrů ve zprávě: 1. Uživatel služby musí sám rozhodnout, zda parametr použít nebo ne, a to na základě kontextu, ve kterém je služba použita. 2. Jeden z několika vzájemně se vylučujících parametrů musí být přítomen (např. parametry, které indikují pozitivní výsledek oproti parametrům, které naopak indikují negativní výsledek). 3. Parametr typu *User Optional* (značen jako typ *U*) nebo parametr typu *Conditional* (značen jako typ *C*), který zaslal v primitivech typu *request* a *response* uživatelem služby, má být zaslán uživateli v odpovídajících primitivech typu *indication* a *confirm*. 4. Pokud je parametr přijat od nějaké jiné entity, musí být zahrnut v úvahu pro danou službu.
Prázdné	Parametr není ve zprávě přítomen
(=)	Hodnota parametru je stejná jako v předchozí zprávě, která jej v popisu předchází (nachází se hned vlevo).

Tabulka 10.1 – Seznam použitých zkratek pro výskyt parametrů v MAP procedurách

Operace poskytované MAP protokolem můžeme rozdělit do několika hlavních kategorií:

1. **Common MAP services** [4]
2. **Mobility Management** (Řízení mobility)
3. **Operation and Maintenance** (Provoz a údržba)
4. **Call Handling** (Vyřizování hovorů)
5. **Supplementary Services** (Doplňkové služby)
6. **Short Message Service** (SMS služba)

10.2.1 Common MAP services

Do této kategorie spadají služby MAP protokolu, které jsou určeny pro součinnost se službami z ostatních kategorií. Jejich význam spočívá v operabilitě s TCAP či SCCP protokoly, kde každá služba koresponduje s některou funkcí z řízených protokolů.

Služba	Význam
MAP_OPEN	Procedura sloužící k založení *MAP dialogu* mezi dvěma uživateli MAP služby.
MAP_CLOSE	Procedura sloužící k uzavření *MAP dialogu.*
MAP_DELIMITER	Procedura sloužící k explicitnímu zadání požadavku na přenos dat MAP

	protokolu jeho vzdáleným entitám.
MAP_U_ABORT	Procedura sloužící k „násilnému“ přerušení aktivního *MAP dialogu*. Iniciátorem je **MAP uživatel služby**.
MAP_P_ABORT	Procedura sloužící k „násilnému“ přerušení aktivního *MAP dialogu*. Iniciátorem je **MAP poskytovatel služby**.
MAP_NOTICE	Tato služba slouží k informování MAP uživatele služby o vzniku problémů, vztahujících se k aktuálnímu *MAP dialogu*, které ale neovlivňují stav MAP poskytovatele služby.

Tabulka 10.2 - MAP služby *Common* kategorie

10.2.2 Mobility Management

Služby z kategorie **Mobility Management** (řízení mobility) zajišťují podporu pro mobilitu uživatelů (Mobile Station).

Služby **Location Management** (správy umístění) slouží ke správě aktuální lokace uživatele. Aby se minimalizovala zátěž HLR databáze, probíhá komunikace, týkající se změn pozice uživatele, pouze mezi VLR databází (a příslušnou MSC), ke kterému je uživatel aktuálně připojen. Komunikace s HLR databází probíhá jen v případě, že uživatel změní svou příslušnost k nové VLR databázi. Tímto způsobem je napříč GSM síti uložena informace o aktuální poloze uživatele – HLR databáze uchovává aktuální příslušnost uživatele k VLR databázi a MSC, ty pak uchovávají konkrétní údaje o pozici uživatele.

Služby kategorie **Paging and Search** (vyvolávání a hledání) používá GSM síť k broadcastovému vysílání v celé servisní oblasti, aby tak nalezla hledanou mobilní stanici. To je nutné v případě, kdy vznikne potřeba komunikovat s mobilní stanicí (např. příchozí hovor), ale její poloha je neznámá (nelze ji zjistit z HLR/VLR registrů).

Služby kategorie **Access Management** (řízení přístupu) se zabývají zajištěním ověřením, zda daný uživatel má mít povolený přístup k prostředkům sítě

Služby kategorie **handover** zajišťují provedení handoveru mezi dvěma MSC ústřednami. Jedná se o tzv. inter-MSC handover (viz kapitola 5.3.1).

Pro ověření identity uživatele sítě slouží služby kategorie **Authentication Management** (správa ověřování).

Kategorie **Security Management** (správa bezpečnosti) obsahuje jedinou službu, která slouží ke konfiguraci a zahájení šifrování komunikace skrze rádiové rozhraní.

Kategorie **IMEI Management** (Správa IMEI) slouží síti k získání IMEI čísla od MS (v případě, že jej ještě nezná) a následně umožňuje provést kontrolu, do kterého seznamu IMEI spadá – zda v black, grey nebo white (viz kapitola 4.5).

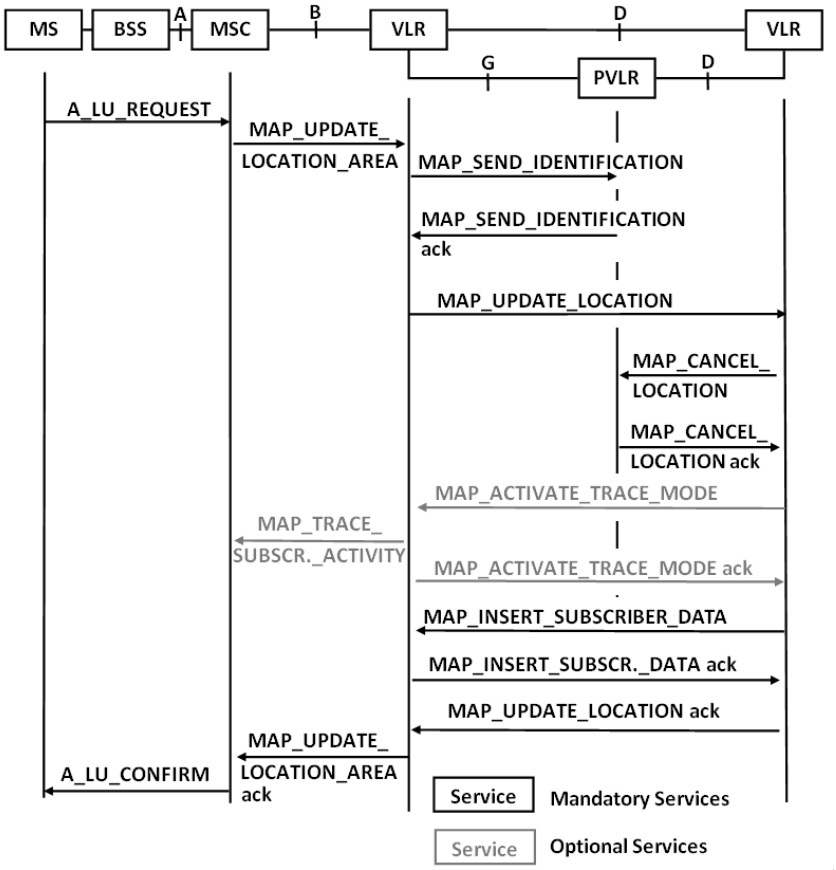
Služby z kategorie **Subscriber Management** (správa účastníků) využívá HLR databáze, aby v případě, že se uživatelovi údaje změní (např. pokud uživatel aktivuje novou doplňkovou službu), mohla provést změnu uživatelských údajů uložených ve VLR databázi.

Kategorie služeb **Identity Management** (správa identit) zprostředkovává funkcionalitu pro zadání požadavku na získání uživatelovi identity ze MSC ústředny.

Kategorie **Fault Recovery** (zotavení po chybě) zajišťuje, že uživatelská data, uložena ve VLR databázi, jsou v konzistentním stavu s uživatelskými daty, která jsou uložena v HLR databázi. K tomuto stavu může dojít při selhání HLR databáze nebo některé z VLR databází. Potom je jedním z klíčových kroků zajistit konzistenci informací uložených v databázích napříč celou GSM sítí a k tomu se používají služby *Fault Recovery*.

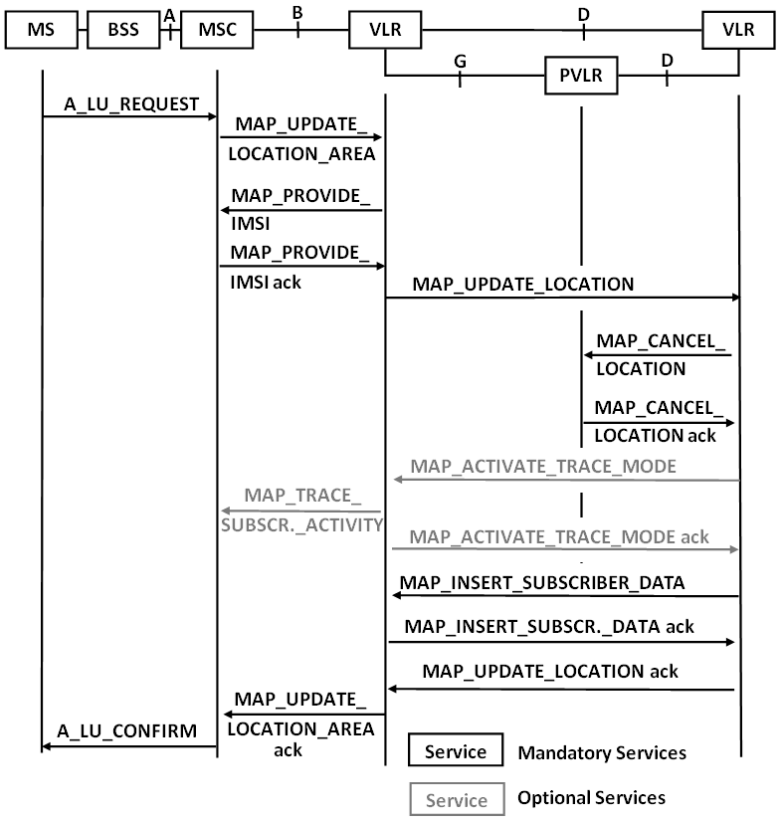
Pro získání informací o uživateli sítě, jako je například jeho status (zda je dostupný nebo není) nebo jeho aktuální lokační oblast, slouží služby kategorie **Subscriber Information** (informace o uživateli). [4]

Obrázek 10.3 popisuje princip *Location Update* operace s popisem zasílaných primitiv. V tomto případě je identifikátor IMSI poskytnut starou VLR databází (aktuální VLR databází, ke které je MS připojen, ale od které se pokouší odpojit, v diagramu zachycena jako PVLR).



Obrázek 10.3 - Location Update procedura, převzato z [17]

Obrázek 10.4 popisuje princip *Location Update* operace s popisem zasílaných primitiv. Oproti předcházejícímu případu PVLR databáze nezná překlad zaslaného TMSI čísla MS na jeho IMSI číslo. Proto jej musí VLR získat přímo od MS (skrze MSC).



Obrázek 10.4 - Location Update procedura, IMSI nebylo poskytnuto starou VLR, převzato z [17]

10.2.3 Operation and Maintenance

Tato kategorie se dělí na dvě skupiny:

1. Subscriber Tracing (Sledování zařízení), která obsahuje služby pro sledování zařízení v rámci GSM sítě.
2. Miscellaneous (Různé), do které patří jediná služba – *sendIMSI*, která slouží k zaslání uživatelského *IMSI* čísla (subscriber IMSI).

10.2.4 Call Handling

Primárním úkolem procesů této skupiny je získat směrovací informace, které umožní úspěšně realizovat příchozí hovory (terminating calls).

10.2.5 Supplementary Services

Služby této kategorie poskytují podporu pro doplňkové služby, jako například call forwarding.

10.2.6 Short Message Service

Tato kategorie poskytuje služby pro výměnu znakových zpráv až do velikosti 160 znaků s ostatními uživateli GSM sítě. Kromě uživatelských zpráv může služeb SMS využít i samotná síť – až již pro broadcast či zasílání cílených zpráv. Pomocí této techniky může síť uživateli poskytnout užitečné informace (jako např. instrukce pro nastavení služby nebo může přenášet i jiná než znaková data – např. logo nebo vyzváněcí tón).

10.3 Sekvence MAP dialogu

Každý *MAP dialog* se skládá z několika sekvencí, které slouží k jeho vytvoření a správě (viz Obrázek 10.5):

1. Opening sekvence slouží k založení *MAP dialogu*.
2. Continuing sekvence slouží
3. Closing sekvence slouží k ukončení *MAP dialogu*.
4. Aborting sekvence slouží k „násilnému“ ukončení *MAP dialogu*.

Sekvence ***opening*** otevírá *MAP dialog*. Musí být provedena před tím, než mohou být zaslána jakákoliv jiná uživatelská primitiva. Začátek sekvence je indikován zasláním primitiva *MAP_OPEN* a konec *MAP_CLOSE*. Součástí této sekvence mohou být i uživatelská primitiva:

1. Pokud mezi primitivy *MAP_OPEN* a *MAP_DELIMITER* nejsou žádná uživatelská primitiva, způsobí to přeložení prázdné *BEGIN* zprávy v TC.
2. V případě více uživatelských primitiv, jsou všechna zaslána v jediné *BEGIN* zprávě.

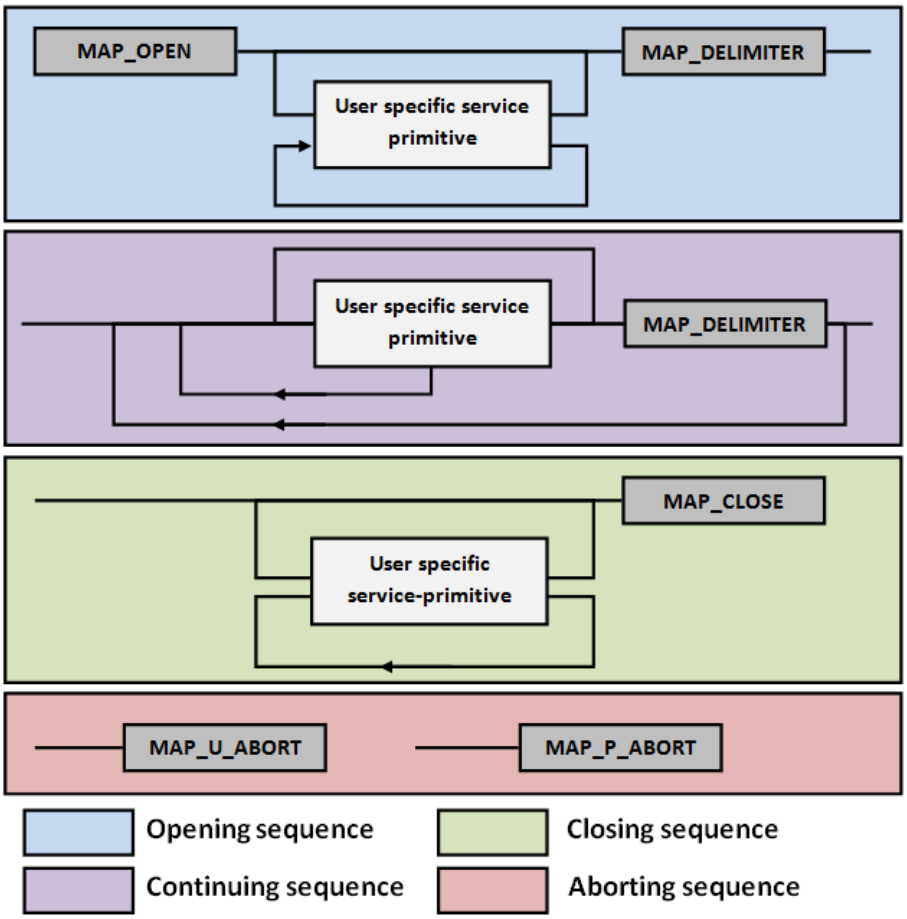
Sekvence ***continuing*** nemusí být ve všech *MAP dialozích* obsažená (je nepovinná). Pokud je přítomna, je ukončena *MAP_DELIMITER* primitivem. Pokud je posíláno více uživatelsky specifických primitiv (všechny ostatní mimo kategorie *common*), jsou zaslány všechny ve stejné *Continue* zprávě.

Sekvence ***closing*** může nastat pouze, pokud jí předcházela *opening* nebo *continuing* sekvence. Stejně jako v případě *opening* sekvence může být současně posláno i několik uživatelských primitiv (v případě normálního ukončení):

1. Pokud nejsou posílána žádná uživatelská primitiva, dojde k překladu na prázdnou *END* zprávu v TC.
2. Pokud se posílá více uživatelských primitiv, jsou poslána ve stejné *END* zprávě.
3. Pokud je indikován typ ukončení jako *prearranged end*, potom sekvence nesmí obsahovat žádné uživatelské primitiva.

Sekvence ***aborting*** slouží k „násilnému“ ukončení *MAP dialogu*. Tato sekvence se vyskytuje ve dvou variantách, lišící se použitým primitivem:

1. *MAP_U_ABORT* – uživatel MAP služby může tuto sekvenci vyvolat kdykoliv po té, co byl *MAP dialog* založen nebo jako reakci na pokus o otevření *MAP dialogu*.
2. *MAP_P_ABORT* – poskytovatel MAP služby může tuto sekvenci vyvolat kdykoliv, pokud existuje *MAP dialog*.



Obrázek 10.5 - Schematické znázornění sekvencí *MAP dialogu*

10.4 Vybrané MAP služby

Na některé důležité služby, které jsou pro téma této práce důležité, se nyní podíváme podrobněji.

10.4.1 MAP_OPEN service

Tato služba slouží k založení MAP *dialogu* mezi dvěma uživateli služby. Tato služba je potvrzovaná (patří do kategorie *confirmed-service*). Tabulka 10.3 ukazuje primitiva, ze kterých se služba *MAP_OPEN* skládá.

Parameter Name	Request	Indication	Response	Confirm
Application context name	M	M(=)	U	C(=)
Destination address	M	M(=)		
Destination reference	U	C(=)		
Original address	U	O		
Original reference	U	C(=)		
Specific information	U	C(=)	U	C(=)

Responding address	U	C(=)
Result	M	M(=)
Refuse-reason	C	C(=)
Provider error		O

Tabulka 10.3 - Parametry *MAP_OPEN* služby

Tabulka 10.4 shrnuje význam parametrů, které se mohou v průběhu běhu procedury *MAP_OPEN* objevit.

Parametr	Význam
Application context name	Tento parametr určuje typ kontextu, ve kterém byla aplikace založena. • Pokud je *MAP dialog* přijat, potom se musí hodnota tohoto parametru zopakovat. • Pokud je *MAP dialog* odmítnut, potom tento parametr indikuje nejvyšší podporovanou verzi.
Destination address	Tento parametr představuje platnou SCCP adresu, která identifikuje cílovou vzdálenou entitu.
Destination-reference	Tento parametr představuje odkaz, který slouží k zpřesnění identifikace volaného procesu. Může být totožný s *destination address,* ale jeho hodnota je zpracovávána na úrovni MAP protokolu. V příloze 4 je uveden seznam MAP služeb, u kterých je použití tohoto parametru povoleno.
Originating address	Tento parametr představuje platnou SCCP adresu, která identifikuje žadatele *MAP dialogu*.
Originating-reference	Tento parametr představuje odkaz, který slouží ke zpřesnění identifikace volajícího procesu. Může být totožný s *originating address,* ale jeho hodnota je zpracovávána na úrovni MAP protokolu. V příloze 5 je uveden seznam MAP služeb, u kterých je použití tohoto parametru povoleno.
Specific information	Tento parametr slouží k přenosu uživatelem definované zprávy. Jeho použití není definováno GSM standardem. Je určen pro provádění specifických požadavků provozovatele sítě.
Responding address	Adresa, která identifikuje odpovídající entitu. Tento parametr je přítomen pouze v případě, že je to vyžadováno v kontextu dané služby (např. hodnota tohoto parametru je odlišná od hodnoty *destination address*).
Result	Tento parametr udává, zda *MAP dialog* je přijat druhou stranou.
Refuse reason	Tento parametr je přítomen pouze v případě, že parametr *Result* indikuje odmítnutí *MAP dialogu*. Může nabývat jednu z následujících hodnot: • Application-context-not-supported • Invalid-destination-reference • Invalid-originating-reference • No-reason-given • Vzdálený uzel není dosažitelný • Potencionální nekompatibilita verzí

Tabulka 10.4 - Význam parametrů procedury *MAP_OPEN*

10.4.2 MAP_CLOSE service

Tato služba slouží k uvolnění *MAP dialogu*, který byl vytvořen službou *MAP_OPEN*. Jedná se o nepotvrzovanou službu (patří do kategorie *Unconfirmed-service*). Tabulka 10.5 ukazuje primitiva, ze kterých se služba *MAP_CLOSE* skládá.

Parameter Name	Request	Indication
Release method	M	
Specific Information	U	C(=)

Tabulka 10.5 - Parametry *MAP_CLOSE* služby

Tabulka 10.6 shrnuje význam parametrů, které se mohou v průběhu běhu procedury *MAP_CLOSE* objevit.

Parametr	Význam
Release method	Tento parametr může nabývat dvou hodnot: [17] 1. Normal release – v tomto případě dojde k namapování primitiva na protokol a jeho zaslání vzdálené straně. 2. Prearranged end – v tomto případě nedochází k mapování primitiva na protokol. Ukončení *MAP dialogu* je v tomto případě řízeno nezávisle dvěma uživateli, tj. je nutné zaslat pouze primitiva typu *request*.
Specific Information	Tento parametr slouží k přenosu uživatelem definované zprávy. Jeho použití není definováno GSM standardem. Je určen pro provádění specifických požadavků provozovatele sítě.

Tabulka 10.6 - Význam parametrů procedury *MAP_CLOSE*

10.4.3 MAP_DELIMITER service

Tato služba slouží k zadání explicitního požadavku na zaslání dat MAP protokolu vzdáleným entitám. Jedná se o nepotvrzovanou službu skládajících se ze dvou primitiv – *Request* a *Indication*. Obě dvě jsou bez parametrů.

10.4.4 MAP_UPDATE_LOCATION service

Tato služba slouží VLR databázi k aktualizaci údajů o aktuální lokační oblasti uživatele v HLR databázi. K identifikaci uživatele se používá *IMSI* nebo *LMSI* číslo. Tabulka 10.7 ukazuje primitiva, ze kterých se služba *MAP_UPDATE_LOCATION* skládá.

Parameter Name	Request	Indication	Response	Confirm
Invoke ID	M	M(=)	M(=)	M(=)
IMSI	M	M(=)		
MSC address	M	M(=)		
VLR address	M	M(=)		

LMSI	U	C(=)		
Supported CAMEL phases	C	C(=)		
SoLSA support indicator	C	C(=)		
HLR number			C	C(=)
User error			C	C(=)
Provider error				O

Tabulka 10.7 - Parametry procedury *MAP_UPDATE_LOCATION*, převzato z [4]

Tabulka 10.8 popisuje význam parametrů, které se mohou proceduře *MAP_UPDATE_LOCATION* vyskytnout.

Parametr	Význam
Invoke Identification	Tento parametr identifikuje odpovídající primitiva. Tento parametr dodává uživatelem MAP služby a musí být unikátní pro všechny dvojce uživatel služby/ poskytovatel služby. [17]
IMSI	Slouží pro přenos identifikátoru mobilní stanice *IMSI* (viz kapitola 4.1).
LMSI	Slouží k přenosu *LMSI* identifikátoru (viz kapitola 4.6).
MSC Number	Jedná se o ISDN číslo, kterým je identifikována MSC ústředna.
VLR Number	Jedná se o ISDN číslo, které identifikuje VLR databázi.
Provider Error	Tento parametr slouží k indikaci chyby související s protokolem: • Duplikovaná hodnota *invoke identification* • Nepodporovaná služba • Překlep v parametru • Nedostatek zdrojů • Zahájení uvolňování *dialogu* (vzdálená strana již zahájila uvolnění *dialogu*, proto jej nelze dále využívat a musí být uvolněn). • Neočekávaná odpověď od vzdálené strany • Selhání při kompletaci služby • Žádná odpověď od vzdálené strany • Přijata nesprávná odpověď

Tabulka 10.8 - Význam parametrů procedury *MAP_UPDATE_LOCATION*

10.4.5 MAP_UPDATE_LOCATION_AREA service

Tato služba slouží k aktualizaci informací o poloze uživatele sítě uložené ve *VLR* databázi. Iniciátorem služby je vždy uživatel (mobilní stanice), který ji využívá v případě registrace do sítě (mobilní stanice byla vypnutá a zapne se) nebo v případě změny lokační oblasti.

Tato služba se liší od služby *MAP_UPDATE_LOCATION* (viz. kapitola 10.4.3) v tom, že informace pocházejí od mobilního uživatele a jsou určeny pro *VLR* databázi. Oproti tomu *MAP_UPDATE_LOCATION* slouží *VLR* databázi k aktualizaci záznamů uložených v *HLR* databázi. Tabulka 10.9 ukazuje primitiva, ze kterých se služba *MAP_UPDATE_LOCATION_AREA* skládá.

Parameter Name	Request	Indication	Response	Confirm
Invoke ID	M	M(=)	M(=)	M(=)
Target location area ID	M	M(=)		
Serving cell ID	M	M(=)		
Location update type	M	M(=)		
IMSI	C	C(=)		
TMSI	C	C(=)		
Previous location area ID	C	C(=)		
Cksn	C	C(=)		
User error			C	C(=)
Provider error				O

Tabulka 10.9 - Parametry procedury *MAP_UPDATE_LOCATION_AREA*, převzato z [4]

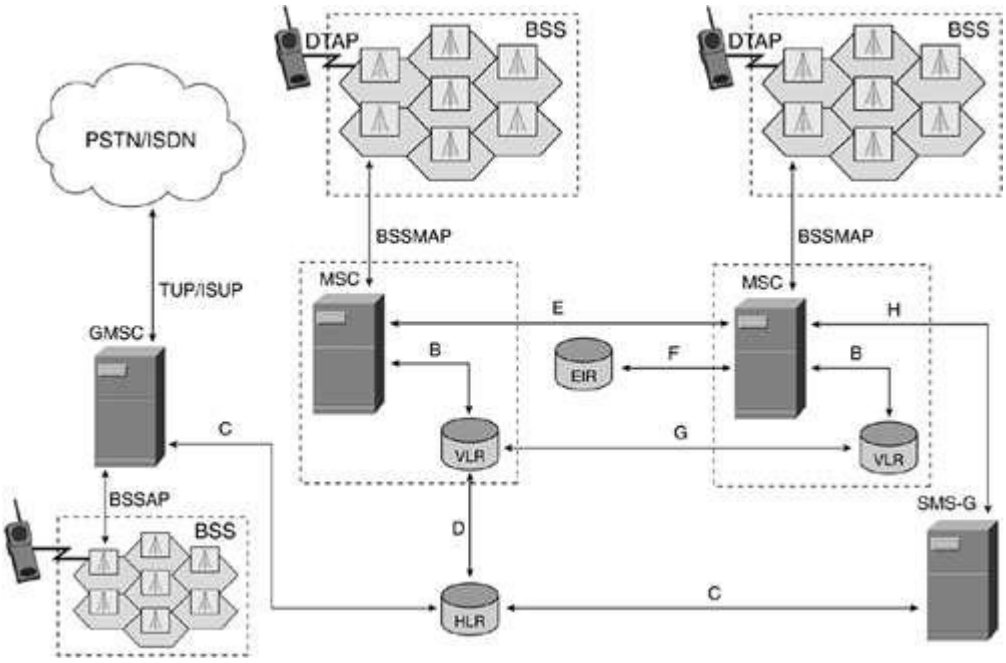
Tabulka 10.10 popisuje význam parametrů, které může procedura *MAP_UPDATE_LOCATION_AREA* obsahovat.

Parametr	Význam
Invoke Identification	Tento parametr identifikuje odpovídající primitiva. Tento parametr dodává uživatelem MAP služby a musí být unikátní pro všechny dvojce uživatel služby/ poskytovatel služby. [17]
Target Location Area Identifier	Jedná se o identifikátor lokační oblasti, ve které se uživatel má v úmyslu pohybovat.
Serving Cell Identifier	Identifikuje buňku, která aktuálně poskytuje uživateli služby (viz kapitola 4.7).
Cksn	Tento parametr se vztahuje k pořadovému číslu šifrovacího klíče.
IMSI	Slouží pro přenos identifikátoru mobilní stanice *IMSI* (viz kapitola 4.1).
TMSI	Přenáší *TMSI* číslo, které slouží k identifikaci uživatele (viz kapitola 4.2).
Location Update Type	Jedná se o parametr, který říká, o který typ operace *location update* se jedná. Celkem se rozlišují tři typy (viz kapitola 12.4): 1. Normal 2. Periodic 3. IMSI attach.
Previous Location Area Identification	Identifikátor předchozí oblasti, ve které se uživatel nacházel.

Tabulka 10.10 - Význam parametrů procedury *MAP_UPDATE_LOCATION_AREA*

10.5 MAP a GSM

Pro komunikaci mezi jednotlivými GSM prvky je použito několik komunikačních rozhraní (viz Obrázek 10.6). Tabulka 10.11 poskytuje bližší popis jednotlivých rozhraní:



Obrázek 10.6 - Rozhraní použité pro komunikaci v páteřní síti GSM, převzato z [10]

Protokol	Mezi	Popis
Um	MS ↔ BSS	Přístup MS do GSM sítě za pomoci bezdrátového spojení. Pro signalizaci se používá LAPDm protokol.
Abis	BSC ↔ BTS BTS↔BTS	BSS interní rozhraní, které slouží ke spojení BSC kontrolérů a BTS stanic. Kromě toho je použito pro komunikaci mezi dvěma BTS stanicemi, které se nacházejí pod společným BSC kontrolorem (převzato [4]). Toto rozhraní není standardizované.
A	BSS ↔ MSC	Propojuje mobilní ústředny s příslušnými BSC kontroléry (a tím i celou přístupovou sítí). Toto rozhraní řídí alokaci vhodných rádiových zdrojů pro uživatele sítě (MS) a zajišťuje jejich správu. Používá BSSAP protokoly (BSSMAP a DTAP).
B	MSC ↔ VLR	Obsluhuje signalizaci mezi MSC a VLR databázemi. Používá MAP/B protokol. Jedná se o logické rozhraní a GSM standart nepožaduje jeho externí implementaci. [4]
C	GMSC ↔ HLR nebo SMSG↔HLR	Slouží pro komunikaci mezi HLR databázemi a GMSC nebo SMSC. Každý hovor, který má původ mimo GSM síť musí jít skrze bránu (gateway), aby získal směrovací informaci, která je nezbytně nutná k úspěšnému provedení hovoru. Pro použití C rozhraní je použit protokol MAP/C.
D	HLR ↔ VLR	Pro komunikaci mezi databázemi HLR a VLR je použito rozhraní D, které používá MAP/D protokol. Slouží pro výměnu informací o pozici mobilní stanice a informací o uživatelských datech.
E	MSC ↔ MSC	Pro propojení ústředen je použito E rozhraní (používá MAP/E protokol). Toto rozhraní slouží pro předávání informací, týkajících se handoveru. E rozhraní může také sloužit pro propojení GMSC a SMSC.
F	MSC ↔ EIR	Toto rozhraní spojuje MSC a EIR. Používá MAPF protokol pro

		ověření stavu IMEI čísla, které MSC získalo od MS.
G	VLR ↔ VLR	Slouží k vzájemnému propojení dvou VLR databází různých MSC. Používá MAP/G protokol pro přenos uživatelských informací – např. během aktualizace polohy MS.
H	MSC ↔ SMSG	Pro přenos signalizace na tomto rozhraní je použit MAP/H protokol, který podporuje přenos SMS zpráv.
I	MSC ↔ MS	Toto rozhraní slouží pro přenos signalizace mezi ústřednou a mobilní stanici. Přenos zpráv přes toto rozhraní je transparentně přenesen skrze BSS sekci.

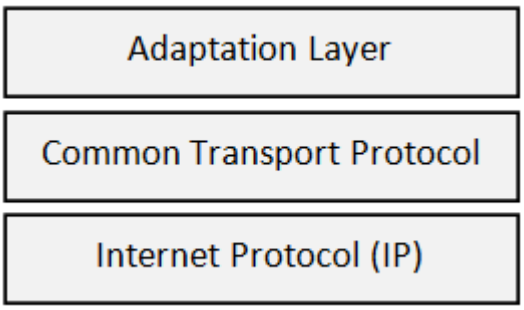
Tabulka 10.11 - Komunikační rozhraní použity v GSM síti, převzato z [4]

11 SIGTRAN

Pod pojmem SIGTRAN shrnujeme skupinu protokolů, které umožňují přenést signalizaci SS7 přes IP síť. Název je odvozen od kombinace slov Signaling Transport. Vzhledem k vysokým nákladů, které se s použití signalizace SS7 vážou (licenční poplatky, cena zařízení s podporou SS7), bylo přirozené, že se s postupem času signalizace vyvinula k využití stávající rozšířené IP struktury.

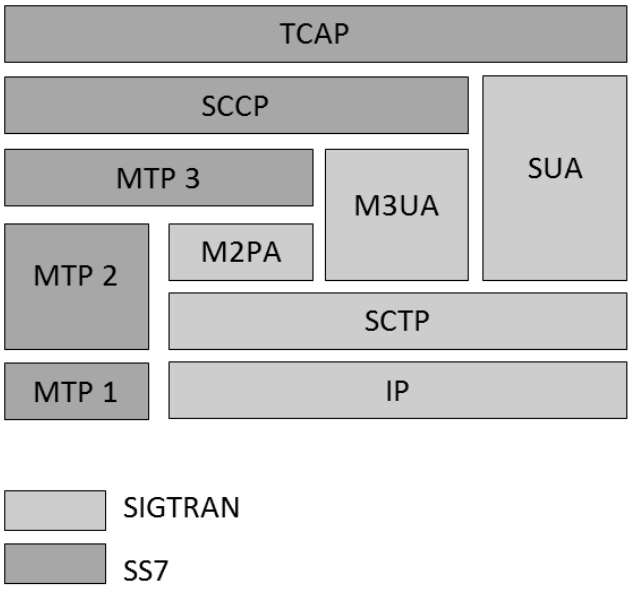
O vývoj a standardizaci se stará uskupení pojmenované jako *The IETF SigTran Working Group*. To definovalo výkonnostní požadavky v dokumentu RFC 2719. Ten definoval tři nezbytné komponenty nutné pro SigTran stack (viz Obrázek 11.1):

1. Množina adaptačních vrstev, které zajišťují podporu pro primitiva signalizačních protokolů.
2. Společný transportní protokol, který splňuje všechny požadavky, kladené na transport telefonní signalizace.
3. Síťový protokol IP.



Obrázek 11.1 - Tři vrstvy SITRAN stacku, převzato z [10]

Obrázek 11.2 ukazuje vztah mezi protokoly SS7 (které zajišťují přenos) a protokoly rodiny SIGTRAN. Do vrstvy *adaptation layer* patří protokoly M2PA, M2UA a SUA, společným transportním protokolem (vrstva *Common Transport Protocol*) je SCTP protokol.



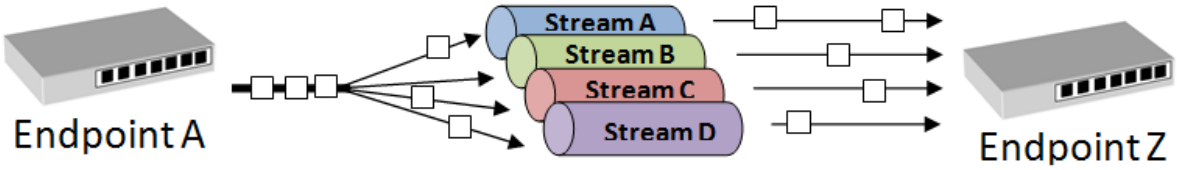
Obrázek 11.2 - Struktura protokolů rodiny SIGTRAN vzhledem k signalizaci SS7

11.1 Stream Control Transmission Protocol (SCTP)

Jedná se o transportní protokol podobný TCP a UDP protokolům. Kombinuje vlastnosti obou – je orientován na doručování zpráv stejně jako UDP a stejně jako TCP poskytuje spolehlivý a bezchybný přenos (doručení ve správném pořadí, bez duplikací atd.) s potvrzováním jejich doručením. Také implementuje systémem detekce a předcházení zahlcení přenosových linek. V terminologii SCTP je komunikační spojení nazýváno jako **asociace**.

Kromě toho přináší SCTP protokol i nové vlastnosti. Jednou z nich je i **multi-streaming** (viz Obrázek 11.3). SCTP protokol byl původně vyvinut pro přenos signalizace v telefonních sítích. Odtud vznikl požadavek na paralelní přenos několika oddělených streamů (dat jedné relace) v rámci jediné asociace. Příkladem použití multi-streamingu je například stahování webové stránky ze serveru, kdy současně se stahováním html souboru jsou stahovány i obrázky v jediné asociaci.

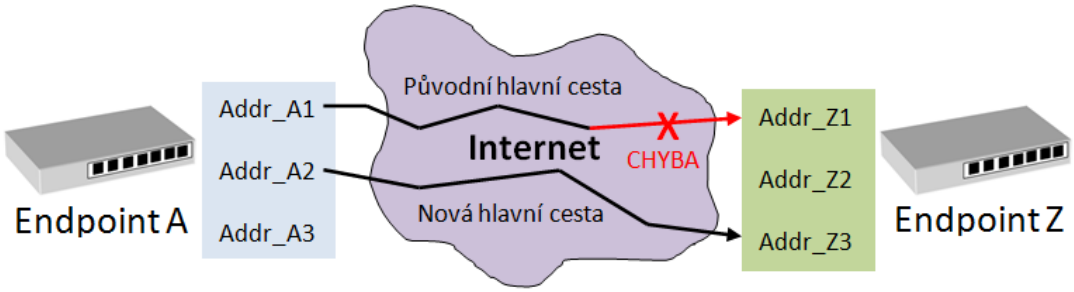
SCTP protokol pro každý stream garantuje doručení ve správném pořadí a případná ztráta paketu v některém ze streamu neovlivňuje ostatní streamy přenášené v asociaci.



Obrázek 11.3 - SCTP vlastnost multi-streaming

Další odlišností od stávajících protokolů je tzv. **multi-homing**. Jedná se o stav, kdy jeden nebo oba komunikující uzly vlastní více než jen jednu IP adresu (jedná se o libovolnou směs IPv4 aIPv6 adres). Seznam dostupných adres si komunikující strany vyměňují během založení asociace. Jedna z těchto adres je vybrána jako primární a je použita pro odesílání dat. Pro přenos opakovaných zpráv se však použije jedna z alternativních adres. To umožňuje automatické vytváření alternativních cest pro přenos dat v síti. O budování alternativních cest se stará směrovací protokol použitý v přenosové síti. Dochází k tomu tedy bez účasti komunikujících stran transparentně na straně sítě. Tyto alternativní cesty je možné použít pro doručení v případě, že hlavní cesta selhala a nelze jí nadále používat (nebo s velmi nepříznivými vlastnostmi přenosu).

Pro správnou činnost multi-houmingu existuje v protokolu systém **výběru a sledování primární cesty**. Protokol si udržuje informace o všech možných cestách, které jsou pro komunikující strany dostupné. Některá z nich je vybrána jako primární a na ní pak testuje její konektivitu. V případě, že se stane nedostupnou, vybere některou z alternativních cest jako novou primární cestu.



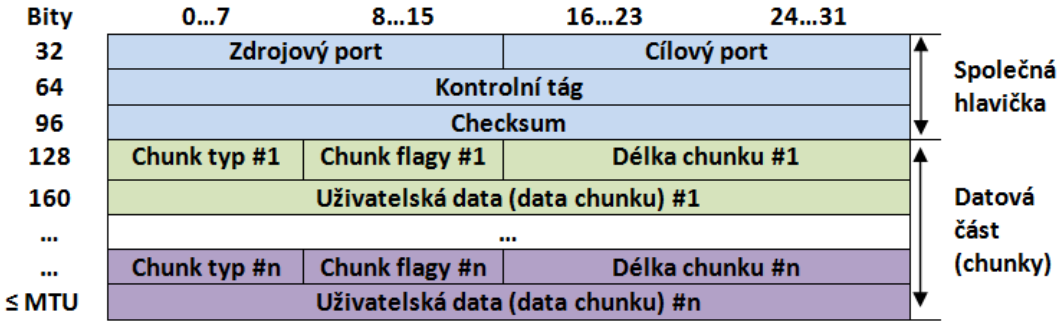
Obrázek 11.4 - SCTP multi-homing

Obrázek 11.4 schematicky vysvětluje princip multi-houmingu. V tomto případě má odesílatel i příjemce tři různé adresy. Nejprve se používá cesta mezi adresami *Addr_A1* a *Addr_Z1*. Časem se na ní vyskytne chyba, která znemožňuje její další použití. Proto vznikne nová cesta mezi adresami *Addr_A2* a *Addr_Z3* a nahradí stávající hlavní cestu.

SCTP protokol také zavádí nové **potvrzovací a validační mechanizmy**. Ty chrání proti útokům typu flooding a poskytují podporu pro ochranu proti duplikovaným či chybějícím chunkům.

11.1.1 Struktura paketu

Struktura SCTP paketu je jednoduší než v případě TCP paketu. Skládá se ze dvou základních částí (viz Obrázek 11.5) – společné hlavičky a datové části. Do datové části může být vloženo více než jen jeden chunk (datová jednotka připadající k jednomu datovému proudu). Limitem je pouze celková délka paketu, která nesmí přesáhnout MTU velikost. Díky tomu dokáže SCTP efektivněji využít přenosovou kapacitu linek.

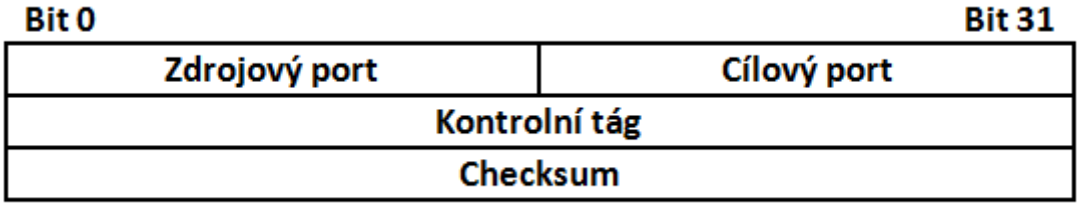


Obrázek 11.5 – Obecná struktura SCTP paketu

Společná hlavička (Common Header) zabírá prvních 12 bajtů paketu. Má pevnou strukturu, skládající se ze čtyř částí (viz Obrázek 11.6):

1. **Cílový port** je šestnácti bitové bezznaménkové číslo, které má stejnou funkci jako v případě TCP (či UDP) protokolu. Identifikuje, které aplikaci má být na cílovém zařízení předána datová část.
2. **Zdrojový port** je šestnáctibitové bezznaménkové číslo, které identifikuje aplikaci na zdrojovém zařízení, která daný paket odesílá.
3. **Kontrolní tag** je 32bitové bezznaménkové číslo, které příjemce používá k ověření odesílatele daného SCTP paketu. Toto číslo se musí shodovat s hodnotou inicializačního tágu (Initiate Tag), které bylo použito během inicializace aktuálně používané asociace. Jedna asociace tak používá dvě hodnoty kontrolního tágu, každý z účastníků komunikace si volí vlastní. Existují tři výjimky, kdy ke shodě nedochází:
    a. Paket, který obsahuje chunk typ INIT musí mít nulový verifikační tág.
    b. Paket, který obsahuje chunk typu SHOTDOWN-COMPLETE s nastaveným T-bit příznakem musí mít shodnou hodnotu, jako paket s chunkem typu SHOUTDOWN-ACK.
    c. Paket, který obsahuje ABORT chunk musí mít verifikační tág shodný s tím, který byl v paketu, který způsobil abort akci.

4. **Checksum** je 32bitový CRC kontrolní součet celého SCTP paketu. Pro výpočet je použit Adler-32 algoritmus.



Obrázek 11.6 - Struktura SCTP hlavičky

Datová část zabírá zbytek celého paketu. Skládá se z několika (i jednoho) datového záznamu, který se nazývá **chunk** (viz Obrázek 11.7). Ty mají přesně definovanou hlavičku, která je nezávislá na přenášené informaci. Skládá se ze tří částí a vlastního pole pro přenos uživatelských dat (to se liší podle typu chunku).

Indikátor typu je osmibitové číslo, které identifikuje typ přenášeného chunku. Tabulka 11.2 shrnuje všechny možné typy chunků, které jsou definovány. Indikátor typu je kódován takovým způsobem, že nejvyšší dva bity určují akci, kterou musí endpoind s paketem udělat, pokud nerozpozná, o který typ se jedná. Tabulka 11.1 shrnuje tyto akce.

Hodnota	Požadovaná akce
00	Zastav zpracování tohoto SCTP paketu a zahoď jej, nezpracovávej žádné budoucí chunky v něm.
01	Zastav zpracování tohoto SCTP paketu a zahoď jej. Nezpracovávej žádný další budoucí chunky. Nahlas nerozpoznaný parametr v poli *Unrecognized Parameter Type* (který se nachází buď v ERROR nebo v INIT ACK chunku)
10	Přeskoč tento chunk a pokračuj dále ve zpracování SCTP paketu.
11	Přeskoč tento chunk a pokračuj dále ve zpracování SCTP paketu. Také pošli ERROR chunk s hodnotou *Unrecognized Chunk Type* jako důvod chyby.

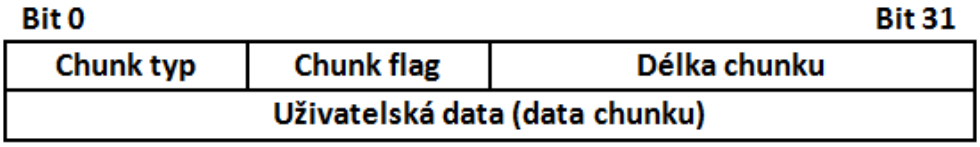
Tabulka 11.1 - Akce při nerozpoznání typu chunku (převzato z [18])

Pole **flag** je osmibitové číslo, které v každém svém bitu nese informaci o určité vlastnosti chunku:

1. **Prvních pět bitů** (osmý až dvanáctý bit v chunku) jsou rezervovány pro budoucí užití a v současnosti nenesou žádnou informaci.
2. **Šestý bit** (tzv. **U-bit,** třináctý bit v chunku) indikuje, že chunk neobsahuje sekvenční číslo streamu.
3. **Sedmý bit** (tzv. **B-bit**, čtrnáctý bit v chunku) indikuje začátek fragmentace.
4. **Osmý bit** (tzv**. E-bit**, patnáctý bit v chunku) indikuje konce fragmentace. Možnou kombinaci hodnot

Každý chunk obsahuje pole pro přenos vlastních dat. To je ale proměnné velikosti, proto musí každý chunk obsahovat i 32bitové pole pro uložení **délky chunku**. Pokud délka chunku není zarovnána na čtyřbajtovou hranici, potom je chunk automaticky doplněn nulami na nejbližší hodnotu násobku čtyř bajtů (32 bitů). Toto rozšíření není zahrnuto do celkové délky chunku, tak je možné při přijetí paketu rozlišit originální datovou část a výplňovou část.

Poslední částí chunku je pole proměnné velikosti, které obsahuje vlastní užitečná data. Pole musí být zarovnáno na hranici čtyř bajtů (viz princip popsaný v předcházejícím odstavci).



Obrázek 11.7 - Struktura chunku

ID value	Chunk Type	
0	Payload Data	DATA
1	Initiation	INIT
2	Initiation Acknowledgement	INIT ACK
3	Selective Acknowledgement	SACK
4	Heartbeat Request	HEARTBEAT
5	Heartbeat Acknowledgement	HEARTBEAT ACK
6	Abort	ABORT
7	Shutdown	SHUTDOWN
8	Shutdown Acknowledgement	SHUTDOWN ACK
9	Operation Error	ERROR
10	State Cookie	COOKIE ECHO
11	Cookie Acknowledgement	COOKIE ACK
12	Reserved for Explicit Congestion Notification Echo	ECNE
13	Reserved for Congestion Window Reduced	CWR
14	Shutdown Complete	SHUTDOWN COMPLETE

Tabulka 11.2 - Typy chunků, převzato z [18]

11.1.2 Proces vytvoření SCTP asociace

Před tím, než je možné zahájit přenos dat, musí úspěšně proběhnout mezi komunikujícími stranami inicializační proces a vytvořit tak **SCTP asociaci**.

SCTP protokol používá pro založení asociace tzv. čtyřcestný handshaking (4way handshaking), tedy proces skládající se ze čtyř přenášených zpráv. Obrázek 11.8 schematický tento proces popisuje, komunikující strany jsou nazvány jako endpoint A a endpoint Z:

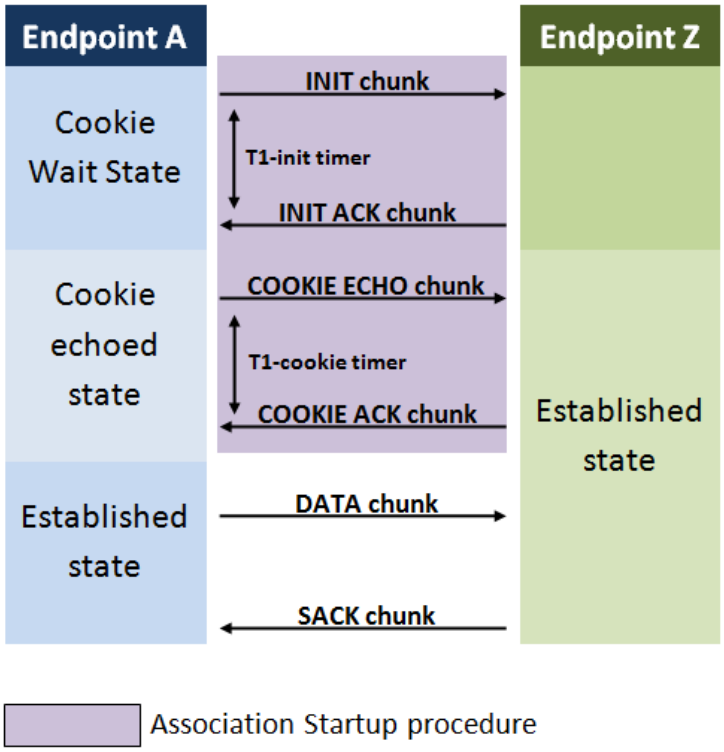
Nejprve pošle endpoint A tzv. **INIT chunk**. Jakmile je chunk úspěšně odeslán, endpoint A spustí časovač T1-init a přejde do stavu *Cookie-Wait*.

Po přijetí tohoto chunku vytvoří endpoint Z **State Cookie** hodnotu, kterou pak odešle jako **INIT ACK chunku**. Poznamenejme, že v tuto chvíli se ještě nealokují žádné systémové prostředky. K tomu dojde až po úspěšném vytvoření asociace.

Při přijetí zprávy INIT ACK zastaví endpoint A svůj T1-init časovač a opouští *Cookie-Wait* stav. Potom odešle **COOKIE ECHO chunk**, jehož součástí je *State Cookie*, kterou poslal endpoint Z v předcházejícím krok, spustí T1-cookie časovač a přejde do stavu *Cookie-echoed.*

Jakmile endpoint Z příjme COOKIE ECHO chunk, vytvoří tzv. **Transmission Control Block** (TCB, datový záznam nesoucí všechna potřebná data pro činnost asociace), přejde do stavu *Established* a odešle zpět tzv. **COOKIE ACK chunk.**

Pokud endpoint A příjme zprávu COOKIE ACK, přejde do stavu *Established* a zastaví T1-cookie časovač. Od této chvíle je vytvořena asociace mezi oběma účastníky komunikace (endpoint A i endpoint B) a je možné zasílat datové chunk.



Obrázek 11.8 - Schéma procesu založení asociace v SCTP protokolu, převzato z [18], přepracováno

11.1.3 Ukončení SCTP asociace

Koncový bod (endpoint) by měl ukončit svou asociaci, jakmile je ukončena služba, která ji používala. Asociace může být ukončena buď *abort* akcí, nebo *shutdown* akcí.

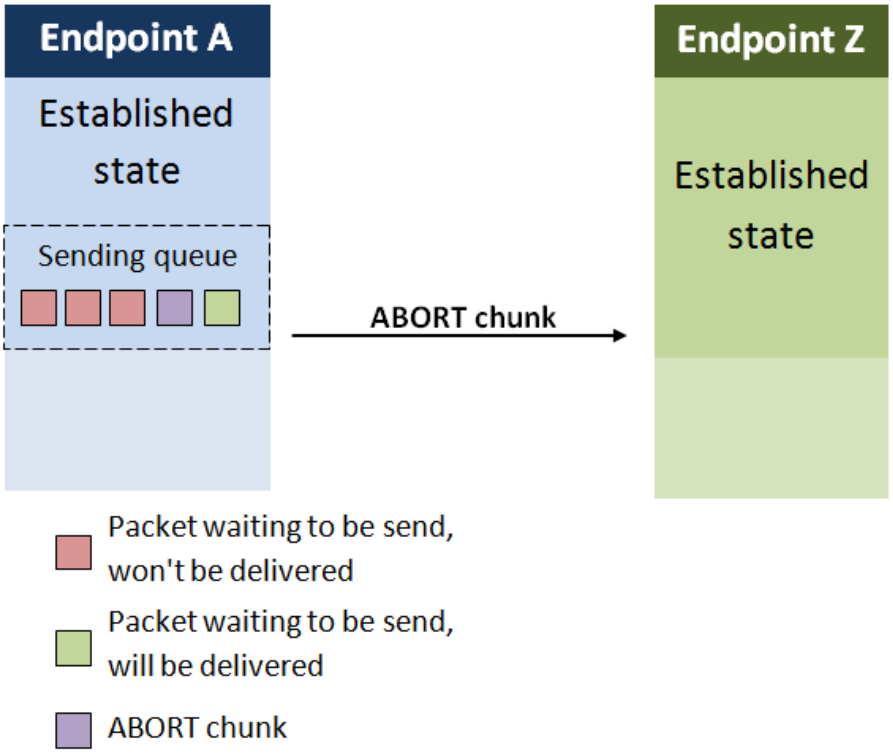
***Abort* akce** je asynchronní způsob ukončení asociace, během kterého jsou veškeré údaje, které čekají na obou koncích asociace k odeslání, zahozeny bez pokusu o doručení protistraně a asociace je okamžitě ukončena.

Jakmile se endpoint rozhodne ukončit asociaci za pomoci *abort* akce, musí poslat protistraně ABORT chunk. Tento chunk musí mít vyplněnu hodnotu verifikačního tágu hodnotou protistrany a nesmí do paketu přidat žádný z datových chunku (DATA chunk). Pokud je asociace ukončována na základě požadavku vyšší vrstvy (uživatele), měl by být součástí ABORT chnuku i důvod ukončení.

Pokud účastník asociace příjme paket obsahující ABORT chunk, nesmí na něj nikterak odpovídat a musí zkontrolovat verifikační tág přijatého chunku. Pokud kontrola proběhne úspěšně, odstraní ze seznamu TCB záznam a ohlásí ukončení asociace své nadřazené vrstvě.

Obrázek 11.9 schematický popisuje tento postup. V tomto případě se endpoint A rozhodl ukončit asociaci a proto zasílá ABORT chunk své protistraně (endpoint Z). Odchozí fronta endpointu A na obrázku schematicky ukazuje, že pakety odeslané před posláním ABORT chunku budou doručeny (a potvrzeny) a pakety, které se nacházejí ve frontě po jeho odeslání, musí endpoint A zahodit a již je nedoručuje. Poznamenejme, že odeslání ABORT chunku je asynchronní – je odesílán

okamžitě po vzniku požadavku na ukončení asociace, nezávisle na paketech, které čekají na své odeslání.



Obrázek 11.9 - Schéma ukončení SCTP asociace za pomoci a*bort* akce

Ukončení asociace za pomoci ***shutdown* akce** je považováno za správný způsob ukončení. Důvodem je, že jsou veškerá data čekající ve frontě obou koncových bodů doručena svým příslušným protistranám. Nicméně SCTP nepodporuje polootevřené stavy (tak jako TCP), v němž jedna strana může pokračovat v odesílání dat, zatímco druhý konec je uzavřen. Když jeden koncový bod provede ukončení asociace (*shutdown* akcí), asociace na obou koncích přestane přijímat nová data od svých uživatelů (služby běžící na vyšší vrstvě, která asociaci používá) a pouze doručí data, která zůstala ve frontě v době odeslání/přijetí SHUTDOWN chunku. [18]

Jakmile se uživatel asociace rozhodne ukončit jí, oznámí to SCTP vrstvě za pomoci *SHUTDOWN* primitiva. Od této chvíle přestane SCTP vrstva přijímat další data k odeslání od svého uživatele a přejde do stavu *shutdown-pending*, ve kterém setrvá až do chvíle, kdy jsou všechny zbývající pakety z odchozí fronty odeslány a potvrzeny.

Jakmile je odchozí fronta prázdná, pošle endpoint **SHUTDOWN chunk**, spustí T2-shutdown časovač a přejde do stavu *shutdown-sent*. Pokud časovač vyprší, musí endpoint odeslat znovu SHUTDOWN chunk.

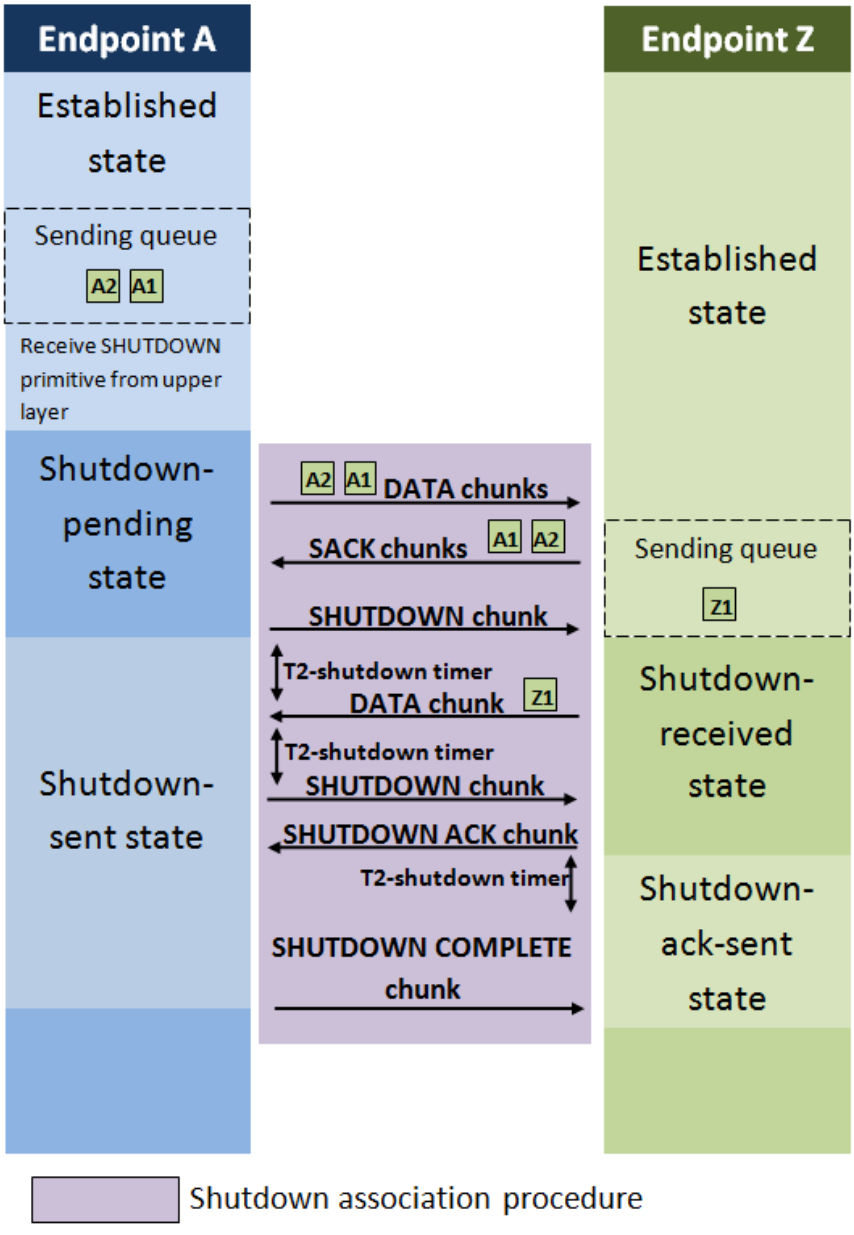
Jakmile vzdálená strana asociace příjme SHUTDOWN chunk, přejde do *shutdown-received* stavu a přestane přijímat nová data od svého uživatele (vyšší vrstvy využívající asociaci). Pokud zůstaly nějaké neodeslané pakety ve frontě, musí se přenést před tím, než je asociace ukončena. Přenos datových chunků probíhá stejně jako v případě stavu *established.*

Jakmile endpoint ve stavu *shutdown-sent* přijme paket obsahující jeden nebo více datových chunků, musí na něj okamžitě odpovědět SHUTDOWN chunkem a restartovat svůj T2-shutdown časovač. Pokud by SHUTDOWN chunk nedokázal potvrdit všechny přijaté datové chunky, je nutné spolu s ním odeslat i SACK chunk (tedy dvojce SACK + SHUTDOWN chunky).

Jakmile příjemce SHUTDOWN chunku odešle všechna svá čekající data, pošle své protistraně **SHUTDOWN ACK chunk**, spustí vlastní T2-shutdown časovač a přejde do stavu *shutdown-ack-sent*.

Po přijetí tohoto chunku zastaví odesílatel SHUTDOWN chunku T2-shutdown časovač, odešle **SHUTDOWN COMPLETE chunk** a odstraní všechny záznamy související s asociací.

Vzdálený bod po přijetí SHUTDOWN COMPLETE chunku zkontroluje, zda se nachází ve stavu *shutdown-ack-sent*. Pokud ne, chunk zahodí a nikterak na něj nereaguje. V opačném případě zastaví svůj T2-shutdown časovač a odstraní všechny záznamy o asociaci, kterou tak uzavře (asociace přejde do stavu *closed*). Obrázek 11.10 popisuje princip *shutdown* akce.



Obrázek 11.10 - Schéma ukončení SCTP asociace za pomoci *shutdown* akce

11.2 MTP3 User Adaptation (M3UA)

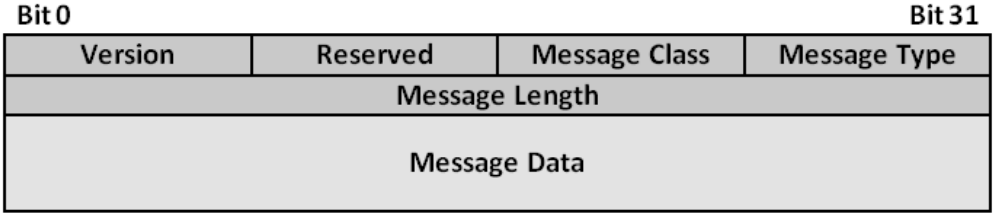
M3UA protokol zajišťuje přenos jakékoliv SS7 MTP3 signalizace (jako je např. ISUP a SCCP zprávy) skrze IP síť. K tomu využívá služeb vrstvy Stream Control Transmission Protocol (SCTP).

Protokol se skládá ze společné hlavičky, která je následována parametry, specifickými pro každý typ přenášené zprávy.

11.3 SCCP User Adaptation (SUA)

Tento protokol se zabývá doručováním uživatelských SCCP zpráv (jako je např. MAP či TCAP) přes IP síť mezi dvěma signalizačními koncovými body za použití služeb SCTP.

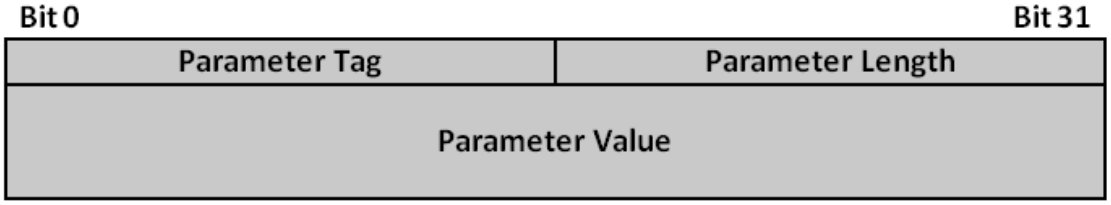
Obrázek 11.11 ukazuje obecný formát SUA zprávy, který se skládá ze společné hlavičky a vlastních přenášených dat. Společná hlavička se skládá z pěti částí:



Obrázek 11.11 - Schéma SUA zprávy

- **Verze** – verze použitého protokolu. Podporované verze jsou *SUA version 1.0* s hodnotou 1 [19]
- **Message Class** – zprávy v SUA protokolu jsou seskupeny do několika skupin podle sémantické podobnosti. Tento identifikátor specifikuje, o kterou třídu se jedná. Těchto tříd existuje celkem osm, ale nejdůležitější a nejvíce používané jsou následující tři:
  - **0** – SUA řídící zpráva.
  - **7** – zpráva pro nespojovanou službu.
  - **8** – zpráva pro spojovou službu.
- **Message Type** – specifikuje typ zprávy, která je přenášena pomocí SUA protokolu. Jinak řečeno, zatímco pole Message Class definuje třídu zprávy, toto pole specifikuje, o kterou z možných zpráv dané třídy se jedná.
- **Délka zprávy** – definuje délku celé zprávy v oktetech včetně hlavičky a všech výplňkových bitů.

SUA zprávy se skládají ze společné hlavičky (zmíněné výše) následovanou několika parametry (i žádným), které souvisí s přenášeným typem zprávy (kombinace *Message Class*/*Message Type*). Přenášené parametry používají formát nazývaný jako *Tag-Length-Value* (viz Obrázek 11.12).



Obrázek 11.12 - Formát parametrů

Šestnáctibitová hodnota ***Parameter Tag*** říká, o který typ parametru se jedná. Délka parametru (uložena v poli ***Parameter Length***) udává velikost přenášeného parametru a to včetně parametrů *Parameter Tag*, *Parameter Length* a *Parameter Value.* Tato hodnota nezahrnuje případné výplňkové bity. Tím lze odlišit přenášenou hodnotu od výplňkových bitů.

Poslední pole ***Parameter Value*** obsahuje vlastní přenášená data. Celková velikost parametru (včetně *Parameter Tag, Parameter Length* a *Parameter Value*) musí být zarovnána na velikost násobku čtyř bytů. Zarovnání se provádí přidáním nulových bytů za přenášená data (za pole *Parameter Value*).

12 Důležité procedury v GSM

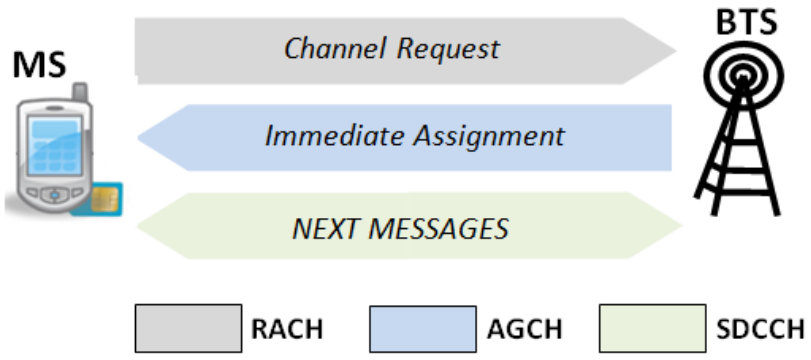
Všem procedurám GSM systému, které jsou inicializovány mobilní stanicí, předchází stejná posloupnost kroků, kterou je nutné vykonat před tím, než se zahájí vykonání vlastního požadavku procedury. Jejím cílem je vytvořit spojení mezi MS a GSM sítí, ověřit uživatelovu identitu a zahájit šifrování v přístupové síti (kde je na rozdíl od páteřní sítě komunikace šifrována). Postup lze shrnout do následujících kroků:

1. Pokud MS vstoupila do nové *buňky*, musí se inicializovat a naladit na danou BTS stanici, která danou *buňku* ovládá.
2. Získání komunikačního kanálu procedurou *Channel Request*.
3. Poslání požadavku na službu (telefonní hovor, přenos dat atd.)
4. Autentizace mobilní stanice
5. Zahájení šifrování komunikace mezi MS a BTS stanicí
6. Provedení požadované operace

12.1 Channel Request

Před tím, než může MS jakkoliv komunikovat se sítí, musí dojít k vytvoření komunikačního kanálu. K jeho vytvoření slouží procedura nazývaná jako ***Channel Request.*** Obrázek 12.1 ukazuje postup:

1. Mobilní stanice vyjádří svůj požadavek na přidělení komunikačního kanálu zaslním zprávy ***Channel Request*** na *RACH* kanálu.
2. BTS stanice odpovídá zasláním zprávy ***Immediate Assignment*** na kanálu *AGCH*. V této zprávě posílá MS informace o přiděleném komunikačním kanálu, na který se musí MS připojit.
3. MS se přepne na daný *SDCCH* kanál.



Obrázek 12.1 - Channel Request procedura

V některých situacích se namísto *SDCCH* kanálu použije ***TCH*** (Traffic Channel) jako komunikační kanál pro předání požadavku na službu. Pro tyto události má *TCH* kanál definovány dva režimy činnosti – *signaling mode*, který slouží k přenosu signalizace a emuluje tak chování *SDCCH* kanálu, a *traffic mode*, který je pro *TCH* běžný a slouží k přenosu hlasu (případně dat). Pokud se jako komunikační kanál použije *TCH* kanál, potom zůstane přidělený i po přijetí požadavku na službu a

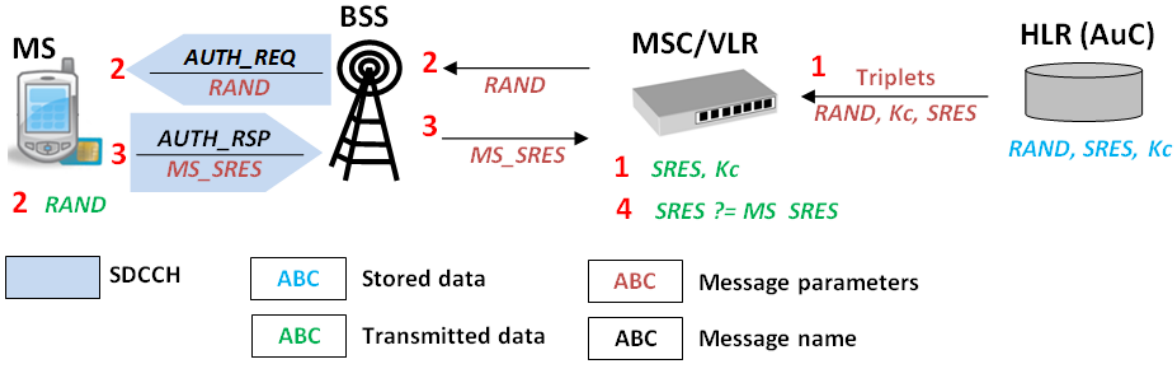
slouží k jejímu uskutečnění. Síť pouze pošle zprávu *channel mode modify command*, která přepne *TCH* do režimu *traffic mode*.

12.2 Autentizace MS

Princip autentizace mobilní stanice, který je použit v GSM, je popsán v kapitole 5.4. Během procesu autentizace spolu komunikují pouze mobilní stanice (MS) a ústřednou (MSC). BSS subsystém (BTS stanice a BSC kontrolér) pouze přeposílají zprávy tak, jak je přijmou. Pro autentizaci je používán nejčastěji *SDCCH* kanál, ale může být použit i *TCH* v režimu *signaling mode* (viz kapitola 12.1).

Obrázek 12.2 popisuje posílané zprávy a jejich parametry, které souvisejí s autentizačním procesem. Modře jsou naznačena data, která jsou na dané entitě uložena a nejsou tedy získána v průběhu autentizačního procesu. Zeleně jsou naznačena data, která entita získá z příchozích zpráv:

1. Nejdříve musí autentizační centrum (AuC) vygenerovat *autentizační triplet* – trojici hodnot *Rand, SRES a Kc*. Ten je poslán *MSC* ústředně, ke které je aktuálně MS připojena. Ta si ponechá ze zprávy dvojici hodnot *SRES a Kc*, které později použije k ověření identity MS.
2. Hodnotu *Rand* pošle skrze BSS subsystém mobilní stanici. Jedná se o jedinou hodnotu, kterou MS od sítě obdrží. V tuto chvíli není komunikace na přístupové síti šifrována, proto nesmí být posílána žádná tajná informace. *Rand* je náhodně vygenerovaná hodnota, která se při každé autentizaci generuje znovu.
3. Mobilní stanice aplikuje na přijatou hodnotu *Rand* algoritmus *A3* a vygeneruje tak hodnotu *MS_SRES*. Ta je opět veřejná a nemusí být utajována (je generována v průběhu autentizace vždy znovu). Tato hodnota přes BSS subsystém poslána zpět *MSC* ústředně.
4. *MSC* porovná přijatou hodnotu *MS_SRES* s hodnotou *SRES*, kterou obdržela od *AuC* během prvního kroku. Pokud jsou tyto hodnoty stejné, je MS úspěšně autentizována, jinak autentizace selhala a další komunikace s MS je zamítnuta.



Obrázek 12.2 - Autentizace

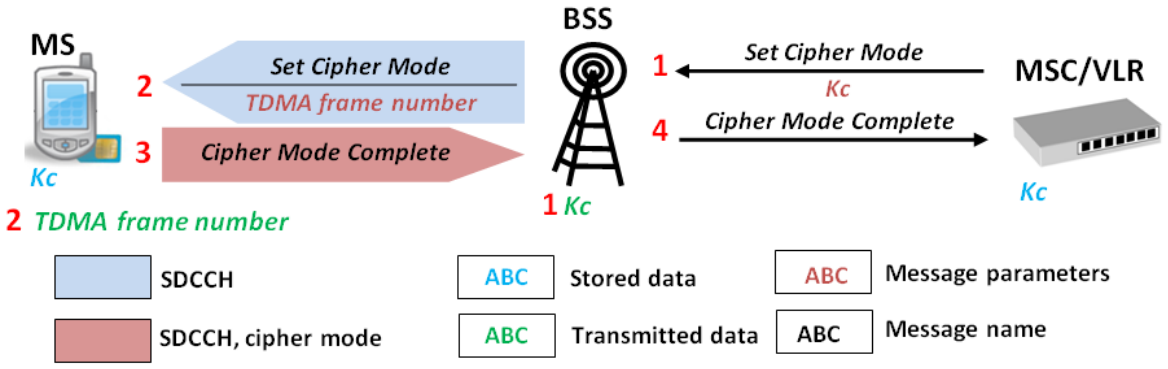
12.3 Šifrování komunikace

Princip šifrování v přístupové síti, který je použit v GSM, je popsán v kapitole 5.5. Obrázek 12.3 popisuje zasílané zprávy a jejich parametry, které zajišťují provedení šifrování.

1. Ústředna (MSC) pošle zprávu *Set Cipher Mode* BSC kontroléru. Součástí zasílané zprávy je jako parametr i klíč *Kc*, který slouží jako vstup šifrovacího algoritmu (viz kapitola 5.4).
2. BSC pošle přijatý klíč *Kc* spolu s 22bitovým číslem TDMA rámce BTS stanici.
3. BTS stanice si přijaté hodnoty uloží a pošle MS zprávu *Set Cipher Mode*, která MS přikazuje zahájit šifrování komunikace. Parametry této zprávy je požadovaná varianta *A5* algoritmu a

přijatá hodnota *TDMA rámce*. Jak je vidět, šifrovací klíč *Kc* není nikdy posílán skrze přístupovou síť a nemůže tak být odposlechnut.

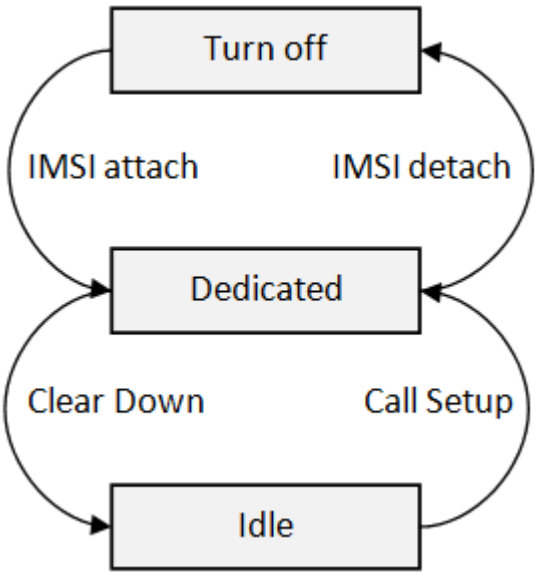
4. Od této chvíle začne MS svou komunikaci šifrovat. K šifrování je použit algoritmus *A5*, jehož vstupy jsou inicializovány hodnotami *Kc* a přijaté hodnoty *TDMA rámce*, který je aplikován na přenášená data. O této skutečnosti informuje MSC zasláním zprávy *Cipher Mode Complete*.



Obrázek 12.3 - Zahájení šifrování komunikace

12.4 Mobility management (správa mobility)

Správa mobility zajišťuje sledování mobilní stanice (MS), zatímco se pohybuje. Funkce se liší podle stavu, ve kterém se MS nachází (z pohledu sítě, viz Obrázek 12.4).



Obrázek 12.4 - Stavy MS, převzato z [15]

V prvním případě se mobilní stanice nachází ve stavu ***turn off***. Tento stav se z pohledu sítě definuje jako stav, kdy mobilní stanice není schopna reagovat na **paging** akci. To může nastat v několika případech:

1. Mobilní stanice je vypnuta, v tomto případě by vypnutí měla předcházet procedura *IMSI detach*.
2. Mobilní stanice se nachází mimo pokrytí sítě. Pro síť se taková MS tváří jako dostupná, protože nedošlo k vykonání procedury *IMSI detach*, a to až do té doby, než se v důsledku

neprovedení periodické operace *location update* provede implicitní *IMSI detach* operace. Díky tomu nemůže provádět pravidelné aktualizace své polohy a nakonec dojde k jejímu odhlášení za pomoci implicitní *IMIS detach* operace.

Druhý stavem, ve kterém se MS může nacházet, se jmenuje ***dedicated***. Ten značí, že mobilní stanice je zapnutá a aktuálně probíhá datová/hlasová komunikace se sítí (např. během telefonního hovoru). V tomto stavu je nutné provádět ***handover*** (viz kapitola 5.3). Díky tomu není nutné provádět *Location Update* operaci, protože její funkci přebírá právě *handover*.

Posledním stavem, ve kterém se může MS nacházet je stav ***idle***. V něm je schna uskutečnit nebo přijmout telefonní hovor. Z pohledu sítě je MS zaregistrována (proběhla operace *IMSI attach*) a reaguje na *paging* akci. Pokud se v tomto stavu MS pohybuje (dochází ke změně lokačních oblastí), musí o tom dát vědět síť a to za pomoci operace ***Location Update***.

Tabulka 12.1 shrnuje popis operací, které MS vykonává během svého pohybu (změny lokačních oblastí).

Stav MS	Prováděná akce	Popis
Turn off	-	V tomto stavu MS nemá žádné spojení se sítí, proto nemůže provádět žádnou akci.
Dedicated	Handover	V případě aktivního hovoru (přenosu dat) je nutné zajisti co nejvyšší kvalitu komunikačního kanálu. Proto se MS aktivně přepíná mezi dostupnými BTS stanicemi podle kvality jejich signálu – provádí handover. Ten v sobě skrývá veškerou funkčnost *LU* operace a proto jí nahrazuje.
Idle	Location Update	MS aktuálně nevyužívá žádnou službu sítě, proto jí pouze zasílá svou aktuální polohu, aby byla síť schopná MS lokalizovat a komunikovat s ní (za pomoci *paging* akce).

Tabulka 12.1 - Operace prováděné MS podle jejího stavu

12.4.1 IMSI attach

Tato operace slouží k přihlášení mobilní stanice do sítě při přechodu ze stavu *turn off*. Iniciátorem je mobilní stanice. Postup této operace je následující:

1. Nejprve musí proběhnout operace *Channel Request*.
2. MS posílá po přiděleném SDCCH kanálu zprávu ***Location Update Request***. Součástí této zprávy je jeden z identifikátorů mobilní stanice – buď *IMSI* nebo *TMSI*.
3. BSS potvrdí přijetí požadavku na změnu lokační polohy zasláním zprávy ***Request Acknowledgment***. Touto zprávou pouze informuje MS o přijetí požadavku na aktualizaci lokační oblasti (nikoliv o jeho dokončení).
4. BSS přepošle přijatou zprávu (LU request) k MSC/VLR.
5. MSC/VLR kontaktuje HLR databázi s požadavkem na verifikaci *IMSI* čísla a zaslání autentizačního *tripletu*.
6. HLR sama o sobě potřebné informace nemá, proto musí poslat požadavek do autentizačního centra (AuC).

7. Autentizační centrum vygeneruje *triplet* a pošle jej (společně s *IMSI* číslem, ke kterému byl *triplet* vygenerován) zpět HLR databázi.
8. HLR databáze provede ověření *IMSI* čísla (zda má uživatel s daným číslem povoleno využívat služeb sítě). Pokud ověření dopadlo dobře, pošle *triplet* a *IMSI* číslo zpět ústředně MSC/VLR.
9. Dalším krokem je provedení autentizace MS (viz kapitola 12.2).
10. Pokud autentizace proběhla úspěšně, musí dojít k šifrování komunikace (viz kapitola 12.3).
11. MSC/VLR pošle mobilní stanici zprávu *Location Updating Accept* (LUA). Také vygeneruje novou hodnotu *TMSI* čísla (přidělení čísla *TMSI* je procesem VLR databáze). Tu pošle MS buď jako parametr zprávy LUA nebo jí pošle odděleně ve zprávě *Reallocation Command.*
12. MS přijme novou hodnotu *TMSI* zasláním zprávy *TMSI Reallocation Complete* určenou pro MSC/VLR.
13. BSS subsystém přikáže MS přejít do *idle* stavu (a uzavřít tak komunikační kanál) zasláním zprávy *Channel Release*. Sám pak komunikační kanál uzavře a uvolní prostředky pro jinou mobilní stanici.
14. MSC/VLR pošle zprávu *Update Location* HLR databázi, která podle této zprávy aktualizuje své záznamy o MS (uloží, pod kterou MSC/VLR MS aktuálně spadá).

12.4.2 Explicitní IMSI detach

IMSI detach procedura slouží k odpojení mobilní stanice ze sítě, ke které byla připojena. V případě explicitní varianty procedury je iniciátorem mobilní stanice. Je zahájena v případě, že MS přechází do stavu *Turn off*, tedy mobilní stanice se vypíná nebo bude nedostupná.

Postup, pro jednoduchost zde neuvádíme nutnost autentizace MS a šifrování komunikace (obě procedury by měly nastat před odesláním zprávy *IMSI Detach Indication*) [20]:

1. Nejprve je nutné provést *Channel Request* operaci.
2. Jakmile je vytvořen komunikační kanál, posílá MS zprávu ***IMSI Detach Indication*.** V tuto chvíli považuje MS proceduru *IMSI detach* za dokončenou a odpojí se z komunikačního kanálu. BSS přeposílá přijatou zprávu odpovídající MSC/VLR ústředně.
3. MSC/VLR zareaguje odesláním zprávy ***Location Cancel Request*** domovské HLR databázi (té, ve které je daná MS registrována).
4. HLR databáze si u daného IMSI čísla poznačí, že je aktuálně odpojené (**detached**) a odstraní všechny ukazatele (např. aktuální VLR databázi) daného IMSI čísla ze své databáze.

12.4.3 Implicitní IMSI detach

Tato procedura slouží ke stejnému účelu, jako explicitní *IMSI detach* (viz kapitola 12.4.2). Liší se v podmínkách, které vedou k jejímu vyvolání. Je inicializována VLR databází v případě, že s danou MS neproběhla žádná komunikace během doby určené *implicit detach time* časovače. Jeho hodnota je odvozena od *periodic location updating* časovače.

Jakmile dojde k založení, je tento časovač pozastaven a to až do doby, kdy je rádiová komunikace ukončena. V tu chvíli je časovač vynulován a znovu spuštěn. Tuto proceduru by měla síť vyvolat i v případě negativní odpovědi na kontrolu *IMEI* čísla.

12.4.4 Location Update

Jedná se o mechanizmus, který je použit k aktualizaci aktuální pozice mobilní stanice, která se nachází ve stavu *idle*. Mobilní stanice musí provést aktualizaci své polohy ve čtyřech případech:

1. MS je poprvé zapnuta
2. MS se pohybuje v rámci stejné MSC/VLR oblasti, dojde ale ke změně lokační oblasti (LA)
3. MS se přesune do nové MSC/VLR oblasti
4. Vyprší časovač pro pravidelné hlášení polohy (*location update timer*)

Celou operaci můžeme rozdělit do několika logických celků (viz Obrázek 12.5, logické celky):

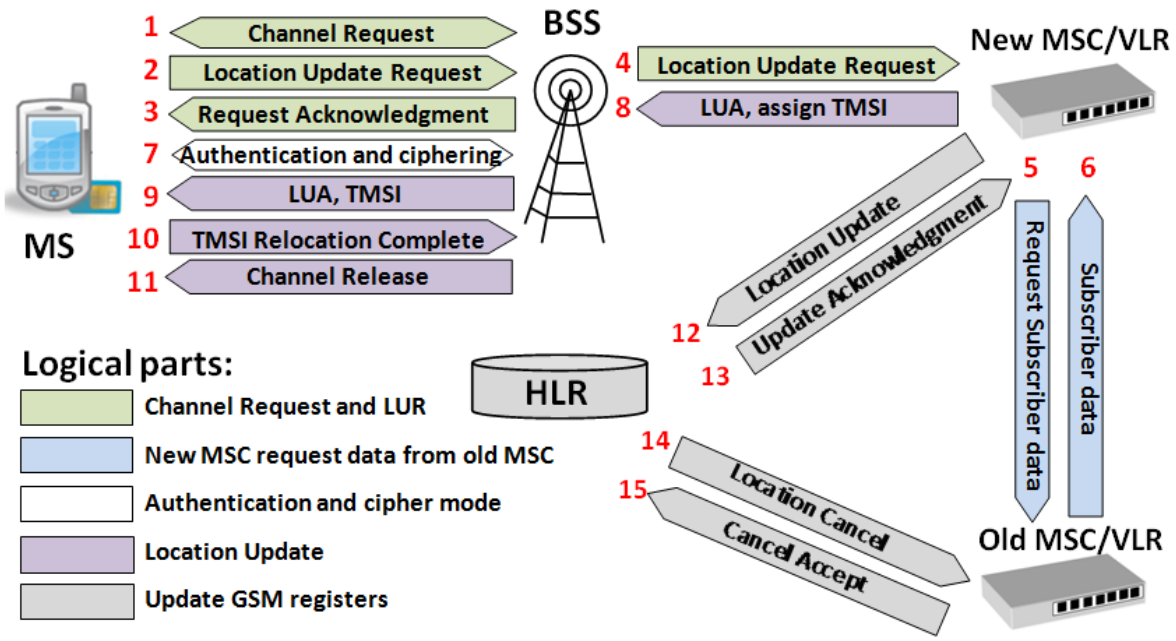
1. Předání požadavku o provedení LU od MS do sítě. Tato část zahrnuje operace v přístupové síti (bezdrátová část GSM sítě) a přenesení všech nutných parametrů.
2. Jakmile je síť informována o nutnosti provést LU operaci, musí kontaktovat VLR databázi, která spravuje lokační oblast, do které MS vstupuje, a získat data o MS z opouštěné VLR databáze. Zde se už veškerá komunikace odehrává v rámci páteřní sítě.
3. Jakmile jsou získána všechna potřebná data, musí se MS autentizovat a začít šifrovat svou komunikaci.
4. Předposledním krokem je přidělení nového *TMSI* čísla a jeho zaslání MS, dokončení *Location Update* procedury na straně MS a uvolnění komunikačního kanálu.
5. Posledním krokem je aktualizace dat v GSM databázích.

V procesu *Location Update* operují dvě odlišné VLR databáze. **Nová MSC/VLR** databáze, do které se mobilní stanice snaží přihlásit, a **stará MSC/VLR databáze**, v jejíž spravované oblasti se MS původně nacházela.

Obrázek 12.5 podrobně popisuje jednotlivé zprávy a operace, které musejí proběhnout v průběhu aktualizace umístění mobilní stanice:

1. Nejprve musí MS požádat o přidělení komunikačního kanálu, tedy provést *Channel request* operaci.
2. Poté po přiděleném *SDCCH* kanálu pošle ***Location Update Request*** zprávu. Součástí zprávy je aktuálně používaná *TMSI* hodnota a také *LAI* opouštěné oblasti.
3. BTS odpoví zasláním zprávy ***Request Acknowledgment***, kterou potvrzuje přijetí předcházející zprávy.
4. BSS přepošle požadavek na změnu lokační oblasti nové MSC/VLR databázi.
5. Nová MSC ústředna nerozpozná IMSI (případně TMSI), proto musí kontaktovat původní ústřednu (podle obdrženého LAI čísla, které obdržela jako parametr zprávy *Location Update Request*). Po ní požaduje informace o uživateli daného *IMSI* (případně *TMSI*).
6. Stará MSC ústředna pošle požadované informace zpět nové MSC.
7. Nyní musí nová MSC/VLR autentizovat MS. To může udělat dvěma způsoby:
    a. Od původní ústředny obdrží spolu s informacemi o MS i balík nevyužitých *tripletů*, které byly již dříve vygenerovány pro danou MS, ale nebyly využity. V tom případě je nová MSC použije pro autentizaci.
    b. O vygenerování *tripletů* se musí nová MSC postarat sama. Proto kontaktuje příslušnou HLR databázi s požadavkem o autentizaci dané MS. Ta kontaktuje své autentizační centrum (AuC), které vygeneruje nový set *tripletů*, které jsou odeslány zpět nové MSC ústředně.

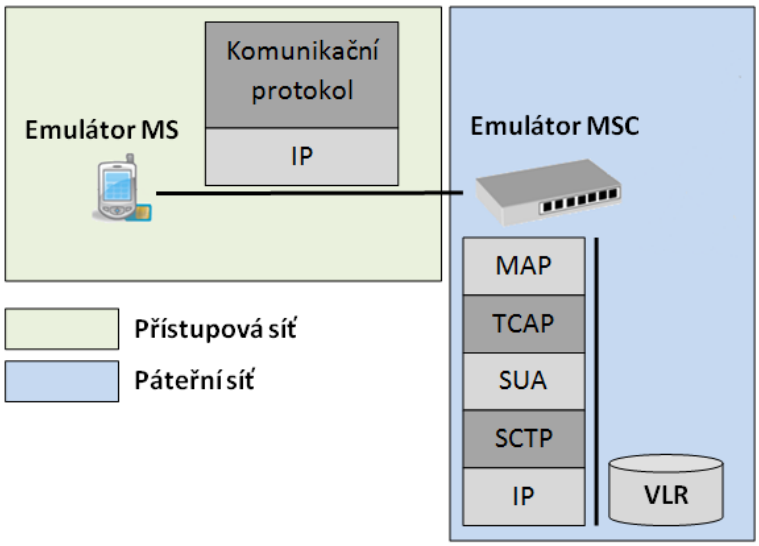
8. Pokud autentizace proběhla úspěšně, zašle MSC mobilní stanici zprávu ***Location Update Accept.*** Během této procedury by mělo být MS přiřazeno *nové TMSI* číslo. K tomu může dojít jedním ze dvou způsobů:
    a. MSC ho pošle jako jeden z parametrů zprávy *Location Update Accept*.
    b. *TMSI* bude přiřazeno za pomoci zprávy *TMSI_REAL_CMD*.
9. BSS subsystém přepošle zprávu ***Location Update Accept*** MS.
10. Mobilní stanice odpoví zasláním zprávy ***TMSI Reallocation Complete***, kterou potvrzuje přijetí nového *TMSI* čísla.
11. BSS poté pošle mobilní stanici zprávu ***Channel Release***, která slouží ke zrušení SDCCH kanálu. Pro MS to znamená, že *Location Update* procedura proběhla úspěšně a proto se ukončí své spojení s BSS subsystémem a přejde do stavu *idle*.
12. Nová MSC/VLR musí HLR databázi poslat zprávu ***Update Location***.
13. HLR databáze odpoví zprávou ***Update Acknowledgement*** a aktualizuje svou databázi o mobilní stanici.
14. HLR databáze pošle ***Cancel Location*** zprávu staré MSC/VLR ústředně.
15. Ta, po jejím přijetí, smaže všechny záznamy o mobilní stanci a její *TMSI* číslo uvolní k dalšímu použití. Poté pošle ***Cancel Location Result*** zprávu zpět HLR databázi.



Obrázek 12.5 - Location Update

13 Emulátor

Obrázek 13.1 schematicky naznačuje *Emulátor mobilní telefonní ústředny* (dále jen *Emulátor*). Jeho činnost lze rozdělit na dvě části – operace v přístupové síti a operace v páteřní síti.



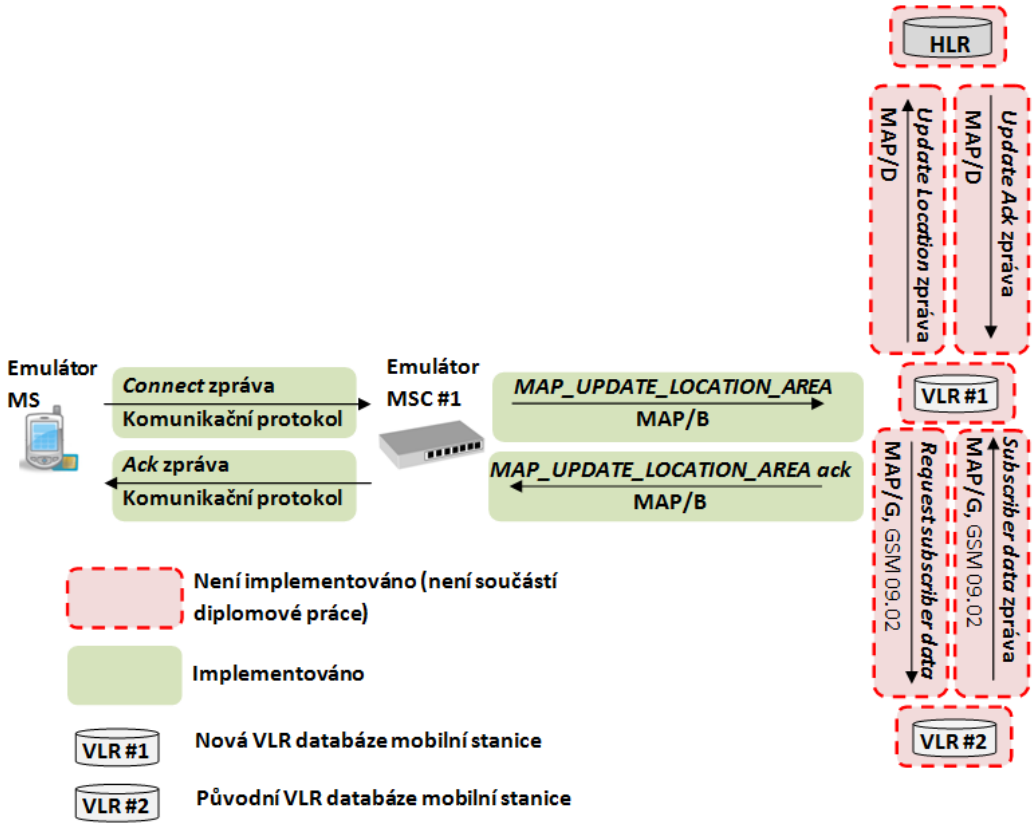
Obrázek 13.1 - Struktura *Emulátoru* a používané protokoly

13.1 Zasílané zprávy

Obrázek 13.2 schematický naznačuje zprávy, které jsou v průběhu přihlášení mobilní stanice (*Emulátoru MS*) posílány. Podrobný popis posílaných zpráv lze nalézt v kapitole 13.5.

Mezi *Emulátorem MS* a *Emulátorem* jsou zasílány dvě zprávy – *Connect* a *Ack*. Zpráva *Connect* slouží k vyjádření požadavku na přihlášení MS do sítě. Následuje zpráva *Ack*, která potvrzuje její přijetí. Jejím odesláním komunikace mezi touto dvojicí entit končí.

Mezi *Emulátorem* a VLR databází jsou zasílány dvě zprávy - MAP_UPDATE_LOCATION_AREA a MAP_UPDATE_LOCATION_AREA ack. První zpráva z této dvojice slouží k zaslání požadavku na aktualizaci údajů o pozici mobilní stanice, které jsou uloženy ve VLR databází (informace v HLR databázi aktualizuje VLR databáze sama). Druhá zpráva slouží k potvrzení úspěšného provedení operace *Location Update*.



Obrázek 13.2 - Zasílané zprávy v aplikaci

13.2 Komunikační protokol

Pro komunikaci mezi *Emulátorem mobilní stanice* a *Emulátorem* je nutné navrhnout komunikační protokol. Ten běží nad TCP/IP stackem. Inspirací při jeho návrhu byl podoba SCTP protokolu.

13.2.1 Obecná struktura zpráv

Obrázek 13.3 ukazuje obecnou strukturu paketu, ve kterém jsou přenášeny zprávy protokolu. Každá zpráva se skládá ze dvou částí:

1. Společná hlavničky
2. Přenášených parametrů

Společná hlavička je povinná pro všechny přenášené zprávy. Má pevně definovanou strukturu o délce 32 bitů a nachází se na začátku paketu. Skládá se ze dvou parametrů – *typ_operace* a *délka_paketu*.

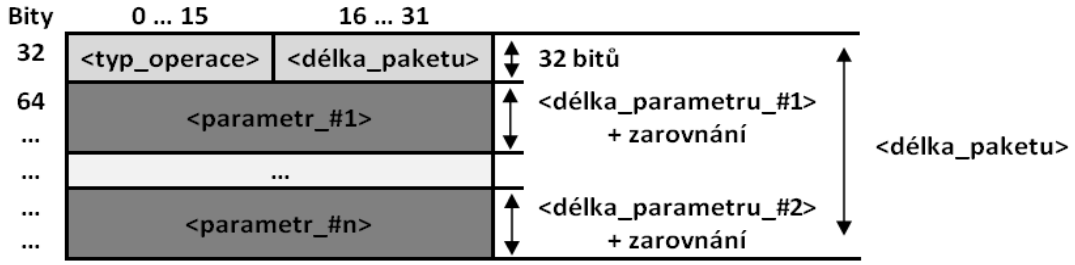
Typ_operace je 16bitová hodnota, která reprezentuje typ přenášené zprávy. V tuto chvíli jsou definovány pouze dvě operace (viz Tabulka 13.1), protokol je ale navržen tak, aby mohl být dále rozšiřován.

Typ operace	Hodnota (hexa)	Popis
Ack	0x00	Tato zpráva slouží k potvrzování přijetí zprávy (identifikace potvrzované zprávy je posílána jako parametr zprávy).
Connect	0x01	Tato zpráva slouží k připojení emulátoru mobilní stanice k

		emulátoru mobilní telefonní ústředny.
Dial	0x02	Tato zpráva slouží k založení telefonního hovoru.

Tabulka 13.1 - Typy zpráv definovaných komunikačním protokolem

Délka_paketu je 16bitová hodnota, ve které je uložena velikost celého přenášeného paketu – tedy délky hlavičky (vždy 32 bitů) a velikosti přenášených parametrů.



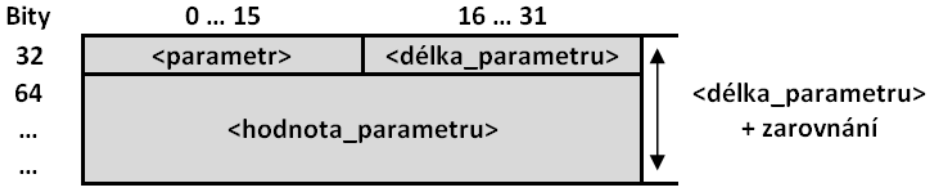
Obrázek 13.3 - Obecná struktura paketu komunikačního protokolu

Protože každá operace vyžaduje rozdílné parametry, následuje za *obecnou hlavičkou* volitelný seznam parametrů. Každý parametr je přenášen zvlášť a je přenášen ve formátu *Tag-Length-Value* – tedy jméno parametru, následuje délka přenášeného parametru a nakonec vlastní hodnota (viz Obrázek 13.4).

Hodnota ***parametr*** specifikuje, o jaký parametr se jedná. Pro každý typ zprávy je specifikována jiná sada parametrů.

Délka_parametru nese velikost přenášeného parametru – tedy součet velikostí polí *parametr*, *délka_parametru* a *hodnota_parametru*.

Pole ***hodnota_parametru*** nese vlastní data přenášeného parametru. Pokud jsou data nezarovnaná na hodnotu 4 bajtů, musí se použít zarovnání (viz kapitola 13.2.2).



Obrázek 13.4 - Struktura pro přenos parametru

13.2.2 Zarovnání

Všechny přenášené zprávy musejí být zarovnány na délku násobků čtyř bajtů. Pokud nejsou přenášena data na tuto hodnotu zarovnána, musí se provést zarovnání. Při jeho provádění narazíme na dva problémy, které musí protokol definovat:

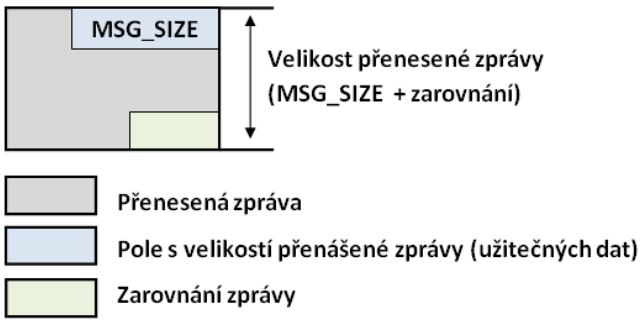
1. Jakou hodnotou se bude zarovnávat
2. Jakým způsobem se zarovnání provede

Pro doplnění přenášených užitečných dat na zarovnávanou velikost je nutné definovat určitý znak, který nazveme *zarovnávací znak*. V případě, že existuje mechanizmus, jak odlišit zarovnávací část od užitečných dat, může být jako *zarovnávací znak* zvolen libovolný znak z přenášené abecedy (v tomto případě na jeho hodnotě nezáleží, protože se na straně příjemce dají lehce oddělit od

zprávy). V opačném případě buďto nesmí být *zarovnávací znak* z přenášené abecedy, nebo musí existovat mechanizmus, jak odlišit, zda je znak použit ve významu *zarovnávacího znaku* nebo ve svém původním významu.

Zarovnání můžeme provést několika způsoby:

1. Přenášená data zarovnáme na požadovanou délku přidáním *zarovnávacích znaků.* Příjemce potom musí tyto dvě části od sebe oddělit. Tento způsob je z hlediska přenášených znaků nejúspornější, vyžaduje ovšem, aby byl *zarovnávací znak* odlišitelný od znaků přenášené abecedy.
2. Další možnost již využívá pole, které příjemce informuje o struktuře přenesené zprávy (říká mu, jak od sebe oddělit výplňkovou část od užitečných dat). Nejprve se přenášená zpráva prodlouží přidáním jednoho *zarovnávacího znaku* na její konec. Díky tomu jsou přenášené zpráva vždy zarovnávány (neexistuje případ, kdy by se zpráva skládala pouze z dat, které je nutné přenést). Výhodou je zajištění jednotného přístupu při zpracování zprávy na úkor efektivnosti využití přenosových linek.
3. Pokud je zpráva již zarovnána, nedochází u ní k žádné další změně. V opačném případě se na konec zprávy přidávají *zarovnávací znaky*, následované jejich počtem
4. Další možností, která je využita i v navrženém komunikačním protokolu, je mít pole, udržující délku užitečných dat (na rozdíl od předcházejících případů, kdy se přenášel počet přidaných *zarovnávacích znaků*). Toto pole má ve zprávě přesně stanovenou pozici a velikost a je přítomno vždy, tedy i v případě, kdy k zarovnání nedochází. Konec zprávy je doplněn zarovnávacími znaky tak, aby velikost zprávy byla násobkem hodnoty čtyř bajtů (32 bitů, viz Obrázek 13.5). Potom se počet zarovnávacích znaků získá odečtením velikosti přenesené zprávy od hodnoty uložené v tomto poli.



Obrázek 13.5 - Princip zarovnávání použitý v komunikačním protokolu

13.2.3 Přenášené zprávy

V současné době jsou specifikovány pouze tři typy zpráv – *Ack, Connect* a *Dial*. Komunikace se skládá vždy z dvojice zasílaných zpráv – *požadovaná operace, potvrzení přijetí zprávy*.

13.2.3.1 Ack zpráva

Zpráva *Ack* slouží k potvrzení přijetí zpráv. Tabulka 13.2 shrnuje všechny parametry zprávy *Ack*.

Typ operace	Hodnota (hexa)	Popis
MSG	0x01	Jedná se o identifikátor, který slouží k identifikaci typu potvrzované zprávy.

Tabulka 13.2 - Parametry zprávy *Ack*

13.2.3.2 Connect zpráva

Zpráva *Connect* slouží k připojení *emulátoru mobilní stanice* k *Emulátoru*. Mezi nejdůležitější parametry zprávy patří zejména parametry *IMSI* a *TMSI*. Oba slouží k identifikaci mobilní stanice. Protokol ale definuje i další parametry zprávy, které slouží zejména pro autentizaci. Ty nejsou v emulátoru implementovány, protože se předpokládá, že autentizace proběhla již na úrovni BSC/BTS ↔ MS. Tabulka 13.3 shrnuje všechny parametry zprávy *Connect*.

Typ operace	Hodnota (hexa)	Popis
IMSI	0x01	V tomto parametru se přenáší hodnota IMSI mobilní stanice (MS), která slouží k její identifikaci (viz kapitola 4.1).
TMSI	0x02	V tomto parametru se přenáší hodnota TMSI mobilní stanice (MS), která slouží k její identifikaci (viz kapitola 4.2).
IMEI	0x03	Přenos IMEI čísla pro potřeby EIR databáze (viz kapitola 4.5).
RAND	0x04	Náhodné číslo, které je generováno autentizačním centrem (AuC) v průběhu autentizačního procesu (viz kapitola 5.4).
SRES	0x05	Odpověď MS na přijaté *RAND* číslo. Používá se v autetnizačním procesu (viz kapitola 5.4).

Tabulka 13.3 - Parametry zprávy *Connect*

13.2.3.3 Dial zpráva

Zpráva *Dial* slouží k založení telefonního hovoru. Důležitým parametrem zprávy je hodnota MSISDN volané mobilní stanice. Tabulka 13.4 shrnuje všechny parametry zprávy *Dial*.

Typ operace	Hodnota (hexa)	Popis
MSISDN	0x01	MSISDN číslo volané mobilní stanice. Maximální délka je 15 číslic/bajtů (viz kapitola 4.3).

Tabulka 13.4 - Parametry zprávy *Dial*

13.3 Konfigurační soubor

Emulátor při své činnosti komunikuje s několika různými entitami. S každou z těchto entit musí navázat spojení, a proto je nutné předat mu informace nezbytné k jejich identifikaci. Mezi tyto entity patří:

1. *Emulátor mobilní stanice*
2. VLR databáze

Pro připojení *emulátoru mobilní stanice* je nutné znát pouze číslo TCP portu, na kterém *Emulátor* naslouchá. Pro spojení s VLR databází je nutné kromě čísla SCTP portu znát i hodnota IP adresy.

Tyto hodnoty jsou uloženy v konfiguračním souboru, který *emulátor* načte při svém spuštění. Jeho název je předán jako parametr aplikace při spuštění (s přepínačem `-c`). Pokud není název konfiguračního souboru předán, potom se *Emulátor* pokusí načíst konfiguraci ze souboru

s implicitním jménem *config*. Pokud i to selže, potom aplikace nemůže pokračovat ve své činnosti a skončí s chybovým hlášením (viz kapitola 13.6).

Tabulka 13.5 shrnuje a popisuje (včetně příkladu) všechny definované parametry, které se v konfiguračním souboru vyskytují. Syntaxe pro zápis parametrů je definována jako dvojice hodnot <*název_parametru*> <*hodnota_parametru*>. Parametry *MS_PORT* a *VLR_PORT* jsou povinné, parametr *VLR_IP* je volitelný a v případě, že není přítomen, je jeho hodnota implicitně nastavena na hodnotu `localhost`.

Pokud se na řádku vyskytuje znak středníku (‚`;`‘), potom je zbytek řádku považován za komentář a je při činnosti *Emulátoru* ignorován.

Parametr	Popis	Příklad	Defaultní hodnota
MS_PORT	Hodnota TCP portu, který *Emulátor mobilní stanice* používá k připojení k *Emulátoru.*	`35258`	-
VLR_PORT	Hodnota SCTP portu, kterou použije MSC k připojení k VLR databázi.	`35259`	-
VLR_IP	IP adresa přidružené VLR databáze.	`10.0.0.17`	`localhost`

Tabulka 13.5 – Parametry konfiguračního souboru

Příklad konfiguračního souboru:

```
MS_PORT         35258       ; TCP port pro komunikaci s MS
VLR_PORT        35259       ; SCTP port pro komunikaci s VLR databází
VLR_IP          10.0.0.17   ; IP adresa pro komunikaci s VLR databází
```

13.4 Parametry *Emulátoru*

Emulátor má definovánu sadu přepínačů, které slouží k předání parametrů nutných k jeho činnosti. Tabulka 13.6 popisuje jejich význam včetně jejich parametrů.

Přepínač	Argument	Význam
`-h`	-	Vytiskne nápovědu *Emulátoru* na standardní výstup a ukončí činnost *Emulátoru*.
`-c`	<*konfigurační_soubor*>	Předá *Emulátoru* název konfiguračního souboru (viz kapitola 13.3).

Tabulka 13.6 - parametry *Emulátoru*

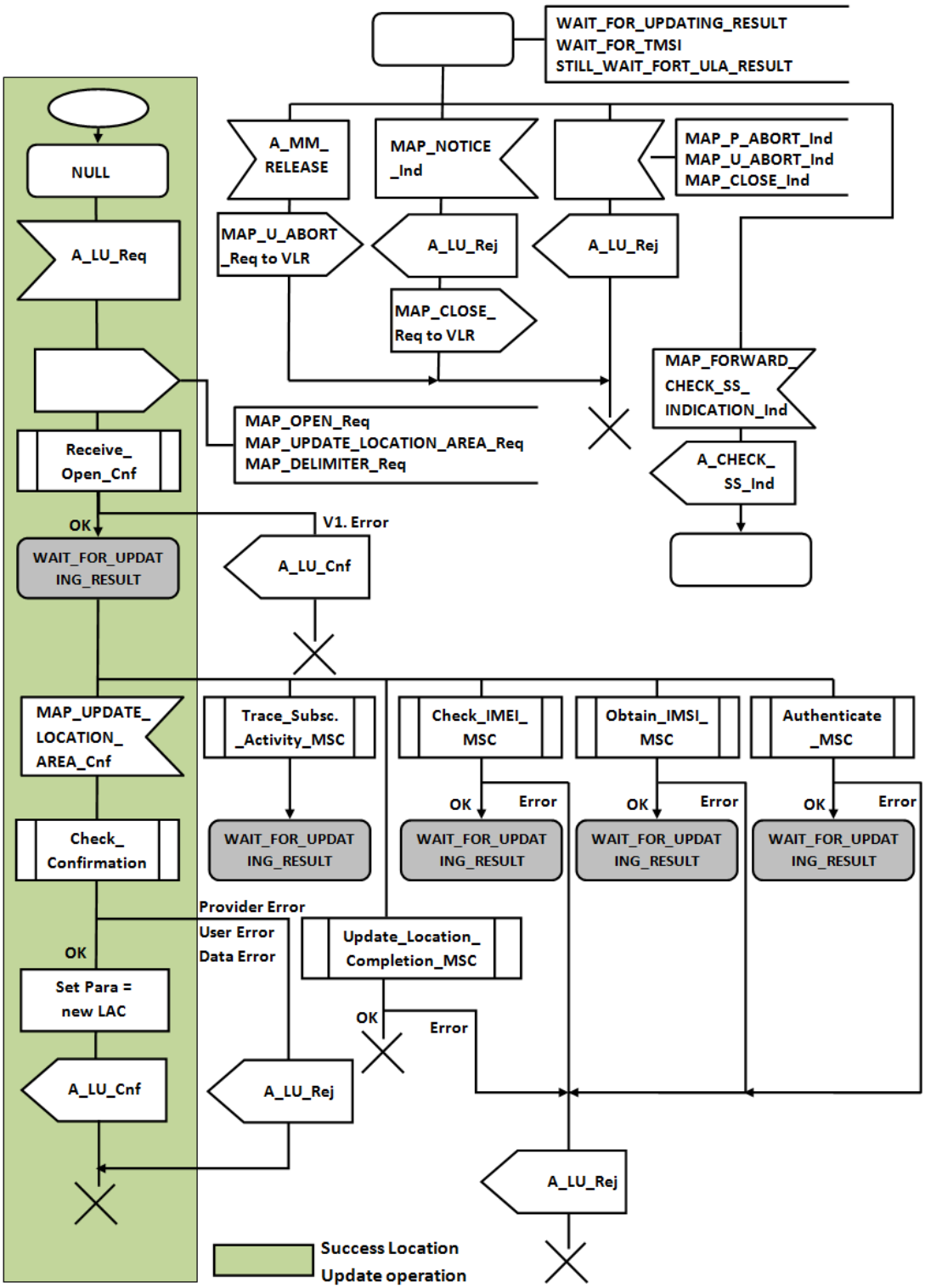
13.5 Činnost emulátoru

Emulátor sám o sobě nic nedělá, pouze reaguje na vnější události, které generuje *emulátor mobilní stanic*e. Požadovanou funkcí *Emulátoru* je provést operaci *Location Update* (viz kapitola 12.4.4).

Po zapnutí se emulátor pokusí načíst konfigurační soubor (viz kapitola 13.3) a zjistit tak svou konfiguraci. Pokud mu jeho název nebyl předán jako parametr, pokusí se načíst konfiguraci z defaultního konfiguračního souboru. Pokud i to skončí neúspěchem, *Emulátor* ukončí svou činnost s chybovým hlášením.

Jakmile se emulátor inicializuje, začne naslouchat na daném portu (parametr MS_PORT) a čeká na připojení *emulátoru mobilní stanice*. Během tohoto čekání nevykonává žádnou činnost.

13.5.1 Činnost MSC během Location update požadavku



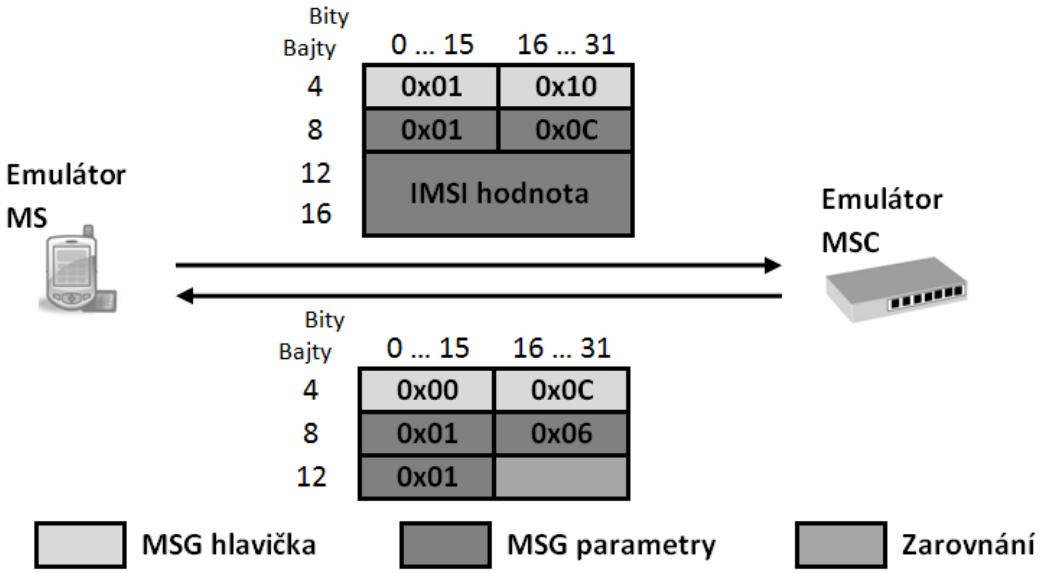
Obrázek 13.6 - Činnost MSC během Location Update požadavku, převzato z [17], přepracováno

Obrázek 13.6 představuje stavový diagram popisující činnost MSC během přijetí požadavku na *Location Update*. Zeleně je vyznačena větev diagramu, která popisuje úspěšné proběhnutí operace. Tato část se překrývá s činností *Emulátoru*.

13.5.2 Komunikace v přístupové síti

Obrázek 13.7 ukazuje, které zprávy jsou zasílány v přístupové síti. Jakmile se *Emulátor mobilní stanice* připojí k *Emulátoru*, zašle zprávu typu *CONNECT* (typ zprávy 0x01) o celkové délce šestnácti bajtů. Parametrem této zprávy je hodnota IMSI čísla mobilní stanice (typ parametru 0x01).

Emulátor potvrdí přijetí zasláním zprávy typu *ACK* (typ zprávy 0x00) o celkové délce dvanácti bajtů. Jediný parametr, který má tato zpráva definovaný je typ zprávy, který potvrzuje. V tomto případě je tedy zasílaný parametr (s hodnotou 0x01) naplněn identifikátorem typu zprávy *CONNECT* (hodnotou 0x01). Tuto zprávu je nutné zarovnat, protože hodnota parametru je definována pouze jako dvoubajtová. Proto se musí poslední dva bajty zprávy vyplnit *zarovnávacími znaky* (viz kapitola 13.2.2).



Obrázek 13.7 - Zprávy zasílané v přístupové síti

13.5.3 Komunikace v páteřní síti

Činnost MSC v průběhu operace *location update* je popsána v kapitole 13.5.1. Oproti ní *Emulátor* implementuje pouze část funkcionality a to pouze úspěšné provedení této operace. Obrázek 13.8 ukazuje zasílané MAP primitiva, která jsou posílána v páteřní síti, včetně jejich parametrů.

Reakcí na přijetí zprávy typu *CONNECT* od *Emulátoru mobilní stanice* je zahájení operace *Location Update* ve spolupráci s VLR databází. Nejprve musí MSC otevřít *MAP dialog* směrem k VLR databázi (provést *opening* sekvenci). To učiní zasláním trojice primitiv MAP_OPEN request, MAP_UPDATE_LOCATION_AREA request a MAP_DELIMITER request.

MAP_OPEN request je zasílán bez service-user parametrů. Zaslány jsou tedy pouze dva parametry (které jsou povinné) – *Application context name* a *Destination address*.

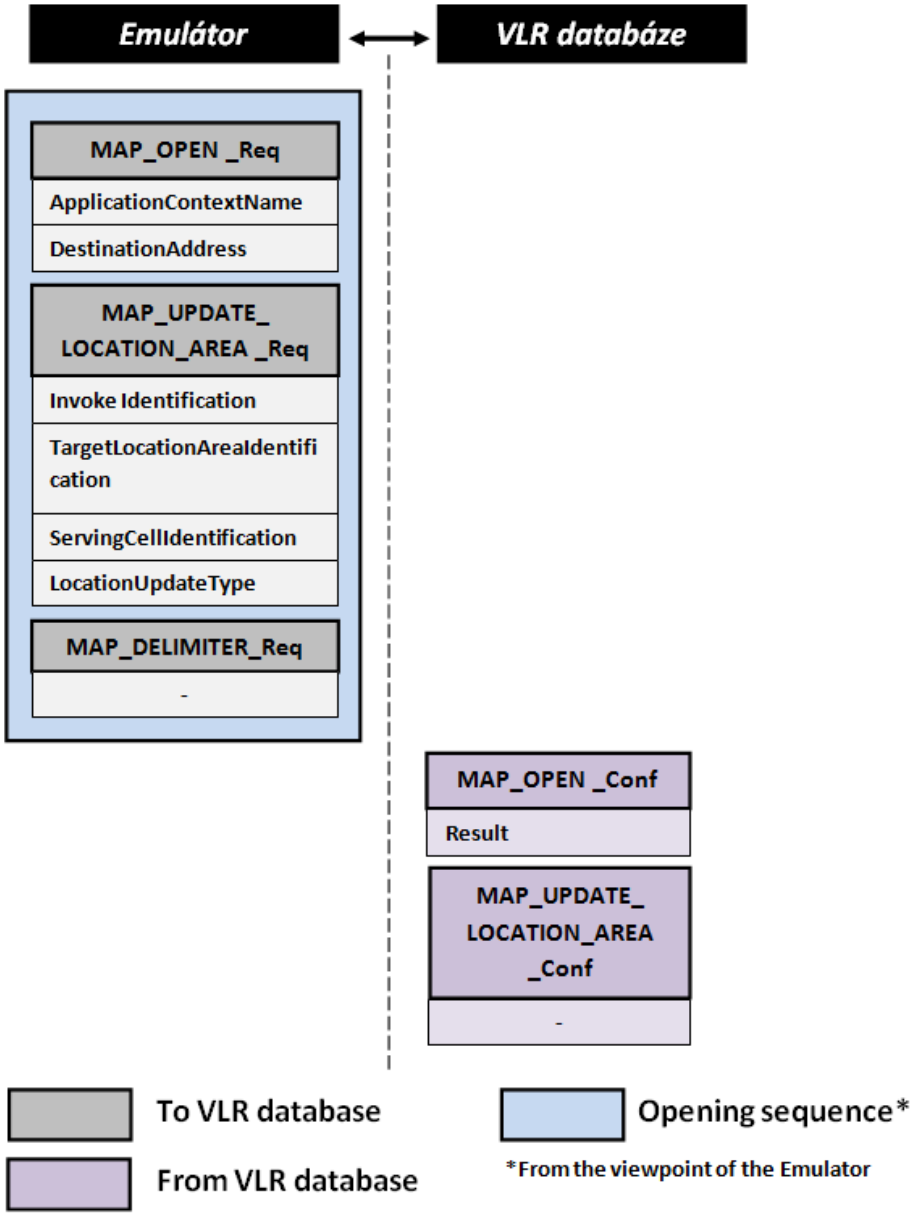
Jako další pošle MSC primitivum **MAP_UPDATE_LOCATION_AREA request**, ve kterém pošle informace získané ze zprávy A_LU_REQUEST (informace získané od MS nebo BSS).

Posledním primitivem *opening* sekvence je **MAP_DELIMITER request**. Ta nemá žádné definované parametry a slouží k explicitnímu vyjádření požadavku na odeslání MAP dat.

Nyní musí *Emulátor* počkat na odpověď VLR databáze. Ta odpovídá zasláním primitiva **MAP_OPEN confirmation** (v případě přijetí *MAP dialogu*). Jeho parametr *Result* má nastavenou hodnotu na *Dialogue Accepted*.

VLR databáze poté pošle primitivum **MAP_UPDATE_LOCATION_AREA confirmation** bez parametrů (čímž vyjadřuje úspěšné provedení LU operace).

Emulátor nakonec zahájí *closing* sekvenci, kterou uzavře *MAP dialog* a dokončí tak svou činnost související s *location update* operací.



Obrázek 13.8 - zasílaná MAP primitiva s jejich parametry při komunikaci v páteřní síti

Tabulka 13.7 ukazuje konverzi jmen použitých primitiv. Kompletní algoritmus pro převod jmen mezi MAP protokolem a TC částí popisuje příloha 9.

Jméno primitiva	Název použitý v síti
MAP_OPEN request	MAP_OPEN_Req
MAP_OPEN confirm	MAP_OPEN_Conf
MAP_DELIMITER request	MAP_DELIMITER_Req
MAP_UPDATE_LOCATION_AREA request	MAP_UPDATE_LOCATION_AREA_Req
MAP_UPDATE_LOCATION_AREA confirm	MAP_UPDATE_LOCATION_AREA_Conf

Tabulka 13.7 - Konverze jmen MAP primitiv

Komunikace v páteřní síti není v *Emulátoru* implementována.

13.6 Chybové stavy

Během své činnosti se *Emulátor* dostat do stavu, ve kterém již není schopen dále pokračovat. Pokud k tomu dojde, vypíše na standardní chybový výstup (*stderr*) typ chyby s krátkým popisem a ukončí svou činnost.

Chyba se vypisuje jako trojice *<číselná_hodnota_chybového_stavu> <název_chybového_stavu> <popis_chybového_stavu>*.

Tabulka 13.8 popisuje definované prefixy jednotlivých chybových kategorií. Jedná se o hodnotu, kterou chybové stavy dané kategorie začínají.

Kategorie	Prefix (hexa)	Popis
Input	0x00	Tato kategorie zahrnuje chyby ve vstupu *Emulátoru* – jedná se o špatně zadané parametry při spuštění, chybějící parametry programu…
Config	0x0A	Zde spadají chybové stavy související s konfiguračním souborem.
Socket	0x14	Zde spadají chybové stavy, které souvisejí se socketem.

Tabulka 13.8 - Prefixy kategorií chybových stavů

13.6.1 Kategorie input

Do této kategorie spadají chyby, které souvisejí s parametry *Emulátoru*, předané při spuštění (*Emulátoru* byl předán neznámý parametr, atd.), a s chybami spojené s konfiguračním souborem (špatná syntaxe konfiguračního souboru, konfigurační soubor nenalezen, atd.). Tabulka 13.9 shrnuje všechny definované chybové stavy, které do této kategorie spadají.

Chyba	Hodnota (hexa)	Popis
`input_missing_config_file`	0x00	*Emulátoru* nebyl předán soubor s konfigurací a současně nebyl nalezen defaultní konfigurační soubor *config*.
`input_missing_config_file_argument`	0x01	U předaného parametru chybí argument.
`input_unknow_parametr`	0x02	*Emulátoru* byl předán neznámý (neplatný) parametr.

Tabulka 13.9 – Chybové stavy definované v kategorii input

13.6.2 Kategorie config

Do této kategorie spadají chyby související s konfiguračním souborem. Tabulka 13.10 popisuje všechny definované chybové stavy této kategorie.

Chyba	Hodnota (hexa)	Popis
`config_unknow_parameter`	0x0A	V konfiguračním souboru byl nalezen neznámý parametr.
`config_missing_msport`	0x0B	V konfiguračním souboru chybí parametr MS_PORT
`config_missing_vlrport`	0x0C	V konfiguračním souboru chybí parametr VLR_PORT

Tabulka 13.10 - Chybové stavy definované v kategorii config

14 Závěr

Tato práce popisuje strukturu GSM systému, jeho vlastnosti a signalizační protokoly. Umožňuje rychle získat přehled v problematice GSM sítí a dohledat požadované informace. Mezi ně patří GSM identifikátory (IMSI, LAI…), vlastnosti GSM sítě (handover, frekvenční plánování …) či signalizační protokoly (SCTP, MAP…).

Tuto práci lze rozdělit na tři tematické části. První část se zabývá obecným popisem GSM systému. Popisuje jeho strukturu a entity, které jej tvoří.

Druhá část, která je nejobjemnější, se zabývá SS7 signalizací, protokoly rodiny SIGTRAN a MAP protokolem.

V dnešní době se od použití čisté signalizace SS7 upouští. Důvodem jsou vysoké finanční náklady, které použití signalizace SS7 provází – SS7 je licencovaná, je nutné zakoupit specializované zařízení s podporou signalizace SS7 atd. Proto vznikla snaha využít stávající infrastrukturu, která je založena na využití IP protokolu. Tyto zařízení jsou velmi rozšířené a proto i velmi levné (v porovnání s SS7 zařízeními). Výhodou je také nižší komplikovanost protokolu a vyšší povědomí veřejnosti o něm. Výsledkem těchto snah je vznik rodiny protokolů SIGTRAN, které umožňují přenášet signalizaci SS7 po IP sítích.

Práce se také výrazně zabývá popisem protokolu *Mobile Application Part (MAP)*, který přináší podporu mobility uživatelů sítě (implementuje operace jako handover, location update atd.). Popisuje obecnou strukturu MAP zpráv, *MAP dialog* a kategorie MAP služeb. Hlavní pozornost je však věnována procedurám podporující operaci *Location Update*. Jedná se o služby z kategorie *common*, které slouží k založení a řízení *MAP dialogu* a službu MAP_LOCATION_UPDATE_AREA, jejímž iniciátorem je MSC a která slouží k aktualizaci lokačních informací ve VLR databázi.

Třetí, a závěrečná část, se zabývá návrhem a implementací *Emulátoru mobilní* telefonní stanice. Popisuje navržený komunikační protokol, který slouží ke komunikaci mezi *Emulátorem* a *Emulátorem mobilní telefonní stanice*. Tento protokol byl navržen s ohledem na jednoduchost dalšího rozšíření – přidání nových zpráv, nezávislost protokolu na přenášených parametrech zpráv atd. Inspirací při návrhu byl protokol SCTP z rodiny SIGTRAN.

Druhá část popisuje zprávy, které jsou nutné pro vykonání operace *Location Update*. Navržená komunikace mezi *Emulátorem* a VLR databází nebyla implementována, pouze byly sestaveny zprávy, které by měly být posílány.

Jednou z možností, jak rozšířit tuto práci, je rozšířit *Emulátor* tak, aby implementoval celou funkčnost operace *Location Update* (viz Obrázek 13.6) nebo implementoval i některou z další funkčnosti, která je pro MSC definována. Dalším rozšířením může být implementace spolupráce s VLR databází.

Literatura

[1] **Pužmanová, Rita.** *Moderní komunikační sitě od A do Z.* Brno : Computer press, a.s., 2006. ISBN 80-251-1278-0.

[2] **Hanáček, Petr.** BMS 0x4 GSM. *Přednáškový materiál k předmětu Bezdrátové a mobilní sítě.*

[3] **Schiller, Jochen.** *Mobile Communications.* Second Edition. London : Person Education Limited, 2003. ISBN 0-321-12381-6.

[4] **Russell, Travis.** *Signaling system 7.* Fifth edition. místo neznámé : McGraw-Hill Professional, 2006. ISBN 978-0071468794.

[5] CAMEL: An Introduction. *3G4G Wireless Resource Center.* [Online] 25. 7 2004. [Citace: 21. 2 2012.] http://www.3g4g.co.uk/Tutorial/ZG/zg_camel.html.

[6] List of mobile country codes - Wikipedia, The Free Encyclopedia. *Wikipedia - The Free Encyclopedia.* [Online] 21. Duben 2012. [Citace: 1. Květen 2012.] http://en.wikipedia.org/wiki/Mobile_country_codes.

[7] Mobile Network Code - Wikipedia, The Free Encyklopedia. *Wikipedia - The Free Encyklopedia.* [Online] 15. 10 2010. [Citace: 10. 1 2011.] http://en.wikipedia.org/wiki/Mobile_Network_Code.

[8] Mobility management - Wikipedia, The Free Encyklopedia. *Wikipedia - The Free Encyklopedia.* [Online] 5. 10 2010. [Citace: 15. 10 2010.] http://en.wikipedia.org/wiki/TMSI.

[9] MSISDN - wikipedie. *Wikipedie - Otevřená encyklopedie.* [Online] 2012. 2 10. [Citace: 15. 11 2010.] http://cs.wikipedia.org/wiki/MSISDN.

[10] **Dryburgh, Lee a Hewett, Jeff.** *Signaling System No. 7.* [Online kniha] Indianapolis : Cisco Press, 2005. CA 95134-1706.

[11] Location Area Identity - Wikipedia, The Free Encyklopedia. *Wikipedia - The Free Encyklopedia.* [Online] 8. 3 2011. [Citace: 12. 10 2011.] http://en.wikipedia.org/wiki/Location_Area_Identity.

[12] GSM - Addresses and Identifiers. *Tutorials point - Simply Easy Learning.* [Online] [Citace: 1. květen 2012.] http://www.tutorialspoint.com/gsm/gsm_addressing.htm.

[13] International Mobile Equipment Identity - Wikipedia, The Free Encyklopedia. *Wikipedia - The Free Encyklopedia.* [Online] 8. 1 2011. [Citace: 17. 10 2011.] http://en.wikipedia.org/wiki/Imei.

[14] Um interface - Wikipedia, The Free Encyclopedia. *Wikipedia - The Free Encyclopedia.* [Online] 15. 1 2012. [Citace: 21. 2 2012.] http://en.wikipedia.org/wiki/Um_air_interface.

[15] **Sčuglík, František.** Signalizace SS7. *Přednáškové materiály k předmětu Pokročilé komunikační systémy.*

[16] Telephone User Part (TUP) - Wikipedia, the free encyclopedia. *Wikipedia - The Free Encyklopedia.* [Online] 17. 12 2009. [Citace: 5. 1 2011.] http://en.wikipedia.org/wiki/Telephone_User_Part.

[17] *Mobile Application Part (MAP) specification (GSM 09.02).* místo neznámé : European Telecommunications Standards Institute, 1996. TS/SMG-030902Q.

[18] RFC 2960 - Stream Control Transmission Protocol. *IETF Tools.* [Online] 2000. [Citace: 22. leden 2012.] http://tools.ietf.org/html/rfc2960.

[19] Signalling Connection Control Part User Adaptation Layer (SUA). *http://www.ietf.org.* [Online] 2004. [Citace: 13. leden 2012.] http://www.ietf.org/rfc/rfc3868.txt.

[20] IMSI detach. *GSM For Dummies.* [Online] [Citace: 18. 4 2012.] http://gsmfordummies.com/gsmevents/detach.shtml.

[21] Stream Control Transmission Protocol - wikipedie. *Wikipedie - Otevřená encyklopedie.* [Online] 20. 11 2010. [Citace: 3. 1 2011.] http://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol.

[22] Cellular network - Wikipedia, The Free Encyklopedia. *Wikipedia - The Free Encyklopedia.* [Online] 4. 2 2012. [Citace: 20. 3 2012.] http://en.wikipedia.org/wiki/Cell_network.

[23] Handover - Wikipedia, The Free Encyclopedia. *Wikipedia - The Free Encyclopedia.* [Online] 5. 2 2012. [Citace: 21. 3 2012.] http://en.wikipedia.org/wiki/Handoff.

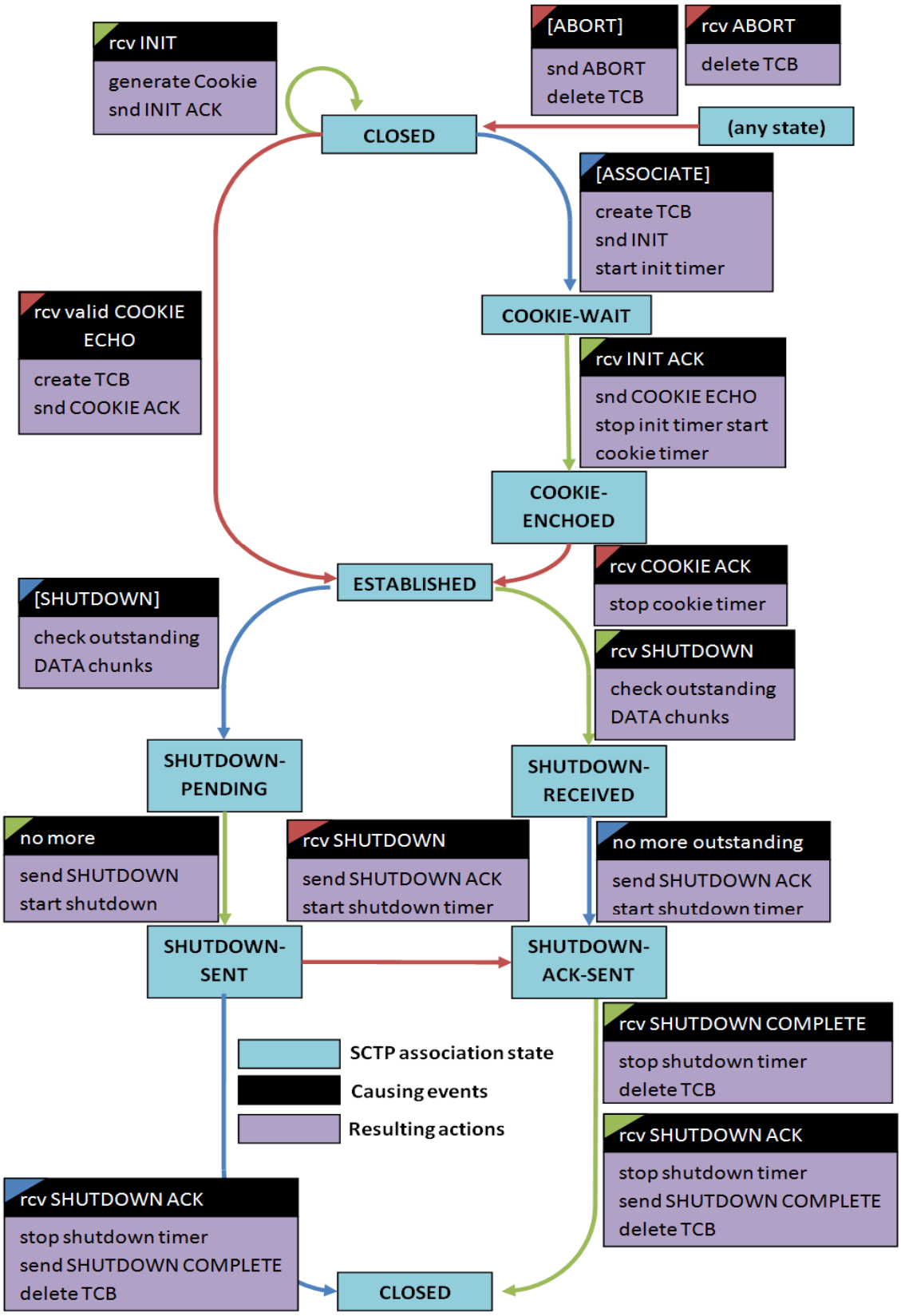
Seznam použitých zkratek

AGCH	Access Grant Channel
AuC	Authentication Center
BCCH	Broadcast Control Channel
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CAMEL	Customized Applications for Mobile network Enhanced Logic
CAS	Channel Associated Signaling
CCCH	Common Control Channels
CCS	Common Channel Signaling
CDMA	Code Division Multiples Access
CdPN	Caller Party Number
CM	Call Management
EIR	Equipment Identification Register
FAC	Final Assembly Code
FACCH	Fast Associated Control Channel
FCCH	Frequency Correction Channel
FCI	Forward Call Indicators
GMSC	Gateway MSC
GSM	Global System for Mobile Communications, původně Groupe Spécial Mobile
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
INAP	Intelligent Network Application Part
INN	Internal Network Number indicator
ISUP	ISDN User Part
IWF	Interworking Functions
LAC	Location Area Code
LAI	Location Area Identity
LMSI	Local Mobile Subscriber Identity
LU	Location Update
MAP	Mobile Application Part
MCC	Mobile Country Code
MM	Mobility Management
MNC	Mobile Nework Code
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
MSISDN	Mobile Station International ISDN number
MSRN	Mobile Subscriber Roaming Number
MTP	Message Transfer Part

NI	Network Identifier
NOC	Nature of connection Indicators
NSS	Network Switching Subsystem
OMC	Operation and Maintenance Center
OSS	Operation Subsystem
PCM	Pulse-code Modulation
PCH	Paging Channel
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RACH	Random Access Channel
RR	Radio Resource Management
RSS	Radio Subsystem
SACCH	Slow Associated Control Channel
SCCP	Signaling Connection Control Part
SDCCH	Standalone Dedicated Control Channel
SCH	Synchronization Channel
SIM	Subscriber Identity Module
SN	Subscriber Number
SPC	Signaling Point Code
SS7	Signaling System No. 7
TAC	Type Allocation Code
TC	Transaction Capabilities
TCAP	Transaction Capabilities Application Part
TCB	Transmission Control Block
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TMR	Transmission Medium Requirement
TMSI	Temporary Mobile Subscriber Identity
TUP	Telephone User Part
UMTS	Universal Mobile Telecommunications System
USI	User Service Information
VLR	Visitor Location Register

Seznam příloh

Příloha 1. Diagram stavů SCTP asociace



Tento stavový diagram ukazuje změny stavů SCTP asociace, kterými během svého života prochází. Nezachycuje všechny stavové chyby, které mohou nastat (např. nerozpoznaný typ chunku či neplatné parametry asociace při inicializaci).

Stavový diagram používá následující syntaxi. Každý přechod mezi stavy je barevně značen. Podle této barvy lze poznat příslušnou dvojici *spouštěcí událost / odpovídající akce*. Názvy chunku jsou psány kapitálkami, názvy parametrů jsou psány kurzívou. Například tak `rcv SHUTDOWN ACK` značí přijetí chunku typu SHUTDOWN ACK zatímco *State Cookie* značí parametr.

Příloha 2. GSM MAP operace

Operation	Binary Code							
Location Registration Operations								
UpdateLocation	0	0	0	0	0	0	1	0
CancelLocation	0	0	0	0	0	0	1	1
PurgeMS	0	1	0	0	0	0	1	1
SendIdentification	0	0	1	1	0	1	1	1
GPRS Location Registration Operations								
UpdateGprsLocation [3G]	0	0	0	1	0	1	1	1
Subscriber Information Enquiry Operations								
ProvideSubscriberInfo [3G]	0	1	0	0	0	1	1	0
Any Time Information Enquiry Operations								
AnyTimeInterrogation [3G]	0	1	0	0	0	1	1	1
Any Time Information Handling Operations								
AnyTimeSubscriptionInterrogation [3G]	0	0	1	1	1	1	1	0
AnyTimeModification [3G]	0	1	0	0	0	0	0	1
Subscriber Data Modification Notification Operations								
NoteSubscriberDataModified [3G]	0	0	0	0	0	1	0	1
Handover Operations								
PerformHandover [P1]	0	0	0	1	1	1	0	0
PrepareHandover	0	1	0	0	0	1	0	0
SendEndSignal	0	0	0	1	1	1	0	0
ProcessAccessSignaling	0	0	1	0	0	0	1	0
ForwardAccessSignaling	0	0	1	0	0	0	1	0
PerformSubsequentHandover [P1]	0	0	0	1	1	1	1	0
PrepareSubsequentHandover	0	1	0	0	0	1	0	1
Authentication Management Operations								
SendAuthenticationInfo	0	0	1	1	1	0	0	0
AuthenticationFailureReport [3G]	0	0	0	0	1	1	1	1
IMEI Management Operations								
CheckIMEI	0	0	1	0	1	0	1	1
Subscriber Management Operations								
SendParameters [P10]	0	0	0	0	1	0	0	1
InsertSubscriberData	0	0	0	0	0	1	1	1
DeleteSubscriberData	0	0	0	0	1	0	0	0
Fault Recovery Management Operations								
Reset	0	0	1	0	0	1	0	1
ForwardChecksIndication	0	0	1	0	0	1	1	0
RestoreData	0	0	1	1	1	0	0	1
GPRS Location Information Retrieval Operations								
SendRoutingInfoForGprs [3G]	0	0	0	1	1	0	0	0
Failure Reporting Operations								
FailureReport [3G]	0	0	0	1	1	0	0	1
GPRS Notification Operations								
NoteMsPresentForGprs [3G]	0	0	0	1	1	0	1	0
Mobility Management Operations								
NoteMmEvent [3G]	0	1	0	1	1	0	0	1
Operation and Maintenance Operations								

ActivateTraceMode	0	0	1	1	0	0	1	0
DeactivateTraceMode	0	0	1	1	0	0	1	1
TraceSubscriberActivity [P10]	0	1	0	1	0	0	1	0
NoteInternalHandover [P10]	0	0	1	1	0	1	0	1
SendIMSI	0	0	1	1	1	0	1	0
Call Handling Operations								
SendRoutingInfo	0	0	0	1	0	1	1	0
ProvideRoamingNumber	0	0	0	0	0	1	0	0
ResumeCallHandling [3G]	0	0	0	0	0	1	1	0
ProvideSIWFSNumber [3G]	0	0	0	1	1	1	1	1
Siwfs-SignallingModify [3G]	0	0	1	0	0	0	0	0
SetReportingState [3G]	0	1	0	0	1	0	0	1
StatusReport [3G]	0	1	0	0	1	0	1	0
RemoteUserFree [3G]	0	1	0	0	1	0	1	1
Ist-Alert [3G]	0	1	0	1	0	1	1	1
Ist-Command [3G]	0	1	0	1	1	0	0	0
Supplementary Service Operations								
RegisterSS	0	0	0	0	1	0	1	0
EraseSS	0	0	0	0	1	0	1	1
ActivateSS	0	0	0	0	1	1	0	0
DeactivateSS	0	0	0	0	1	1	0	1
InterrogateSS	0	0	0	0	1	1	1	0
ProcessUnstructuredSsData	0	0	0	1	1	0	0	1
ProcessUnstructuredSsRequest	0	0	1	1	1	0	1	1
UnstructuredSsRequest	0	0	1	1	1	1	0	0
UnstructuredSsNotify	0	0	1	1	1	1	0	1
RegisterPassword	0	0	0	1	0	0	0	1
GetPassword	0	0	0	1	0	0	1	0
BeginSubscriberActivity [P1O]	0	1	0	1	0	1	0	0
SsInvocationNotification [3G]	0	1	0	0	1	0	0	0
RegisterCcEntry [3G]	0	1	0	0	1	1	0	0
EraseCcEntry [3G]	0	1	0	0	1	1	0	1
Short Message Service Operations								
SendRoutingInfoForSM	0	0	1	0	1	1	0	1
ForwardSM	0	0	1	0	1	1	1	0
MtForwardSM [3G]	0	0	1	0	1	1	0	0
ReportSmDeliveryStatusNoteSubscriberPresent [P1O]	0	0	1	0	1	1	1	1
AlertServiceCentreWithoutResult [P1O]	0	1	0	0	1	0	0	0
AlertServiceCentre	0	1	0	0	1	0	0	1
InformServiceCentre	0	0	1	1	1	1	1	1
ReadyForSM	0	1	0	0	0	0	1	0
NoteSubscriberPresent [P1O]	0	1	0	0	1	0	0	0
Group Call Operations								
PrepareGroupCall [3G]	0	0	1	0	0	1	1	1
SendGroupCallEndSignal [3G]	0	0	1	0	1	0	0	0
ProcessGroupCallSignaling [3G]	0	0	1	0	1	0	0	1
ForwardGroupCallSignaling [3G]	0	0	1	0	1	0	1	0
Location Service Operations								
SendRoutingInfoForLCS [3G]	0	1	0	1	0	1	0	1
ProvideSubscriberLocation [3G]	0	1	0	1	0	0	1	1
SubscriberLocationReport [3G]	0	1	0	1	0	1	1	0

Secure Transport Operations								
SecureTransportClass1 [3G]	0	1	0	0	1	1	1	0
SecureTransportClass2 [3G]	0	1	0	0	1	1	1	1
SecureTransportClass3 [3G]	0	1	0	1	0	0	0	0
SecureTransportClass4 [3G]	0	1	0	1	0	0	0	1

Key:

P1O = Specified for use in MAP Phase 1 only (no longer published).

3G = Found in 3GPP R6 MAP Phase 3 specification, but not in ETSI MAP Phase 2.

Převzato z [10]

Příloha 3. Typy TCAP zpráv (ANSI, ITU)

ANSI Package Types	Hex hodnota	Popis
Unidirectional	11100001	Posílána pouze jedním směrem a není očekávána odpověď
Query with Permission	11100010	Zahájení transakce, dává možnost příjemci ukončit transakci
Query without Permission	11100011	Zahájení transakce, bez možnosti
Response	11100100	Ukončení transakce
Conversation with Permission	11100101	Pokračuj v založené transakci, dána možnost přijímací straně ukončit transakci
Conversation without Permission	11100110	Pokračuj v transakci, ale přijímací strana nemá povoleno ukončit transakci
Abort	11110110	Zpráva poslána k informování cíle o okamžitém ukončení transakce bez zaslání jiných zpráv, které by mohly být očekávány (okamžité ukončení transakce, po této zprávě se již nic jiného neposílá)

ITU Typ zprávy	Hex hodnota	Popis
Unidirectional	01100001	Posílána pouze jedním směrem a není očekávána odpověď
Begin	01100010	Zahájení transakce
(Reserved)	01100011	Nepoužito
End	01100100	Konec transakce
Continue	01100101	Pokračuj v založené transakci
(Reserved)	01100110	Nepoužito
Abort	01100111	Zpráva poslána k informování cíle o okamžitém ukončení transakce bez zaslání jiných zpráv, které by mohly být očekávány (okamžité ukončení transakce, po této zprávě se již nic jiného neposílá)

Převzato z [10]

Příloha 4. MAP služby používající parametr *destination-reference*

MAP služba	Typ reference	Použití parametru
MAP-REGISTER-SS	IMSI	Subscriber identity
MAP-ERASE-SS	IMSI	Subscriber identity
MAP-ACTIVATE-SS	IMSI	Subscriber identity
MAP-DEACTIVATE-SS	IMSI	Subscriber identity
MAP-INTERROGATE-SS	IMSI	Subscriber identity
MAP-REGISTER-PASSWORD	IMSI	Subscriber identity
MAP-PROCESS-UNSTRUCTURED-SS-REQUEST	IMSI	Subscriber identity
MAP-UNSTRUCTURED-SS-REQUEST	IMSI	Subscriber identity
MAP-UNSTRUCTURED-SS-NOTIFY	IMSI	Subscriber identity
MAP-FORWARD-SHORT-MESSAGE	IMSI (pozn.)	Subscriber identity

Pozn.: Pouze v případě, kdy MS přijme *IMSI* a *LMSI* čísla společně z HLR databáze v průběhu přenosu SMS zpráv.

Převzato z [17]

Příloha 5. MAP služby používající parametr *originating-reference*

MAP služba	Typ reference	Použití parametru
MAP-REGISTER-SS	ISDN-Address-String	Originated entity address
MAP-ERASE-SS	ISDN-Address-String	Originated entity address
MAP-ACTIVATE-SS	ISDN-Address-String	Originated entity address
MAP-DEACTIVATE-SS	ISDN-Address-String	Originated entity address
MAP-INTERROGATE-SS	ISDN-Address-String	Originated entity address
MAP-REGISTER-PASSWORD	ISDN-Address-String	Originated entity address
MAP-PROCESS-UNSTRUCTURED-SS-REQUEST	ISDN-Address-String	Originated entity address

Převzato z [17]

Příloha 6. Pravidla pro mapování common MAP služeb na TC

MAP service-primitive	TC service-primitive
MAP-OPEN request **(+ any user specific service primitives)** **+ MAP-DELIMITER request**	TC-BEGIN request (+ component handling primitives)
MAP-OPEN response **(+ any user specific service primitives)** **+ MAP-DELIMITER request**	TC-CONTINUE request (note 0) (+ component handling primitives)
(any user specific service primitives) **+ MAP-DELIMITER request**	TC-CONTINUE request (+ component handling primitives)
(any user specific service primitives) **+ MAP-CLOSE request**	TC-END request (+ component handling primitives)
MAP-U-ABORT request	TC-U-ABORT request

TC service-primitive	MAP service-primitive
TC-BEGIN indication **(+ component handling primitives)**	MAP-OPEN indication (+ user specific service primitives) + MAP-DELIMITER indication (note 1)
TC- CONTINUE indication **(+ component handling primitives)**	First time: MAP-OPEN confirm (+ user specific service primitives) + MAP-DELIMITER indication (note 1) Subsequent times: (user specific service primitives) + MAP-DELIMITER indication (note 1)
TC-END indication **(+ component handling primitives)**	MAP-OPEN confirm (note 6) (user specific service primitives) + MAP-CLOSE indication
TC-U-ABORT indication	MAP-U-ABORT indication or MAP-P-ABORT indication (note 2) MAP-OPEN confirmation (note 3)
TC-P-ABORT indication	MAP-P-ABORT indication (note 4) MAP-OPEN confirmation (note 5)

Note 0: Or TC-END if the MAP-CLOSE request has been received before the MAP-DELIMITER request.

Note 1: It may not be necessary to present this primitive to the user for MAP version 2 applications.

Note 2: The mapping depends on whether the TC-U-ABORT indication primitive contains a MAP-abort-PDU from the remote MAP service-provider or a MAP-user-abort-PDU from the remote MAP service-user.

Note 3: Only if the opening sequence is pending and if the "Abort Reason" in the TC-U-ABORT indication is set to "Application Context Not Supported".

Note 4: If the "Abort Reason" in the TC-P-ABORT indication is set to a value different from

"Incorrect Transaction Portion".

Note 5: Only if the opening sequence is pending and if the "Abort Reason" in the TC-P-ABORT indication is set to "Incorrect Transaction Portion".

Note 6: Only if opening sequence is pending.

Převzato z [17]

Příloha 7. Pravidla pro mapování user-specific MAP služeb na TC

MAP service-primitive	TC-service-primitive
MAP-xx request	TC-INVOKE request
MAP-xx response (note 1)	TC-RESULT-L request TC-U-ERROR request TC-U-REJECT request TC-INVOKE request (note 2)

TC-service-primitive	MAP service-primitive
TC-INVOKE indication	MAP-xx indication
TC-RESULT-L indication (note 3) **TC-U-ERROR indication** **TC-INVOKE indication (note 2)** **TC-L-CANCEL indication**	MAP-xx confirm
TC-U-REJECT indication **TC-L-REJECT indication** **TC-R-REJECT indication**	MAP-xx confirm or MAP-NOTICE indication

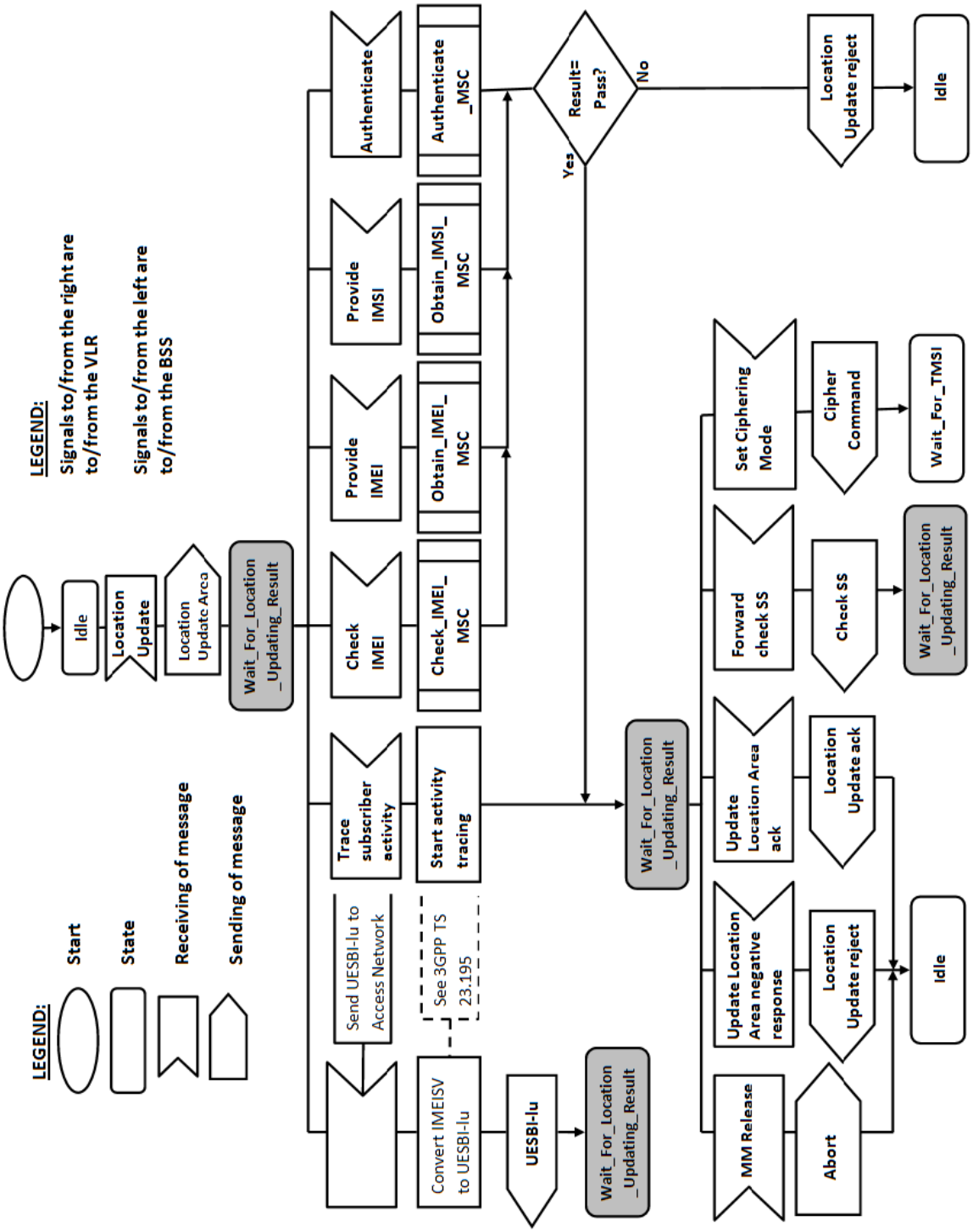
Note 1: The mapping is determined by parameters contained in the MAP-xx response primitive.

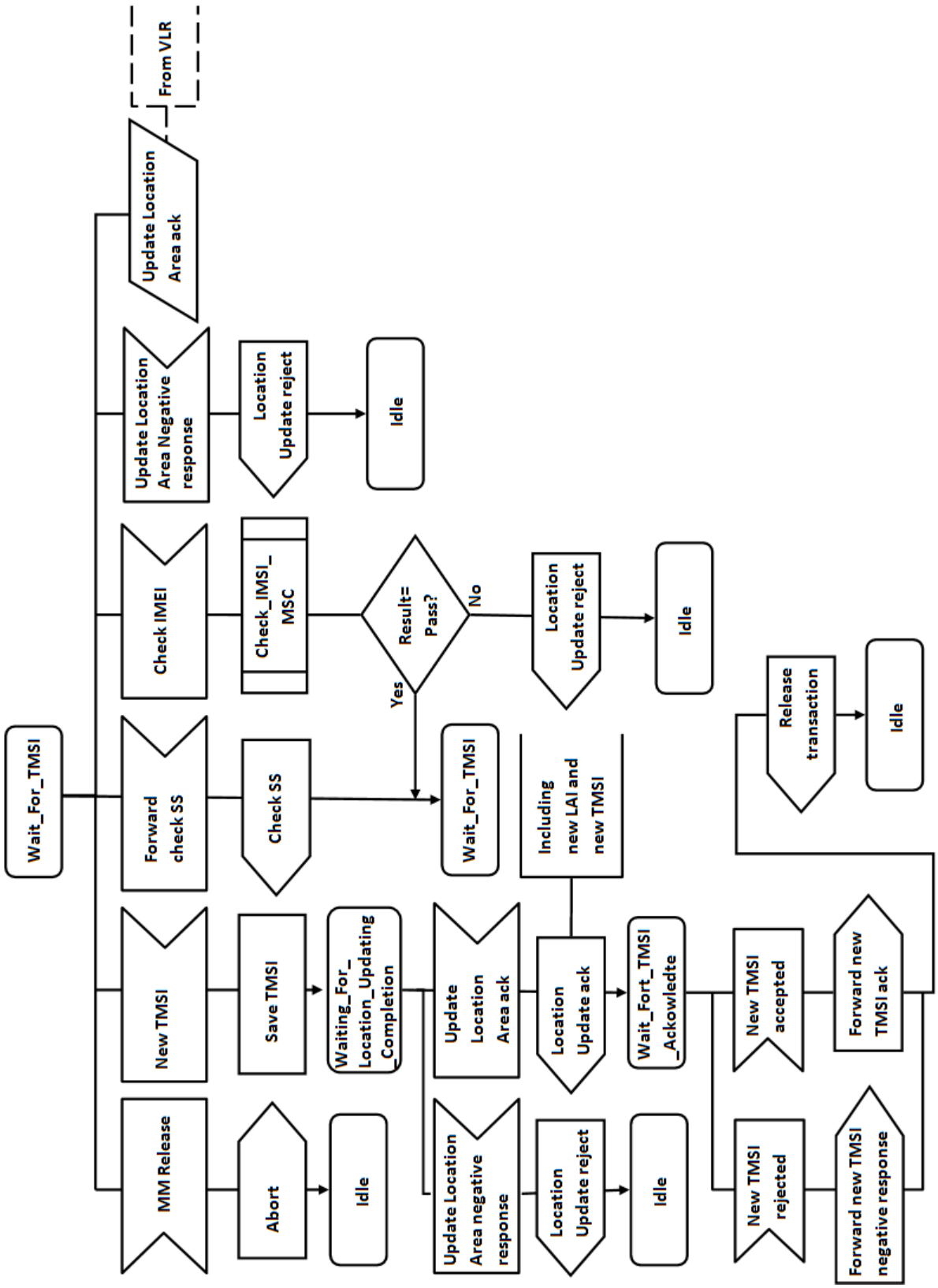
Note 2: This applies only to TC class 4 operations where the operation is used to pass a result of another class 2 or class 4 operation.

Note 3: If RESULT-NL components are present they are mapped on to the same MAP-xx confirm.

Převzato z [17]

Příloha 8. Činnost MSC během Location Update operace





Převzato z [17]

Příloha 9. Naming Conventions

<Event_Name> := <MAP_Primitive> | <External_Event>

<MAP_Primitive> := <PAP_Open> | <MAP_Close> | <MAP_U_Abort> | <MAP_P_Abort> | <MAP_Specific> | <MAP_Notice>

<MAP_Open> := MAP_Open_Req |MAP_Open_Ind |MAP_Open_Rsp | MAP_Open_Cnf

<MAP_Close> := MAP_Close_Req |MAP_Close_Ind

<MAP_U_Abort> := MAP_U_Abord_Req | MAP_U_Abord_Ind

<MAP_P_Abort> := MAP_P_Abort_Ind

<MAP_Notice> := MAP_Notice_Ind

<MAP_Specific> := <MAP_Req> | <MAP_Ind> | <MAP_Rsp> | <MAP_Cnf>

<MAP_Req> := MAP_<Service_Name>_Req

<MAP_Ind> := MAP_<Service_Name>_Ind

<MAP_Rsp> := MAP_<Service_Name>_Rsp_

<MAP_Cnf> := MAP_<Service_Name>_Cnf

<External_Event> := <Interface_Type>_<External_Signal>

<Interface_Type> := I | A | OM | SC | HO_AC | US

<External_Signal> := <Lexical_Unit>

<Service_Name> := <Lexical_Unit>

<Lexical_Unit> := <Lexical_Component> | <Lexical_Unit>_<Lexical_Component>

<Lexical_Component> := <Upper_Case_Letter><Letter_Or_Digit_List>

<Letter_Or_Digit_List> := <Letter_Or_Digit> | <Letter_Or_Digit_List><Letter_Or_Digit>

<Letter_Or_Digit> := <Letter> | <Digit>

<Upper_Case_Letter> := A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z

<Lower_Case_Letter> := A|b|c|d|e|f|g|h|i|j|k|l|m|n|o|p|q|r|s|t|u|v|w|x|y|z

<Digit> := 1|2|3|4|5|6|7|8|9|0

Popis zkratek použitých pro komunikační interface (<Interface_Type>):

"I"	For interfaces to the fixed network. "I" stands for ISUP interface.
"A"	For interfaces to BSS (i.e. A-interfaces);
"OM"	For network management interfaces (communication with OMC, MML interface, ...);
"SC"	For interfaces to a Service Centre
"HO_CA"	For internal interfaces to the Handover Control Application
"US"	For a local USSD application.

Převzato z [17].

Příloha 10. Application Context

Každý *MAP dialog*, který je založen MAP uživatelem služby, je asociován s ***application-context*** (kontextem aplikace). Následující algoritmus slouží k vytvoření *application-context*: [17]

```
APPLICATION-CONTEXT MACRO ::=

BEGIN

      TYPE NOTATION ::= Symmetric | InitiatorConsumerOf
            ResponderConsumerOf | empty

      VALUE NOTATION ::= value(VALUE OBJECT IDENTIFIER)

      Symmetric ::= "OPERATIONS OF" "{" PackageList "}"

      InitiatorConsumeOf ::= "INITIATOR CONSUMER OF" "{"
            PackageList "}"

      ResponderConsumerOf::= "RESPONDER CONSUMER OF" "{"
            PackageList "}" | empty

      PacageList ::= Package | packageList "," Package

      Package ::= value(OPERATION-PACKAGE)
            | type -- shall reference a package type

END
```