IP multimediálny podsystém – IMS – architektúra a koncepcia

DIPLOMOVÁ PRÁCA

Martin Sloboda

ŽILINSKÁ UNIVERZITA V ŽILINE

Elektrotechnická fakulta

Katedra telekomunikácií

Študijný odbor:

TELEKOMUNIKÁCIE

Vedúci diplomovej práce: prof. Ing. Karol Blunár, DrSc.

Stupeň kvalifikácie: inžinier (Ing.)

Dátum odovzdania diplomovej práce: 16.5.2008

ŽILINA 2008

Žilinská univerzita v Žiline | Elektrotechnická fakulta

KATEDRA TELEKOMUNIKÁCIÍ
Univerzitná 1, 010 26 Žilina

Akademický rok 2007/2008

ZADANIE DIPLOMOVEJ PRÁCE

Meno, priezvisko: **Martin Sloboda**

Študijný odbor: **Telekomunikácie**

Téma diplomovej práce: **IP multimediálny podsystém - IMS - architektúra a koncepcia**

Pokyny pre vypracovanie diplomovej práce:

1. Analyzujte architektúru IP multimediálneho podsystému podľa odporúčaní medzinárodných organizácií, ako aj jednotlivé firemné riešenia. Porovnajte vlastnosti.
2. Podrobne rozoberte architektúru a koncepciu IMS relácie.
3. Uvedenú problematiku spracujte formou prednáškového cyklu vhodného pre pracovníkov telekomunikačného sektoru.

Vedúci diplomovej práce: prof. Ing. Karol Blunár, DrSc.,
Katedra telekomunikácií, EF, Žilinská univerzita v Žiline

Dátum odovzdania diplomovej práce: 16. 05. 2008

Žilinská univerzita v Žiline
Elektrotechnická fakulta
KATEDRA TELEKOMUNIKÁCIÍ
Univerzitná 1, 010 26 Žilina

prof. Ing. Milan Dado, PhD.
vedúci katedry

Žilina 26. 10. 2007

Abstrakt

Diplomová práca sa zaoberá popisom IP multimediálneho podsystému (IMS) a vysvetlením už navrhnutej IMS technológie.

V úvodnej časti som sa venoval histórii a vývoju IMS od počiatku, popisu služieb a na čo slúži IMS. Druhá časť podrobnejšie rozoberá architektúru IP multimediálneho podsystému a funkčný opis. Nasledujúca tretia kapitola popisuje koncept pre vytvorenie relácií IMS. A v štvrtej kapitole sa venujem prednáškovým cyklom.

Žilinská univerzita v Žiline, Elektrotechnická fakulta,
Katedra telekomunikácií a multimédií

ANOTAČNÝ ZÁZNAM - DIPLOMOVÁ PRÁCA

Priezvisko, meno: Martin Sloboda akademický rok: 2007/2008

Názov práce: **IP multimediálny podsystém – IMS – architektúra a koncepcia**

Počet strán: 164	Počet obrázkov: 47	Počet tabuliek: 18
Počet grafov: 0	Počet príloh: 0	Použitá lit.: 45

Anotácia (slov. resp. český jazyk):

Diplomová práca sa zaoberá vysvetlením IP multimediálneho podsystému (IMS). Sú charakterizované základné vlastnosti a funkcie IMS. Jadro práce spočíva v podrobnom popise jednotlivých funkčných častí architektúry a konceptu. Hlavnou myšlienkou je objasnenie čitateľovi problematiku IMS.

Anotácia v cudzom jazyku (anglický resp. nemecký):

Diploma work consults about explanation IP multimedial subsystem IMS. Thw work characterises basic functions an properties of IMS. The main core of the work explains detailed entry of each fuction parts of architecture and concept. The main idea is to get the reader an explanation of IMS system.

Kľúčové slová: IMS, archytektúra, koncept, 3GPP

Vedúci práce: prof. Ing. Karol Blunár, DrSc.

Recenzent práce: …….....

Dátum odovzdania práce: 16.5.2008

Obsah

Zoznam obrázkov

Zoznam tabuliek

Zoznam skratiek

1G	First generation
2G	Second generation
3G	Third generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
AAR&AAA	AA-Request/AA-Answer
ACA	Accounting Answer
ACR	Accounting Request
ADSL	Asynchronous Digital SubscriberLine
AKA	Authentication and Key Agreement
AMR	Adaptive Multi-Rate
API	Application Programming Interface
APN	Access Point Name
AS	Application Server
ASR&ASA	Abort-Session-Request/Abort-Session-Answer
ATM	Asynchronous Transfer Mode
AUC	Authentication Centre
AUTN	Authentication token
AUTS	Synchronization token
AVP	Attribute Value Pair; Audio Video Profile
BER	Bit Error Ratio
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
BSF	Bootstrapping Server Function
BTS	Base Transceiver Station
CA	Certificate Authority
CAMELCustomized	Applications for Mobile network EnhancedLogic
CAP	CAMELApplication Part
CCR	Credit-Control-Request
CDF	Charging Data Function

CDMA	Code Division Multiple Access
CDR	Charging Data Record; Call Data Record
CGF	Charging Gateway Function
CK	Ciphering (Cipher) Key
CN	Core Network
CRF	Charging Rule Function
CS CN	Circuit Switched Core Network
CSCF	Call Session Control Function
CSE	CAMELService Environment
CTF	Charging Trigger Function
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DNS	Domain Name System
DTMF	Dual-Tone Multi-Frequency
EDGE	Enhanced Data Rates for Global Evolution
ESP	Encapsulating (Encapsulated) Security Payload
ETSI	European Telecommunications Standards Institute
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GCID	GPRS Charging IDentifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HLR/AUC	Home Location Register and AUthentication Center
HSS	Home Subscriber Server
HTTP	Hypertext Transfer (or Transport) Protocol
I-CSCF	Interrogating-CSCF
ICID	IMS Charging IDentifier
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange
IM-SSF	IP Multimedia Service Switching Function

IMS	IP Multimedia Subsystem
IMS-GWF	IMS-Gateway Function
IMS-MGW	IP Multimedia Subsystem-Media Gateway Function
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISC	IMS Service Control
ISDN	Integrated Services Digital Network
ISIM	IP Multimedia Services Identity Module
ISUP	ISDN User Part
LCS	Location services
MAA	Multimedia-Auth-Answer
MAP	Mobile Application Part
MAR	Multimedia-Auth-Request
MBR	Maximum Bit Rate
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Media Gateway Function
MIME	Multipurpose Internet Mail Extension
MITM	Man In The Middle
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller
MRFP	Media Resource Function Processor
MSC	Mobile Switching Centre
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Subscriber Integrated Services Digital Network;
MTP	Message Transfer Part
NAF	Network Application Function
NAI	Network Access Identifier

NAPTR	Naming Authority PointeR
NASREQ	Network Access Server Requirements
NAT	Network Address Translator
NAT-PT	Network Address Translator–Protocol Translator
NDS	Network Domain Security
NDS/AF	NDS Authentication Framework
OCS	Online Charging System
OMA	Open Mobile Alliance
OSA	Open Services Architecture
OTA	Over The Air
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PDP	Packet Data Protocol; Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PNA	Push-Notification-Answer
PNR	Push-Notification-Request
POTS	Plain Old Telephone Service
PPA	Push-Profile-Answer
PPR	Push-Profile-Request
PS	Packet Switched; Presence Server
PSI	Public Service Identity
PSK	Pre-shared Secret Key
PSTN	Public Switched Telephone Network
PUA	Presence User Agent; Profile-Update-Answer
PUR	Profile-Update-Request
QOS	Quality of Service
RAND	Random challenge
RAR&RAA	Re-Auth-Request/Re-Auth-Answer
RES	Response
RFC	Requests For Comments
RNC	Radio Network Controller
RR	Receiver Report; Resource Record
RTA	Registration-Termination-Answer

RTCP RTP	Control Protocol; Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTP/AVP	RTP Audio and Video Profile
RTR	Registration-Termination-Request
S-CSCF	Serving-CSCF
SAA	Server-Assignment-Answer
SAR	Server-Assignment-Request
SBC	Session Border Controller
SBLP	Service-Based Local Policy
SCS	Service Capability Server
SDU	Service Data Unit
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SGW	Signalling Gateway
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SMS	Short Messaging Service
SNA	Subscribe-Notifications-Answer
SNR	Subscribe-Notifications-Request
SPD	Security Policy Database
SPT	Service Point Trigger
SQN	Sequence number
SRF	Single Reservation Flow
SS7	Signaling System No. 7
STR&STA	Session-Termination-Request/Session-Termination-Answer
TCP	Transmission Control Protocol
TD-CDMA	Time Division/Code Division Multiple Access
THIG	Topology Hiding Inter-network Gateway
TLS	Transport Layer Security
TPF	Traffic Plane Function
UA	User Agent
UAA	User-Authorization-Answer
UAR	User-Authorization-Request
UDA	User-Data-Answer

UDP	User Datagram Protocol
UDR	User-Data-Request
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VHE	Virtual Home Environment
VOIP	Voice over IP
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
WWW	World Wide Web obvious
XRES	Expected response

1 Úvod

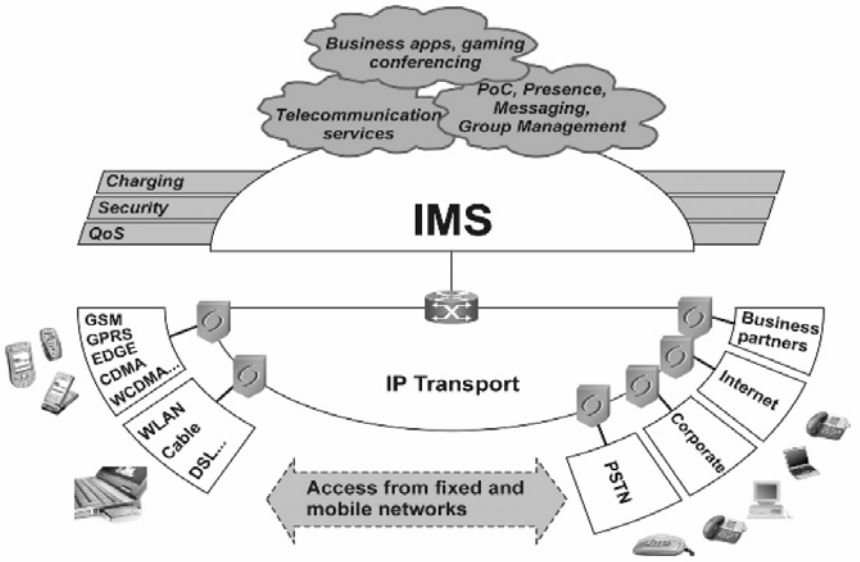
V posledných 20 rokoch zaznamenali pevné a mobilné siete významný posun. V mobilnom svete boli systémy prvej generácie (1G) uvedené v polovici 80. rokov. Tieto siete ponúkali užívateľom základné služby. Hlavný dôraz sa kládol na hovor a služby spojené s hovorom. Systémy druhej generácie (2G) priniesli v 90. rokoch určité dátové služby a prepracovanejšie doplnkové služby pre užívateľov. Tretia generácia (3G) dnes umožňuje rýchlejšie prenosy dát a rôzne multimediálne služby. V oblasti pevných sietí tradičná verejná komutovaná telefónna sieť (Public Switched Telephone Network - PSTN) a digitálna sieť integrovaných služieb (Integrated Services Digital Network - ISDN) prevládali v tradičnej hlasovej a video komunikácii. V posledných rokoch používanie internetu zažíva veľký boom a čoraz viac užívateľov využíva rýchlejšie a lacnejšie internetové pripojenie ako napríklad asymetrická digitálna účastnícka linka (Asymetric Digital Subscriber Line - ADSL). Tieto typy internetového pripojenia umožňujú nepretržité pripojenie nevyhnutné pre ľudí, ktorí začínajú používať prostriedky komunikácie v reálnom čase - napr. aplikácie pre internetový rozhovor, hranie online hier, prenos hlasu cez internet (Voice over IP - VoIP).

V súčasnosti dochádza k rýchlemu zbližovaniu pevného a mobilného sveta spôsobeného každoročným zvyšovaním penetrácie mobilných zariadení a čoskoro bude na svete viac ako 2 miliardy používateľov mobilných zariadení. Tieto mobilné zariadenia majú veľké displeje s vysokým rozlíšením, zabudované kamery a veľké množstvo zdrojov pre aplikácie. Sú to nepretržite zapnuté a nepretržite pripojené mobilné zariadenia. Tým dochádza k predefinovaniu aplikácií. Aplikácie už nie sú izolované entity, ktoré vymieňajú informácie len s užívateľským rozhraním. Ďalšou generáciou zaujímavých aplikácií sú peer-to-peer entity, ktoré zjednodušujú zdieľanie: zdieľané prehliadanie, zdieľaná tabuľa, zdieľané herné zážitky, zdieľané dvojsmerné rádiové spojenie (napr. Push-to-talk na mobilných sieťach). Predefinovaný bude aj koncept stavu pripojenia. Vytočenie čísla a hovor budú čoskoro pokladané len za malú podmnožinu pripojenia do siete. Schopnosť vytvoriť peer-to-peer spojenie medzi novými zariadeniami s aktivovaným internetovým protokolom (Internet Protocol - IP) je kľúčovou požiadavkou. Toto nové paradigma komunikácií vo veľkej miere presahuje možnosti klasickej telefónnej služby (Plain Old Telephone Service - POTS).

Pre umožnenie komunikácie musia mať IP aplikácie mechanizmus pre zastihnutie korešpondenta. V súčasnosti zabezpečuje túto kritickú úlohu vytvorenia pripojenia telefónna sieť. Po vytočení peera môže sieť vytvoriť *ad hoc* pripojenie medzi akýmikoľvek dvoma terminálmi cez IP sieť. Táto kritická schopnosť IP konektivity je dostupná len v izolovaných prostrediach poskytovateľov jedinej služby na internete; uzavreté systémy súťažia na užívateľskej báze, kde je lock-in užívateľa kľúčový a komunikácia prepojených systémov medzi poskytovateľmi služby je neželanou vlastnosťou. Potrebujeme teda globálny systém – IP multimediálny subsystém (IP Multimedia Subsystem - IMS). Umožňuje aplikáciám v zariadeniach s aktivovaným IP vytvoriť peer-to-peer a peer-to-content pripojenie ľahko a bezpečne.

Reálna integrácia hlasových a dátových služieb zvyšuje produktivitu a celkovú efektívnosť, pričom vývoj inovatívnych aplikácií integrujúcich hlas, údaje a multimédiá vytvorí požiadavky na nové služby, ako napríklad prístupnosť, multimediálny internetový rozhovor, push to talk a vedenie konferencií. Schopnosť skombinovať mobilitu a IP sieť bude kľúčová pre úspech služby v budúcnosti.

Obrázok 1.1 zobrazuje konvergovanú komunikačnú sieť pre pevné mobilné prostredie. IMS zavádza kontrolu multimediálnej relácie v paketovo spínanej doméne a zároveň prináša funkčnosť spínania obvodov v paketovo spínanej doméne. IMS je kľúčová technológia pre takúto konsolidáciu siete.



Obrázok 1.1 IMS v konvergujúcich sieťach

Business apps, gaming, conferencing –Obchodné aplikácie, hry, vedenie konferencií

Telecommunication services - Telekomunikačné služby

PoC, Presence, Messaging, Group Management – PoC, Prístupnosť, Posielanie správ, Správa skupín
Charging - Účtovanie
Security - Bezpečnosť
QoS
Cable - Káblové pripojenie
IP Transport - IP prenos
Business partners - Obchodní partneri
Corporate - Spoločnosť
Access from fixed and mobile networks - Prístup z pevných a mobilných sietí

1.1 Príklad IMS služieb

Po zapnutí sa zariadenie s aktivovaným multimediálnym subsystémom na báze internetového protokolu (IMS) automaticky zaregistruje na IMS sieť pomocou informácií v module identity (ako napríklad USIM). Počas registrácie sa autentifikuje zariadenie aj sieť a zariadenie získa zo siete užívateľské identity. Po tejto jedinej registrácii budú dostupné všetky uživateľove služby, vrátane push to talk, prístupnosti, hlasových a video konferencií, odosielania správ a hier s viacerými hráčmi. Okrem toho sa aktualizujú informácie o dostupnosti na serveri spravujúcom prístupnosť a zmenia sa na "online“ a zobrazí sa zoznam aktuálnych aplikácií.

Všetka požadovaná komunikácia prebieha prostredníctvom IP konektivity, ktorú poskytuje IMS. IMS ponúka možnosť vybrať si najlepšie a najvhodnejšie komunikačné médiá, spontánne zmeniť médium počas relácie a použiť preferované komunikačné zariadenie (SIP- spôsobilé) na akýkoľvek IP prístup.

1.2 Vývoj IMS

Európsky inštitút pre telekomunikačné normy (European Telecommunications Standards Institute - ETSI) bol štandardizačnou organizáciou, ktorá definovala Globálny systém pre mobilnú komunikáciu (Global System for Mobile Communications - GSM) koncom 80. a počas 90. rokov. ETSI tiež definovala sieťovú architektúru Všeobecná paketová rádiová služba (General Packet Radio Service - GPRS). Posledný štandard výlučne GSM bol vyrobený v roku 1988 a v rovnakom roku bolo založené 3GPP

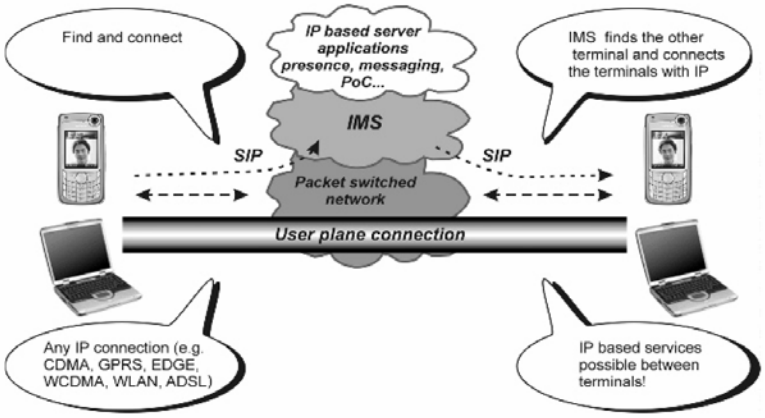
štandardizačnými orgánmi z Európy, Japonska, Južnej Kórey, USA a Číny s cieľom vymedziť 3G mobilný systém zahrňujúci rádiový prístup s širokopásmovým viacnásobným prístupom s kódovým delením (Wideband Code Division Multiple Access - WCDMA) a viacnásobným prístupom s časovým delením/kódovým delením (Time Division/Code Division Multiple Access – TD-CDMA) a vyvinutú GSM základnú sieť. Väčšina pracovných a základných špecifikácií bola prevzatá zo špeciálnej mobilnej skupiny ETSI (Special Mobile Group - SMG). 3GPP sa pôvodne rozhodla pripravovať špecifikácie každý rok, prvým špecifikovaným vydaním bol Release 99.

1.2.1 3GPP Release 99 (3GPP R99)

O rok bolo vypracované prvé vydanie – Release 1999. Funkčnosť vydania bola zamrazená v decembri 1999, pričom niektoré špecifikácie boli uzatvorené neskôr – v marci 2001. Rýchle dokončenie umožnilo rozdelenie práce medzi dve organizácie: 3GPP a ETSI SMG. 3GPP vyvinula služby, architektúru systému, rádiové prístupy WCDMA a TD-CDMA a spoločnú základnú sieť. ETSI SMG vyvinula rádiový prístup na zvýšené prenosy údajov pre globálny vývoj GSM (GSM/Enhanced Data Rates for Global Evolution - EDGE).

Rádiový prístup WCDMA predstavoval najvýznamnejšie zlepšenie 3G systému na báze GSM v Release 1999. Okrem WCDMA, Sieť pozemného rádiového prístupu do UMTS (UMTS Terrestrial Radio Access Network - UTRAN) uviedla tiež Iu rozhranie. V porovnaní s rozhraním A a Gb prinieslo dva významné rozdiely. Prvým je, že transkódovanie reči pre Iu prebieha v základnej sieti. V GSM to logicky bola funkčnosť Vysielacej/prijímacej základňovej stanice (Base Tranceiver Station - BTS). Druhým rozdielom je, že šifrovanie a správa mobility na úrovni buniek pre Iu prebiehajú v riadiacej jednotke rádiovej siete (Radio Network Controller - RNC). V GSM prebiehali v obslužnom GPRS podpornom uzle (Serving GPRS Support Node - SGSN) pre GPRS služby.

Pre vytvorenie služby bola uvedená architektúra pre otvorené služby (Open Service Architecture - OSA). Na strane služby bolo cieľom ukončiť štandardizovanie nových služieb a sústrediť sa na schopnosti služby, ako toolkity (CAMEL, SIM Aplikačný toolkit a OSA). Tento princíp bol relatívne dobre dodržiavaný, aj keď pre virtuálne domáce prostredie (Virtual Home Environment - VHE), čo je zastrešujúci koncept pokrývajúci vytvorenie celej služby, stále chýba vhodná definícia.



Obrázok 1.2 Úloha IMS v paketovo spínaných sieťach

Find a contact - Nájsť kontakt

IP based server applications presence, messaging, PoC... - Serverové aplikácie na báze IP, prístupnosť, posielanie správ, PoC...

IMS finds the other terminal and connects the terminals with IP - IMS nájde druhý terminál a prepojí terminály s IP

Any IP connection (e.g. CDMA, GPRS, EDGE, WCDMA, WLAN, ADSL) - Akékoľvek IP pripojenie (napr. CDMA, GPRS, EDGE, WCDMA, WLAN, ADSL)

IP based services possible between terminals! – Služby na báze IP možné medzi terminálmi!

User plane connection - Pripojenie na užívateľskej rovine

1.2.2 3GPP Release 4

Po Release 1999 3GPP začala špecifikovať Release 2000, vrátane tzv. All-IP, ktorý bol neskôr premenovaný na IMS. V roku 2000 bolo zrejmé, že vývoj IMS nebude v tom roku dokončený. Release 2000 bol teda rozdelený na Release 4 a Release 5.

Bolo rozhodnuté, že Release 4 bude ukončený bez IMS. Najvýznamnejšie nové funkčnosti v 3GPP Release 4 boli: koncept serverovej mediálnej brány (Server Media Gateway - MGW) mobilného prepájacieho centra (Mobile Switching Centre - MSC) pre bránu server- médií, IP prenos protokolov základnej siete, zlepšenia lokalizačných služieb (Location Services - LCS) pre UTRAN a posielanie multimediálnych správ a IP prenos pre užívateľskú rovinu Gb.

3GPP Release 4 bol funkčne zamrazený a oficiálne ukončený v marci 2001. Požiadavka spätnej kompatibility pre zmeny, nevyhnutná pre rádiové rozhranie, bola presadená až koncom septembra 2002.

1.2.3 3GPP Release 5, 6 a 7

Release 5 konečne zaviedlo IMS ako súčasť špecifikácií 3GPP. IMS by mal byť štandardizovaná architektúra na báze IP nezávislá od prístupu, ktorá je prepojená s existujúcimi hlasovými a dátovými sieťami pre pevných (napr. PSTN, ISDN, Internet) aj mobilných užívateľov (napr. GSM, CDMA). Architektúra IMS umožňuje vytvoriť peer-to-peer IP komunikácie so všetkými typmi klientov s požadovanou kvalitou služieb. Okrem správy relácií sa architektúra IMS zameriava tiež na funkčnosti, ktoré sú potrebné pre kompletnú dodávku. Celkovo IMS vytvorí jadro základnej IP siete.

Obsah Release 5 bol predmetom mnohých diskusií a nakoniec bol funkčný obsah 3GPP Release 5 zamrazený v marci 2002. Dôsledkom tohto rozhodnutia bolo, že mnohé vlastnosti boli odložené do ďalšieho vydania – Release 6. Po zamrazení obsahu práca pokračovala a stabilita bola dosiahnutá začiatkom roku 2004. Release 6 IMS opravuje nedostatky Release 5 IMS a tiež obsahuje nové vlastnosti. Release 6 bol dokončený v septembri 2005. Tabuľka 1.1 zobrazuje najdôležitejšie vlastnosti Release 5 a Release 6. Tabuľka obsahuje aj plánované vlastnosti Release 7. Práca na Release 7 stále prebieha a očakáva sa, že jeho vlastnosti budú pripravené počas roku 2006.

V Tabuľke 1.1 môžete vidieť, že 3GPP definovala konečnú architektúru pre zariadenia IP multimediálnych služieb na báze SIP. Obsahuje funkčnosť logických prvkov, popis prepojenia prvkov, vybrané protokoly a procedúry. Je dôležité uvedomiť si, že optimalizácia pre mobilné komunikačné prostredie bola navrhnutá vo forme autentifikácie a autorizácie užívateľa na báze mobilných identít, presných pravidiel pre užívateľské sieťové rozhranie pre kompresiu SIP správ a kontrolných mechanizmov bezpečnostnej politiky, ktoré umožňujú rádiovú stratu a detekciu obnovy. Vývoj architektúry sa ďalej zameriava na aspekty dôležité z hľadiska operátora, ako napríklad účtovací rámec a politika a kontrola služby.

Tabuľka 1.1 Vlastnosti IMS

Relase 5	Release 6	Release 7
Architektúra: sieťové entity a referenčné body vrátane účtovacích funkcií.	*Architektúra:* komunikácia prepojených systémov (CS, iné IP siete, WLAN) a niekoľko nových entít a referenčných bodov.	*Architektúra:* kontinuita hlasového hovoru medzi CS a PS doménami, pevné širokopásmové pripojenie k IMS.
Signalizácia: všeobecné princípy smerovania, registrácia, iniciovanie relácie, zmena relácie, rozloženie relácie, odpojenie relácie iniciované sieťou/toky pre zrušenie registrácie: • SIP kompresia medzi UE a IMS sieťou; • dátový prenos medzi úložiskom užívateľských informácií (HSS) a kontrolnými entitami relácie (CSCF); • dátový prenos medzi úložiskom užívateľských informácií (HSS) a aplikačným serverom (AS).	*Signalizácia:* smerovanie skupinových identít, viacnásobná registrácia.	*Signalizácia:* núdzové relácie, SMS podpora pomocou SIP, kombinovanie CS hovorov a IMS relácií.
Bezpečnosť: IMS AKA pre autentifikáciu užívateľov a siete, ochrana integrity SIP správ medzi UE a IMS sieťou, bezpečnosť sieťovej domény.	*Bezpečnosť:* ochrana dôvernosti SIP správ, autentifikácia na báze IP, Generická architektúra autentifikácie?	*Bezpečnosť*: prispôsobenie širokopásmovému prístupu, podpora TLS.
Kvalita služby: kontrola politiky medzi IMS a GPRS prístupovou sieťou, predpoklady a autorizačná známka.	*Kvalita služby:* multiplexovanie mediálnych tokov rôznych relácií v rovnakom PDP kontexte.	*Kvalita služby:* harmonizácia politiky a kontroly účtovania, QoS autorizácia bez známky.
Služby: použitie aplikačných serverov a referenčný bod IMS kontroly služby.	*Služby:*prístupnosť, posielanie správ, vedenie konferencií, Push to talk cez mobilný telefón, správa skupín, lokálne služby.	*Služby:* doplnkové služby v SIP.
Všeobecné: ISIM		*Rôzne:* Mobilita WLAN-UMT

2 Architektúra IP multimediálneho subsystému

Táto kapitola predstavuje multimediálny systém na báze internetového protokolu (Internet Protocol (IP) Multimedia Subsystem (IMS)).

2.1 Architektonické požiadavky

Existuje sada základných požiadaviek, ktorá riadi spôsob, akým bola IMS architektúra vytvorená a ako by sa mala vyvíjať v budúcnosti. Táto časť popisuje najvýznamnejšie požiadavky. IMS požiadavky Projektu partnerstva tretej generácie (Third Generation Partnership Project - 3GPP) sú zdokumentované v [3GPP TS 22.228].

2.1.1 IP multimediálne relácie

Existujúce komunikačné siete sú schopné ponúknuť hlasové služby, video služby a služby posielania správ pomocou obvodovo spínaných nosičov. Kvalita ponuky služieb pre koncových užívateľov by sa samozrejme nemala zhoršiť, keď užívatelia prejdú na obvodovo spínanú doménu a začnú používať IMS. IMS posunie komunikáciu na nasledujúcu úroveň svojou ponukou obohatených komunikačných prostriedkov. IMS užívatelia sú schopní kombinovať a spájať rôzne služby na báze IP akýmkoľvek spôsobom, aký si vyberú počas jednej komunikačnej relácie. Užívatelia môžu spojiť hlas, video a text, zdieľanie obsahu a prístupnosť ako súčasť ich komunikácie a môžu pridať alebo ukončiť služby kedykoľvek a akýmkoľvek spôsobom sa rozhodnú. Napríklad dvaja ľudia môžu začať reláciu ako hlasovú reláciu a neskôr pridať hernú alebo obrazovú zložku do tej istej relácie.

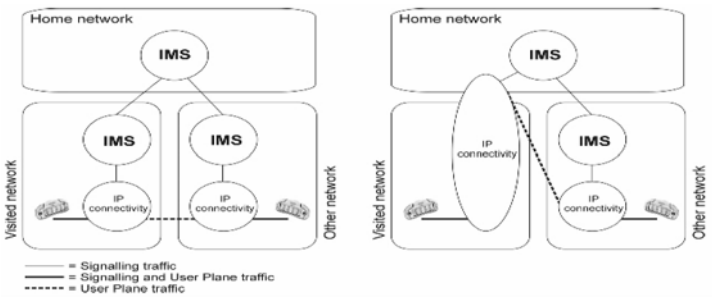
2.1.2 IP konektivita

Ako to naznačuje názov IP multimediálny subsystém základnou požiadavkou je, aby zariadenie malo IP konektivitu, ktorá k nemu umožní prístup. Peer-to-peer aplikácie vyžadujú dostupnosť na úrovni koncového zariadenia a táto konektivita je najľahšie dosiahnuteľná pomocou IP verzie 6 (IPv6), pretože IPv6 má dostatok adries. 3GPP to teda zariadil tak, že IMS podporuje výlučne IPv6 [3GPP TS 23.221]. Prvé implementácie

a nasadenia IMS môžu používať IP verziu 4 (IPv4). 3GPP vytvoril odporúčanie o spôsobe riadenia vzájomnej komunikácie IP verzií v IMS.

IP konektivitu je možné získať buď z domácej siete alebo z navštívenej siete. Časť úplne vľavo na obrázku 2.1 znázorňuje možnosť, kde užívateľské zariadenie (UE) získalo IP adresu z navštívenej siete. V UMTS sieti to znamená, že rádiová prístupová sieť (Radio Access Network - RAN), obslužný podporný uzol GPRS (Serving GPRS Support Node - SGSN) a stykový podporný uzol GPRS (Gateway GPRS Support Node - GGSN) sú umiestnené v navštívenej sieti, keď užívateľ využíva roaming v navštívenej sieti. Časť úplne vpravo na obrázku 2.1 znázorňuje možnosť, kde UE získalo IP adresu z domácej siete. V UMTS sieti to znamená, že RAN a SGSN sú umiestnené v navštívenej sieti, keď sa užívateľ využíva roaming v navštívenej sieti. Je zrejmé, že keď sa užívateľ nachádza v domácej sieti, všetky potrebné prvky sú v domácej sieti a IP konektivita je získaná v tejto sieti.

Je dôležité poznamenať, že užívateľ môže využívať roaming a získať IP konektivitu v domácej sieti, ako je to znázornené na obrázku. To by umožnilo užívateľom používať nové, prvotriedne služby aj keď sa využívajú roaming v oblasti, ktorá nemá IMS sieť, ale poskytuje IP konektivitu. Teoreticky je možné nasadiť IMS sieť v jedinej oblasti/krajine a použiť napríklad roaming všeobecnej paketovej rádiovej služby (General Packet Radio Service - GPRS) pre pripojenie zákazníkov k domácej sieti. V praxi by k tomu nedošlo, pretože efektívnosť smerovania by nebola dostatočne vysoká. Predstavte si smerovanie hlasových paketov pomocou protokolu prenosu v reálnom čase (Real-time Transport Protocol - RTP) z USA do Európy a potom naspäť do USA. Tento model nasadenia je však dôležitý, keď operátori posilňujú IMS siete alebo v počiatočnej fáze, keď ponúkajú multimediálne služby nevyžadujúce prenos v reálnom čase alebo s prenosom blízkym reálnemu času.



Obrázok 2.1 Možnosti IMS konektivity, keď užívateľ využíva roaming

Home network – Domáca sieť
Visited network - Navštívená sieť
Other network - Iná sieť
IP connectivity – IP konektivita
Signalling traffic - Signalizácia prevádzky
Signalling and User Plane traffic - Signalizácia a prevádzka na užívateľskej rovine
User plane traffic – Prevádzka na užívateľskej rovine

2.1.3 Zaistenie kvality služby pre IP multimediálne služby

Na verejne prístupnom internete bývajú oneskorenia veľké a premenlivé, pakety prichádzajú nefunkčné a niektoré pakety sú stratené alebo vyradené. S IMS to bude ale úplne inak. Základné prístupové a prenosové siete spolu s IMS poskytujú kvalitu služby (Quality of Service – QoS) na úrovni koncových zariadení. Prostredníctvom IMS UE vyjedná svoje schopnosti a vyjadrí svoje QoS požiadavky počas nastavenia relácie protokolu iniciácie relácie (Session Initiation Protocol – SIP) alebo procedúry zmeny relácie. UE je schopné vyjednať také parametre ako:

- Typ média, smer alebo prevádzka.
- Bitová rýchlosť typu média, veľkosť paketu, frekvencia prenosu paketu.
- Použitie RTP nákladu pre typy médií.
- Prispôsobenie šírky pásma.

Po vyjednaní parametrov na úrovne aplikácie, UE zaistia vhodné zdroje z prístupovej siete. Keď je vytvorená QoS na úrovni koncového zariadenia, UE zakódujú a vytvoria pakety z individuálnych typov médií s príslušným protokolom (napr. RTP) a pošlú tieto mediálne pakety do prístupovej a prenosovej siete pomocou protokolu prenosovej vrstvy (Transport Layer Protocol - TCP alebo UDP) cez IP. Predpokladá sa, že operátori vyjednajú dohody o úrovni služby na zabezpečenie požadovanej QoS v prepojovacej chrbticovej sieti. V prípade UMTS môžu užívatelia použiť GPRS roamingovú výmennú chrbticovú sieť.

2.1.4 Kontrola IP politiky pre zabezpečenie správneho použitia mediálnych zdrojov

Kontrola IP politiky znamená schopnosť autorizovať a kontrolovať použitie prevádzky nosičov určených pre IMS média, na základe signalizačných parametrov v IMS relácii. To vyžaduje interakciu medzi prístupovou sieťou s IP konektivitou a IMS. Prostriedky nastavenia interakcie môžu byť rozdelené do troch rôznych kategórií [3GPP TS 22.228, 23.207, 23.228]:

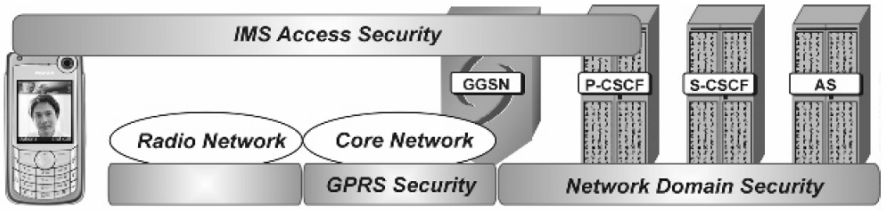
- Prvok kontroly politiky je schopný overiť, či sú hodnoty vyjednané v SIP signalizácii použité pri aktivovaní nosičov pre mediálnu prevádzku. To umožní operátorovi overiť, či jeho zdroje nosičov nie sú zneužité (napr. zdrojová a cieľová IP adresa a šírka pásma v nosiči sú úplne rovnaké ako tie, ktoré boli použité pri vytvorení SIP relácie).
- Prvok kontroly politiky je schopný stanoviť, kedy mediálna prevádzka medzi koncovými bodmi SIP relácie začne alebo skončí. To umožní predísť použitiu nosiča, kým nie je vytvorenie relácie ukončené a umožní začatie/ukončenie prevádzky zároveň so začatím/ukončením účtovania pre reláciu v IMS.
- Prvok kontroly politiky je schopný získať upozornenia, keď služba prístupovej siete s IP konektivitou zmenila, zastavila alebo uvoľnila nosič(e) užívateľa spojeného s reláciou. To umožní IMS uvoľniť prebiehajúcu reláciu, pretože užívateľ sa už napríklad nenachádza v oblasti pokrytia.

Lokálna politika založená na službe (Service-Based Local Policy - SBLP) sa používa ako synonymum pre kontrolu IP politiky v IMS.

2.1.5 Bezpečná komunikácia

Bezpečnosť je základnou požiadavkou v každom telekomunikačnom systéme a IMS nie je výnimkou. IMS má svoje vlastné autentifikačné a autorizačné mechanizmy medzi UE a IMS sieťou, okrem procedúr prístupovej siete (napr. GPRS sieť). Okrem toho, je zabezpečená integrita a dobrovoľná dôvernosť SIP správ medzi UE a IMS sieťou a medzi entitami IMS siete, bez ohľadu na podkladovú základnú sieť (napr. RAN a GPRS). IMS teda poskytuje minimálne rovnakú úroveň bezpečnosti ako príslušné

GPRS a obvodovo spínané siete; IMS napríklad zabezpečuje, že užívatelia sú autentifikovaní predtým, ako môžu začať používať služby a užívatelia môžu požadovať ochranu súkromia, keď sú zapojení do relácie. Prehľad použitých bezpečnostných riešení je zobrazený na Obrázku 2.2.



Obrázok 2.2 Prehľad bezpečnosti IMS.

IMS Access Security – Bezpečnosť IMS prístupu
Radio Network – Rádiová sieť
Core Network – Základná sieť
GPRS Security – Bezpečnosť GPRS
Network Domain Security – Bezpečnosť sieťovej domény

2.1.6 Účtovacie opatrenia

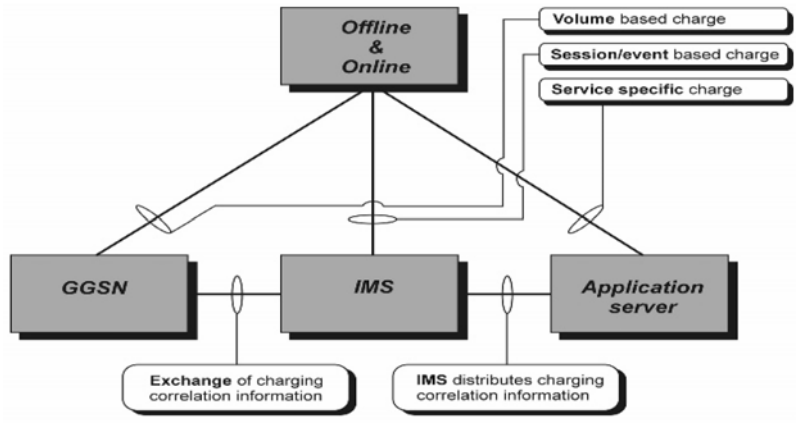
Z pohľadu operátora alebo poskytovateľa služby je schopnosť spoplatniť užívateľov v sieti nevyhnutnosťou. IMS architektúra umožňuje použitie rôznych účtovacích modelov. To zahrňuje napríklad schopnosť spoplatniť len volajúcu stranu alebo spoplatniť obe, teda aj volajúcu stranu aj volanú stranu na základe použitých zdrojov na úrovni prenosu. V druhom prípade volajúca strana môže byť spoplatnená v plnom rozsahu na úrovni IMS relácie: to znamená, že je možné použiť rôzne účtovacie metódy na úrovni prenosu a IMS. Operátor však môže požadovať koreláciu účtovacích informácií vytvorených na úrovni účtovania prenosu a IMS (služba a obsah). Táto schopnosť je zabezpečená ak operátor používa referenčný bod kontroly politiky.

Keďže IMS relácie môžu zahrňovať viaceré mediálne komponenty (napr. audio a video) je nevyhnutné, aby IMS poskytoval prostriedky pre účtovanie podľa mediálnych komponentov. To by umožnilo spoplatniť volanú stranu, ak si pridá nový mediálny

komponent do relácie. Je tiež nevyhnutné, aby boli rôzne IMS siete schopné vymieňať informácie o účtovaní, ktoré majú byť použité pre aktuálnu reláciu [3GPP TS 22 101.

Architektúra IMS podporuje online aj offline účtovacie možnosti. Online účtovanie je účtovací proces, pri ktorom môže účtovacia informácia v reálnom čase ovplyvniť poskytovanú službu a teda priamo reaguje na kontrolu relácie/služby. V praxi by mohol operátor skontrolovať účet užívateľa predtým, ako mu umožní spustiť reláciu a skončiť reláciu, keď sú spotrebované všetky kredity. Predplatené služby sú aplikácie, ktoré musia mať online účtovacia schopnosti. Offline účtovanie je účtovací proces, pri ktorom účtovacia informácia neovplyvňuje v reálnom čase poskytovanú službu. To je tradičný model, pri ktorom sú účtovacie informácie zhromažďované počas určitého obdobia a na konci tohto obdobia operátor vystaví zákazníkovi faktúru.

Obrázok 2.3 znázorňuje zjednodušený pohľad na všeobecné účtovacie opatrenia v IMS prostredí. Kľúčovým postrehom je, že IMS pridáva možnosť účtovania IP prevádzky užívateľa detailnejším spôsobom ako predtým.

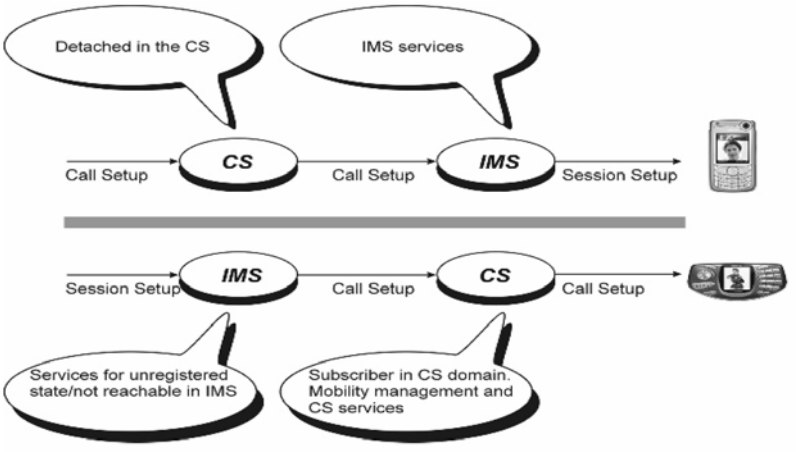


Obrázok 2.3 Prehľad účtovania IMS

Volume based charge – Účtovanie na základe objemu
Session/event based charge – Účtovanie na základe relácie/udalosti
Service specific charge – Špecifické účtovanie služby
Exchange of charging correlation information – Výmena účtovacích korelačných informácií
IMS distributes charging correlation information – **IMS** rozdeľuje účtovacie korelačné informácie
Application server - Aplikačný server.

2.1.7 Podpora roamingu

Z hľadiska užívateľa je dôležité získať prístup k službám bez ohľadu na ich geografické umiestnenie. Vlastnosť roamingu umožňuje použitie služieb aj keď sa užívateľ z geografického hľadiska nenachádza v oblasti služby domácej siete. Vyššie už boli popísané dva príklady roamingu: jednalo sa o GPRS roaming a IMS roaming. Okrem týchto dvoch existuje prípad obvodovo spínaného IMS roamingu. GPRS roaming znamená schopnosť prístupu k IMS, kde navštívená sieť poskytuje RAN a SGSN a domáca sieť poskytuje GGSN a IMS. IMS roamingový model predstavuje sieťovú konfiguráciu, pri ktorej navštívená sieť poskytuje IP konektivitu (napr. RAN, SGSN, GGSN) a vstupný bod IMS (napr. P-CSCF) a domáca sieť poskytuje ostatné IMS funkčnosti. Hlavnou výhodou roamingového modelu v porovnaní s GPRS roamingovým modelom je optimálne použitie zdrojov na užívateľskej rovine. Roaming medzi IMS a CS CN doménou predstavuje medzidoménový roaming medzi IMS a CS. Keď užívateľ nie je registrovaný alebo dostupný v jednej doméne, relácia môže byť presmerovaná na inú doménu. Je potrebné poznamenať, že aj CS CN doména aj IMS doména majú svoje vlastné služby a nemôžu byť používané z inej domény. Niektoré služby sú rovnaké a dostupné v obidvoch doménach (napr. Voice over IP v IMS a hlasové telefonovanie v CS CN). Obrázok 2.4 zobrazuje rôzne prípady IMS/CS roamingu.



Obrázok 2.4 IMS/CS roamingové alternatívy

Detached in the CS – Oddelený v CS
IMS services – IMS služby

Call Setup – Nastavenie hovoru
Session Setup – Nastavenie relácie
Services for unregistered state/not reachable in IMS – Služby pre neregistrovaný stav/nedostupné v IMS
Subscriber in CS domain. Mobility management and CS service – Účastník v CS doméne. Správa mobility a CS služby

2.1.8 Spolupráca s inými sieťami

Je zrejmé, že IMS nebolo zavedené vo svete v rovnakom čase. Okrem toho ľudia nemusia mať možnosť rýchlo zmeniť terminály alebo účastnícke služby. Vzniká tak problém, ako sa spojiť s ľuďmi bez ohľadu na to, aký druh terminálov majú alebo kde žijú. Aby mohol byť IMS novou, úspešnou technológiou a architektúrou komunikačnej siete, musí byť schopný pripojiť čo najviac užívateľov. IMS teda podporuje komunikáciu s PSTN, ISDN, mobilnými a internetovými užívateľmi. Okrem toho bude možné podporovať relácie s internetovými aplikáciami, ktoré boli vyvinuté mimo komunitu 3GPP [3GPP TS 22.228].

2.1.9 Model kontroly služby

V 2G mobilných sieťach sa používa navštívená kontrola služby. To znamená, že keď užívateľ využíva roaming, entita v navštívenej sieti poskytuje služby a kontroluje prevádzku pre užívateľa. Táto entita sa v druhej generácii (2G) nazýva navštívené prepínacie centrum mobilnej služby. Na počiatku Release 5 bol podporovaný model navštívenej kontroly aj domácej kontroly služby. Podpora oboch modelov by vyžadovala, aby mal každý problém viac ako jedno riešenie; okrem toho by sa znížil počet optimálnych riešení architektúry, keďže jednoduché riešenia nemusia byť vhodné pre obidva modely. Podpora oboch modelov by znamenala dodatočné rozšírenia pre protokoly Internet Engineering Task Force (IETF – Operačná skupina internetového inžinierstva) a viedla k nárastu práce v registračných a relačných tokoch. Navštívená kontrola služby bola vynechaná, pretože to bolo príliš komplexné riešenie a neposkytovala žiadnu významnejšiu pridanú hodnotu v porovnaní s domácou kontrolou služby. Naopak navštívená kontrola služby stanovuje určité obmedzenia. Vyžaduje viacnásobné vzťahy a roamingové modely medzi operátormi. Vývoj služby je pomalší,

keďže aj navštívená aj domáca sieť by potrebovali podporu rovnakých služieb, inak by užívatelia roamingu zaznamenali zhoršenie služby. Okrem toho počet referenčných bodov medzi operátormi sa zvyšuje, čo vyžaduje komplikované riešenia (napr. čo sa týka bezpečnosti a účtovania). Bola teda vybraná domáca kontrola služby; to znamená, že entita, ktorá má prístup k účastníckej databáze a priamo spolupracuje s platformami služby, sa vždy nachádza na domácej sieti užívateľa.

2.1.10 Vývoj služby

Dôležitosť dostupnosti variabilnej platformy služby a možnosť rýchleho spustenia nových služieb znamenala, že starý spôsob štandardizácie kompletných sad telekomunikačných služieb, aplikácií a doplnkových služieb už nie je prijateľný. 3GPP teda znamená štandardizáciu schopností služby a nie samotných služieb [3GPP TS 22.101]. IMS architektúra by mala obsahovať rámec služby, ktorý poskytuje potrebné funkcie pre podporu hlasu, videa, multimédií, posielania správ, zdieľania súborov, prenosu dát, hrania hier a základných doplnkových služieb v rámci IMS.

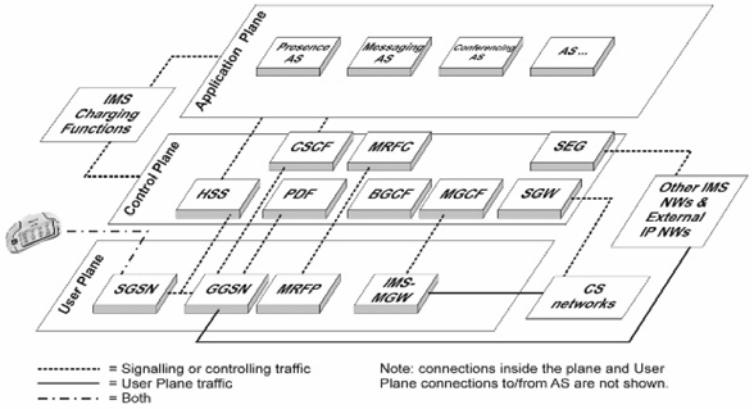
2.1.11 Vrstvený dizajn

3GPP sa rozhodlo použiť vrstvený prístup k architektonickému dizajnu. To znamená, že prenos a služby nosičov sú oddelené od signalizačnej siete IMS a služieb správy relácie. Okrem signalizačnej siete IMS sú poskytované ďalšie služby. Obrázok 2.5 znázorňuje dizajn.
V niektorých prípadoch môže byť nemožné rozlíšiť medzi funkčnosťou na horných a dolných úrovniach. Vrstvený prístup sa zameriava na minimálnu závislosť medzi vrstvami. Výhodou je, že uľahčuje neskoršie pridávanie nových prístupových sietí do systému. Prístup do IMS prostredníctvom bezdrôtovej lokálnej počítačovej siete (Wireless Local Area Network - WLAN) bol pridaný v 3GPP Release 6 a pevný širokopásmový prístup k IMS je štandardizovaný v Release 7.

Vrstvený prístup zvyšuje dôležitosť aplikačnej vrstvy, keďže sú služby navrhnuté tak, aby pracovali nezávisle od prístupovej siete a IMS je vybavený na premostenie medzery medzi nimi. Či už účastník používa mobilný telefón alebo PC klienta pre komunikáciu, budú použité rovnaké funkcie prístupnosti a zoznamu skupín v IMS. Rôzne služby majú rôzne požiadavky. Tie zahrňujú:

- šírku pásma;
- oneskorenie;
- výpočtový výkon zariadenia.

To znamená, že aby mohli byť rôzne služby správne vykonané musí byť sieť vybavená kontrolovaným prístupom a servisnou logikou pre multimediálne služby. Funkčnosť viacnásobného prístupu je zabudovaná do architektúry IMS, ktorá ponúka pevným a mobilným operátorom spôsob, ako umožniť konvergentné riešenie z pevného smerom na mobilné. To umožní poskytovateľom služby využiť charakteristiky a schopnosti aktuálne zvoleného zariadenia a jeho spôsob prístupu na internet a dynamicky to prispôsobovať.



Obrázok 2.5 IMS a vrstvená architektúra

IMS Charging Functions – Účtovacie funkcie IMS
Application plane – Aplikačná rovina
Control plane – Kontrolná rovina
User Plane – Užívateľská rovina
Other IMS NWs & External IP NWs - Iné IMS NW a externé IP NW
CS networks - CS siete
Signalling or controlling traffic - Signalizácia alebo kontrola prevádzky
User Plane Traffic – Prevádzka na užívateľskej rovine
Both - Obidva

Note: connection inside the plane and User Plane connections to/from AS are not shown. – Poznámka: spojenia v prepojeniach roviny a užívateľskej roviny do/z AS nie sú zobrazené.

2.1.12 Nezávislosť prístupu

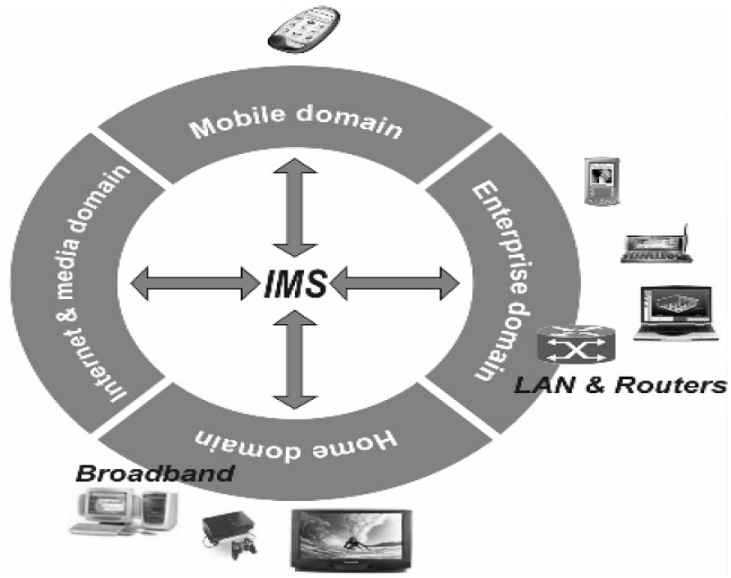
IMS bol pôvodne navrhnutý tak, aby bol nezávislý od prístupu, aby IMS služby mohli byť poskytované cez akékoľvek siete s IP konektivitou (napr. GPRS, WLAN, širokopásmová prístupová x-digitálna účastnícka linka). Nanešťastie špecifikácie Release 5 IMS obsahujú niektoré vlastnosti špecifické pre GPRS. V Release 6 (napr. GPRS) sú otázky špecifické pre prístup oddelené od základného popisu IMS a IMS architektúra sa vracia k svojmu pôvodnému stavu (t.j. nezávislý prístup). Obrázok 2.6 znázorňuje rôzne typy sieti nezávislé od prístupu, na ktorých môže fungovať IMS. Tieto zahŕňajú pevné širokopásmové pripojenie, WLAN, GPRS a UMTS. Ako príklad je použité GPRS.

2.2 Popis entít a funkčností súvisiacich IMS

Táto časť sa venuje IMS entitám a kľúčovým funkčnostiam. Tieto entity môžu byť rozdelené približne do šiestich hlavných kategórií:

- Správa relácie a rodina smerovačov (CSCF).
- Databázy (HSS, SLF).
- Služby (aplikačný server, MRFC, MRFP).
- Vzájomne komunikujúce funkcie (BGCF, MGCF, IMS-MGW, SGW).
- Podporné funkcie (PDF, SEG, THIG).
- Účtovanie.

Je dôležité pochopiť, že špecifikácie IMS sú nastavené tak, aby interná funkčnosť sieťových entít nebola špecifikovaná detailne. Miesto toho špecifikácie popisujú referenčné body medzi entitami a funkčnosti podporované v referenčných bodoch. Napríklad ako získa CSCF užívateľské údaje z databáz?



Obrázok 2.6 IMS nezávislý od prístupu

Mobile domain - Mobilná doména
Internet & media domain - Internetová a mediálna doména
Entreprise domain – Podniková doména
Home domain – Domáca doména

2.2.1 Riadiace funkcie relácie volania (Call Session Control Functions - CSCF)

Existujú tri rôzne druhy riadiacich funkcií relácie volania (Call Session Control Functions - CSCF): Proxy-CSCF (P-CSCF), Obslužná-CSCF (Serving-CSCF - S-CSCF) a Dotazovacia-CSCF (Interrogating-CSCF - I-CSCF). Každá CSCF má svoje špeciálne úlohy a tieto úlohy sú popísané v nasledujúcich pododdieloch. Pre všetky CSCF je spoločné, že všetky zohrávajú úlohu počas registrácie a vytvorenia relácie a vytvárajú SIP smerovací mechanizmus. Okrem toho sú všetky funkcie schopné poslať účtovacie údaje offline účtovacej funkcii. Existujú niektoré spoločné funkcie, ktoré sú P-CSCF a S-CSCF schopné vykonávať. Obe entity sú schopné uvoľniť relácie v prospech užívateľa (napr. keď S-CSCF rozpozná reláciu zavesenia alebo P-CSCF dostane upozornenie, že nosič média je stratený) a sú schopné skontrolovať obsah nákladu popisného protokolu relácie (Session Description Protocol –SPD) a skontrolovať, či obsahuje typy médií alebo kodeky, ktoré nie sú pre užívateľa povolené. Keď sa navrhovaný SPD nehodí do politiky operátora, CSCF odmietne požiadavku a pošle UE chybovú správu SIP.

Proxy riadiaca funkcia relácie volania (Proxy Call Session Control Function - P-CSCF)

Proxy riadiaca funkcia relácie volania (Proxy Call Session Control Function - P-CSCF) je prvý kontaktný bod pre užívateľov v rámci IMS. To znamená, že každá SIP signalizácia prevádzky z UE bude poslaná P-CSCF. Podobne každé ukončenie SIP signalizácie zo siete je poslané z P-CSCF do UE. Existujú štyri jedinečné úlohy priradené P-CSCF: SIP kompresia, IPSec bezpečnostné spojenie, interakcia s funkciou rozhodovania politiky (Policy Decision Function - PDF) a rozpoznanie núdzovej relácie.

Keďže SIP protokol je signalizačný protokol na báze textu, obsahuje veľký počet hlavičiek a parametrov hlavičiek, vrátane rozšírení a informácií týkajúcich sa bezpečnosti, čo znamená, že veľkosti ich správ sú vyššie ako pri binárne kódovaných protokoloch. Pre rýchlejšie vytvorenie relácie 3GPP nariadil podporu SIP kompresie medzi UE a P-CSCF. P-CSCF musí komprimovať správy ak UE signalizovalo, že chce dostať signalizačné správy skomprimované.

P-CSCF zodpovedá za dodržiavanie bezpečnostných asociácií (Security Associations - SAs) a použitie ochrany integrity a dôvernosti SIP signalizácie. To je zabezpečené počas registrácie SIP, keď UE a P-CSCF vyjednávajú IPSec SAs. Po počiatočnej registrácii je P-CSCF schopná aplikovať ochranu integrity a dôvernosti SIP signalizácie.

P-CSCF má za úlohu prenášať informácie týkajúce sa relácie a médií funkcii PDF, keď chce operátor použiť SBLP. Na základe získaných informácií je PDF schopná odvodiť informáciu o autorizovanej IP QoS, ktorá bude ďalej postúpená GGSN, keď GGSN potrebuje vykonať lokálnu politiku na založenú na službe pred prijatím sekundárnej PDP kontextovej aktivácie. Okrem toho prostredníctvom PDF je IMS schopný dodať IMS účtovacie korelačné informácie do GPRS siete a prostredníctvom PDF je IMS tiež schopný získať GPRS účtovacie korelačné informácie z GPRS siete. To umožňuje zlúčiť záznamy o účtovacích údajoch pochádzajúcich z IMS a GPRS sietí v platobnom systéme.

Núdzové relácie IMS ešte nie sú plne špecifikované (prebiehajúce práce na Release 7), je teda dôležité, že sieť IMS rozpozná pokusy o núdzovú reláciu a vedie UMTS UE k použitiu CS siete pre núdzové relácie. Takéto rozpoznanie je úlohou P-CSCF. Táto funkčnosť nezmizne, keď sú podporované IMS núdzové relácie, keďže v niektorých prípadoch roamingu je možné, že UE samotné nerozpozná, že užívateľ

vytočil núdzové číslo. Plánovanou funkciou v Release 7 je, aby P-CSCF bola schopná vybrať núdzovú CSCF pre riadenie núdzovej relácie. Tento výber je potrebný, pretože v prípadoch IMS roamingu sa priradená S-CSCF nachádza v domácej sieti a domáca S-CSCF nie je schopná smerovať požiadavku správnemu núdzovému centru.

Dotazovacia riadiaca funkcia relácie volania (Interrogating Call Session Control Function - I-CSCF)

Dotazovacia riadiaca funkcia relácie volania (Interrogating Session Control Function - I-CSCF) je kontaktným bodom v sieti operátora pre všetky spojenia smerujúce k účastníkovi tohto sieťového operátora. Existujú štyri jedinečné funkcie priradené I-CSCF:

- Získanie názvu ďalšieho hopu (buď S-CSCF alebo aplikačný server) z domáceho účastníckeho servera (Home Subscriber Server - HSS).
- Priradenie S-CSCF na základe schopností získaných z HSS. K priradeniu S-CSCF dôjde, keď sa užívateľ registruje na sieť alebo keď užívateľ príjme SIP požiadavku pričom nie je registrovaný na sieti, ale má služby vzťahujúce sa k neregistrovanému stavu (napr. hlasová pošta).
- Smerovanie prichádzajúcich požiadaviek ďalej k priradenej S-CSCF alebo aplikačnému serveru.
- Poskytnutie funkčnosti medzisieťovej brány ukrývajúcej topológiu (Topology Hiding Inter-network Gateway - THIG).

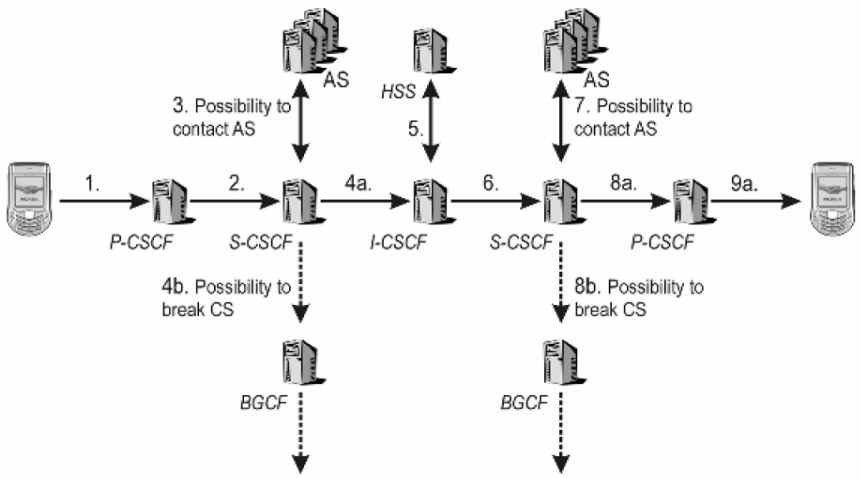
Obslužná riadiaca funkcia relácie volania (Serving Call Session Control Function - S-CSCF)

Obslužná riadiaca funkcia relácie volania (Serving Call Session Control Function - S-CSCF) je ústredným bodom IMS, keďže je zodpovedná za riadenie registračných procesov, rozhodnutí o smerovaní a udržovanie relačných stavov a ukladanie profilu(ov) služby. Keď užívateľ odošle registračnú požiadavku, bude nasmerovaná na S-CSCF, ktorá stiahne autentifikačné údaje z HSS. Na základe autentifikačných údajov vytvorí výzvu pre UE. Po prijatí odpovede a jej overení S-CSCF prijme registráciu a začne

dohliadať na registračný status. Po tejto procedúre je užívateľ schopný spustiť a prijať IMS služby. S-CSCF ďalej sťahuje profil služby z HSS ako súčasť registračného procesu.

Profil služby je súbor informácií špecifických pre užívateľa, ktoré sú trvalo uložené v HSS. S-CSCF stiahne profil služby priradený k určitej verejnej užívateľskej identite (napr. *joe.doe@ims.example.com*), keď je táto konkrétna užívateľská identita registrovaná v IMS. S-CSCF použije informácie zahrnuté v profile služby pre rozhodnutie kedy a hlavne ktorý aplikačný(é) server(y) bude(ú) kontaktovaný(á), keď užívateľ pošle SIP požiadavku alebo príjme od niekoho požiadavku. Okrem toho môže profil služby zahrňovať ďalšie pokyny o tom, aký typ mediálnej politiky má S-CSCF aplikovať - napríklad môže stanoviť, že užívateľ je oprávnený použiť len zvukové a aplikačné mediálne komponenty, ale nie obrazové mediálne komponenty.

S-CSCF je zodpovedná za kľúčové rozhodnutia o smerovaní, keďže prijíma všetky relácie a transakcie, ktoré vyvolá a ukončí UE. Keď S-CSCF príjme požiadavku od UE cez P-CSCF, musí sa rozhodnúť, či pred ďalším odoslaním požiadavky kontaktuje aplikačné servery. Po prípadnej interakcii s aplikačným(i) serverom(mi) S-CSCF buď pokračuje reláciu v IMS alebo prepne na iné domény (CS alebo iná IP sieť). Okrem toho ak UE používa číslo mobilnej stanice ISDN (Mobile Station ISDN – MSISDN) na adresovanie volanej strany, pred ďalším odoslaním požiadavky S-CSCF skonvertuje číslo MSISDN (napr. tel URL) do formátu jednotného identifikátora zdroja SIP (Universal Resource Identifier (URI)), keďže IMS nesmeruje požiadavky na báze MSISDN čísel. S-CSCF tiež prijíma všetky požiadavky, ktoré budú ukončené v UE. Aj keď S-CSCF pozná IP adresu UE z registrácie, smeruje všetky požiadavky cez P-CSCF, keďže P-CSCF zodpovedá za SIP kompresiu a bezpečnostné funkcie. Pred odoslaním požiadavky funkcii P-CSCF môže S-CSCF nasmerovať požiadavku napríklad na aplikačný(é) server(y), pričom skontroluje prípadné pokyny na presmerovanie. Obrázok 2.7 znázorňuje úlohu S-CSCF v rozhodnutiach o smerovaní. S-CSCF je ďalej schopná poslať informácie súvisiace s účtovaním do Online účtovacieho systému pre účely online účtovania (napr. podpora predplatiteľov).



Obrázok 2.7 S-CSCF smerovanie a nastavenie základnej relácie IMS.

Possibility to contact AS – Možnosť kontaktovať AS
Possibility to break CS – Možnosť prepnúť CS

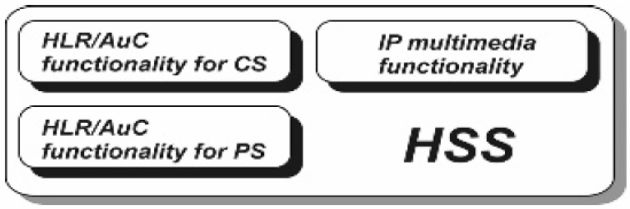
2.2.2 Databázy

V IMS architektúre existujú dve hlavné databázy: domáci účastnícky server (Home Subscriber Server - HSS) a funkcia lokalizátora prihlásenia (Subscription Locator Function - SLF).

HSS je hlavným dátovým úložiskom pre všetky účastnícke údaje a údaje týkajúce sa služby z IMS. Medzi hlavné údaje uložené v HSS patria užívateľské identity, registračné informácie, prístupové parametre a informácie spúšťajúce službu [3GPP TS 23.002]. Užívateľské identity tvoria dva typy: súkromné a verejné užívateľské identity. Súkromná užívateľská identita je užívateľská identita, ktorá je priradená operátorom domácej siete a používa sa na také účely, ako napríklad registrácia a autorizácia, zatiaľ čo verejná užívateľská identita je identita, ktorú ostatní užívatelia môžu použiť pre vyžiadanie komunikácie s koncovým užívateľom. Prístupové parametre IMS sa používajú pre nastavenie relácie a zahŕňajú parametre ako autentifikácia užívateľa, autorizácia roamingu a pridelené názvy S-CSCF. Informácia spúšťajúca službu umožní vykonanie SIP služby. HSS tiež poskytuje požiadavky špecifické pre užívateľa týkajúce sa schopností S-CSCF. Túto informáciu použije I-CSCF pre vybranie najvhodnejšej S-CSCF pre užívateľa. Okrem funkcií súvisiacich s funkčnosťou IMS, HSS obsahuje podskupinu funkčnosti Registra domácich lokácií a Autentifikačného centra (Home Location Register

and Authentication Center - HLR/AUC) vyžadovanú paketovo spínanou (PS) doménou a obvodovo spínanou (CS) doménou. Táto štruktúra HSS je znázornená na Obrázku 2.8 Funkčnosť HLR sa vyžaduje pre poskytnutie podpory entitám PS domény, ako SGSN a GGSN. To umožní účastnícky prístup k službám PS domény. Podobne HLS poskytuje podporu aj entitám CS domény, ako MSC/MSC servery. To umožňuje účastnícky prístup k službám CS domény a podporuje roaming pre siete Globálneho systému pre mobilnú komunikáciu (Global System for Mobile Communications -GSM)/UMTS CS domény. AUC uloží tajný kľúč pre každého mobilného účastníka, ktorý sa použije pre vytvorenie dynamických bezpečnostných údajov pre každého mobilného účastníka. Údaje sú použité pre vzájomnú autentifikáciu medzinárodnej identity mobilného účastníka (International Mobile Subscriber Identity (IMSI) a siete. Bezpečnostné údaje sú tiež použité pre poskytnutie ochrany integrity a pre šifrovanie rádiovej komunikácie medzi UE a sieťou. V domácej sieti môže byť viac ako jeden HSS, v závislosti od počtu mobilných účastníkov, kapacity zariadenia a organizácie siete. Medzi HSS a inými sieťovými entitami existujú viaceré referenčné body.

SLF sa používa ako rozlišovací mechanizmus, ktorý umožňuje I-CSCF, S-CSCF a AS nájsť adresu HSS, ktorá uchováva účastnícke údaje pre danú užívateľskú identitu po tom, sieťový operátor nasadil viaceré a samostatne adresovateľné HSS (Obrázok 2.12).



Obrázok 2.8 Štruktúra HSS

HLR/AuC functionality for CS - Funkčnosť HLR/AuC pre CS
HLR/AuC functionality for PS - Funkčnosť HLR/AuC pre PS
IP multimedia functionality – IP multimediálna funkčnosť

2.2.3 Funkcie služby

Tri funkcie boli kategorizované ako funkcie súvisiace so službou IMS a to riadiaca jednotka funkcie multimediálnych zdrojov (Multimedia Resource Function Controller - MRFC), procesor funkcie multimediálnych zdrojov (Multimedia Resource Function Processor – MRFP) a aplikačný server (Application Server – AS).

Vzhľadom na to, že dizajn je založený na vrstvách, AS sú skôr funkciami na IMS ako samostatnými IMS entitami. AS sú tu však popísané ako časť IMS funkcií, pretože AS sú entity, ktoré poskytujú multimediálne služby s pridanou hodnotou v IMS, ako napríklad prístupnosť a Push to talk cez mobilný telefón. AS sídli v domácej sieti užívateľa alebo v umiestnení u tretej strany. Tretia strana tu predstavuje sieť alebo samostatný AS. Hlavné funkcie AS sú:

- Možnosť spracovať a ovplyvniť prichádzajúcu SIP reláciu prijatú z IMS.
- Schopnosť vytvoriť SIP požiadavky.
- Schopnosť poslať účtovné informácie účtovacím funkciám.

Ponúkané služby nie sú obmedzené len na služby založené na SIP, keďže operátor je schopný ponúknuť prístup k službám na základe prostredia služieb (Service Environment - CSE) s prispôsobenými aplikáciami pre zdokonalenú logiku mobilnej siete (Customized Applications for Mobile network Enhanced Logic - CAMEL) a otvorenej architektúry služby (Open Service Architecture - OSA) pre svojich účastníkov IMS [3GPP TS 23.228]. AS je pojem používaný všeobecne pre vystihnutie správania SIP AS, OSA Servera pre spôsobilosť služby (Service Capability Server - SCS) a CAMEL funkcie prepájania IP multimediálnej služby (IP Multimedia Service Switching Function – IM-SSF).

Pomocou OSA môže operátor využiť také vlastnosti spôsobilosti služby ako kontrola hovoru, užívateľská interakcia, užívateľský status, kontrola dátovej relácie, schopnosti terminálu, správa účtu, účtovanie a riadenie politiky pre vývoj služieb [3GPP TS 29.198]. Ďalšou výhodou OSA rámca je, že môže byť použitý ako štandardizovaný mechanizmus pre poskytovanie AS tretích strán pre IMS bezpečnou cestou, keďže samotné OSA obsahuje počiatočné prístupové, autentifikačné, autorizačné, registračné a odhaľovacie schopnosti (S-CSCF neposkytuje autentifikačnú a bezpečnostnú funkčnosť

pre bezpečný prístup tretích strán k IMS). Keďže o podpore OSA služieb rozhoduje operátor, nie je architektonicky vhodné podporovať OSA protokoly a vlastnosti vo viacnásobných entitách. OSA SCS sa teda používa pre ukončenie SIP signalizácie z S-CSCF. OSA SCS používa aplikačné programové rozhranie (Application Program Interface – API) pre komunikáciu s aktuálnym OSA aplikačným serverom.
IM-SSF bola zavedená do architektúry IMS pre podporu odkazových služieb, ktoré sú vyvinuté v CSE. Zabezpečuje sieťové vlastnosti CAMEL (spúšťacie detekčné body, CAMEL, Stroj s konečným počtom stavov pre prepájanie služby atď) a vzájomne komunikuje s rozhraním aplikačnej zložky CAMEL (CAMEL Application Part – CAP).

SIP AS je server na báze SIP, ktorý zabezpečuje širokú škálu multimediálnych služieb s pridanou hodnotou. SIP AS by mohol byť použitý pre poskytovanie prístupnosti, Push to talk cez mobilný telefón a konferenčných služieb.

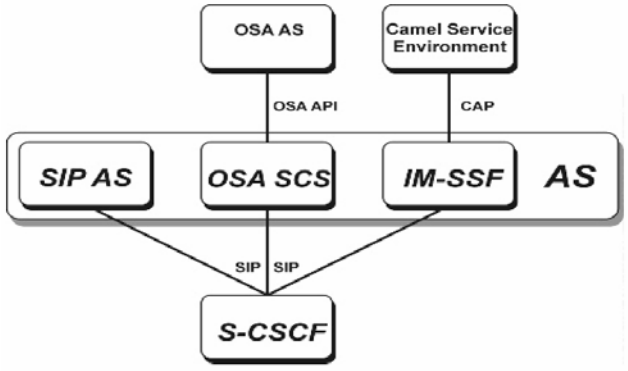
Obrázok 2.9 zobrazuje, akým spôsobom sú rôzne funkcie prepojené. Z hľadiska S-CSCF SIP AS, OSA server pre spôsobilosť služby a IM-SSF vykazujú rovnaké správanie referenčného bodu.

AS môže byť zameraný na jednu službu a užívateľ môže mať viac ako jednu službu, jeden účastník môže mať teda jeden alebo viac AS. Okrem toho v jednej relácii môže byť zahrnutý jeden alebo viac AS. Napríklad operátor môže mať jeden AS pre kontrolu ukončenia prevádzky užívateľovi na základe užívateľských preferencií (napr. presmerovanie všetkých prichádzajúcich multimediálnych relácií na telefónny záznamník medzi 17.00 a 7.00) a iný AS na prispôsobenie obsahu okamžitých správ schopnostiam UE (veľkosť obrazovky, počet farieb, atď).

MFRC a MRFP spolu poskytujú mechanizmy pre služby súvisiace s nosičmi, ako vedenie konferencií, oznamy užívateľovi alebo transkódovanie nosičov v architektúre IMS. MRFC má za úlohu riadiť SIP komunikáciu do a z S-CSCF a kontrolovať MRFP. MRFP zas poskytuje zdroje na užívateľskej rovine, ktoré vyžaduje a určí MRFC. MRFP vykonáva nasledujúce funkcie:

- Mixovanie prichádzajúcich mediálnych tokov (napr. pre viaceré strany).
- Zdroj mediálneho toku (pre multimediálne oznamy).
- Spracovanie mediálneho toku (napr. zvukové transkódovanie, mediálna analýza) [3GPP TS23.228, TS 23.002].

V súčasnosti je úloha MRFC a MRFP v architektúre IMS menej významná, pretože v konferenčnej práci IMS je [3GPP TS 24.147] MRFC lokalizovaná spoločne s AS a referenčný bod medzi MRFC a MRFP nie je zatiaľ vhodne definovaný.



Obrázok 2.9 Vzťah medzi rôznymi typmi aplikačných serverov.

CAMEL Service Environment - Prostredie služby CAMEL

2.2.4 Vzájomne komunikujúce funkcie

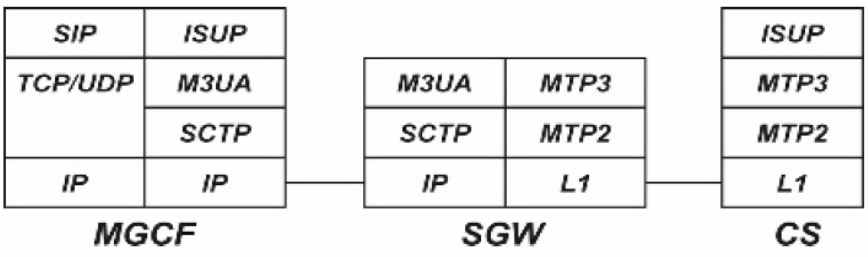
Táto časť predstavuje štyri spolupracujúce funkcie, ktoré sú potrebné pre výmenu signalizácie a médií medzi IMS a CS CN.

Bolo vysvetlené, že S-CSCF rozhoduje, kedy prepne do CS CN. Pre prepnutie S-CSCF pošle požiadavku na SIP reláciu riadiacej funkcii prepínacej brány (Breakout Gateway Control Function - BGCF); potom si vyberie, kde dôjde k prepnutiu do CS domény. Výsledkom výberového procesu môže byť buď prepnutie v tej istej sieti, v ktorej sa nachádza BGCF alebo v inej sieti. Ak dôjde k prepnutiu v tej istej sieti, potom BGCF zvolí riadiacu funkciu mediálnej brány (Media Gateway Control Function – MGCF) pre ďalšie riadenie relácie. Ak k prepnutiu dôjde v inej sieti, BGCF pošle reláciu inej BGCF vo vybranej sieti. Druhá možnosť umožní presmerovanie signalizácie a média cez IP blízko k volanému užívateľovi.

Keď požiadavka na SIP reláciu zasiahne MGCF, táto uskutoční konverziu protokolov medzi SIP protokolmi a užívateľskou zložkou ISDN (ISDN User Part – ISUP) alebo riadením hovoru nezávisle od nosiča (Bearer Independent Call Control (BICC) a pošle skonvertovanú požiadavku cez signalizačnú bránu (Signalling Gateway) do CS

CN. SGW vykoná konverziu signalizácie (obidvoma smermi) na úrovni prenosu medzi prenosom signalizácie na báze IP (napr. medzi Sigtran SCTP/IP a SS7 MTP) a prenosom signalizácie na báze Signalizačného systému č.7 (SS7). SW neinterpretuje správy aplikačnej vrstvy (napr. BICC, ISUP), ako je to znázornené na Obrázku 2.10. MGCF ovláda tiež mediálnu bránu IMS (IMS Media Gateway – IMS-MGW). IMS-MGV zabezpečuje spojenie na užívateľskej rovine medzi CS CN sieťami a IMS. Ukončí kanály nosiča z CS siete a mediálne toky z chrbticovej siete (napr. RTP toky v IP sieti alebo AAL2/ATM spojenia v ATM chrbticovej sieti), vykonáva konverziu medzi týmito ukončeniami a v prípade potreby uskutočňuje transkódovanie a spracovanie signálu pre užívateľskú rovinu. Okrem toho je IMS-MGW schopná poskytnúť tóny a oznamy CS užívateľom.

Podobne je aj riadenie signalizácie všetkých prichádzajúcich hovorov od užívateľa CS užívateľovi IMS smerované do MGCF, ktorá vykoná všetky potrebné konverzie protokolov a pošle I-CSCF požiadavku SIP relácie na ukončenie relácie. Zároveň MGCF vzájomne komunikuje s IMS-MGW a zaistí potrebné zdroje IMS-MGW na užívateľskej rovine.



Obrázok 2.10 Konverzia signalizácie v SGW.

2.2.5 Podporné funkcie

PDF zodpovedá za prijímanie rozhodnutí o politike na základe informácií o relácii a médiách získaných z P-CSCF. Plní funkciu rozhodovacieho bodu politiky pre riadenie SBLP.

Vytvorenie relácie v IMS zahŕňa výmenu správ na úrovni koncového zariadenia pomocou SIP a SDP. Počas výmeny správ UE vyjedná sadu mediálnych charakteristík (napr. spoločný(e) kodek(y)). Ak operátor použije SBLP, P-CSCF odošle PDF príslušné

SDP informácie zároveň s určením pôvodcu. PDF príslušným spôsobom pridelí a vráti autorizačnú známku, ktorú P-CSCF postúpi UE. PDF zaregistruje a autorizuje IP toky zvolených mediálnych komponentov namapovaním z SPD parametrov do autorizovancýh IP QoS parametrov pre prenos na prístupovú sieť - t.j. GGSN v prípade UMTS/GPRS prístupu (ďalej v texte sa predpokladá GPRS prístup) – prostredníctvom Go rozhrania. Po prijatí PDP kontextovej aktivácie alebo zmeny GGSN požiada PDF o autorizačné informácie. PDF porovná prijaté záväzné informácie s uloženými autorizačnými informáciami a vráti autorizačné rozhodnutie. Ak sú záväzné informácie potvrdené ako správne, PDF oznámi GGSN podrobnosti o autorizácii média v rozhodnutí.

Okrem rozhodnutia o autorizácii nosiča PDF príjme informácie o tom, kedy bol PDP kontext riadený politikou SBLP uvoľnený alebo kedy UE stratilo/obnovilo svoj(e) rádiový(é) nosič(e) alebo kedy PDP riadený politikou SBLP používa tokovú alebo konverzačnú prevádzkovú triedu. Na základe týchto informácií je PDP schopný informovať P-CSCF o udalosti, ktorá sa vyskytla. To umožní P-CSCF previesť účtovanie a môže tiež začať uvoľňovať IMS reláciu v prospech užívateľa. PDF môže tiež požiadať GGSN o deaktivovanie konkrétneho PDP kontextu riadeného politikou SBLP.

Bezpečnostná brána (Security Gateway – SEG) má za úlohu chrániť prevádzku na riadiacej rovine medzi bezpečnostnými doménami. Bezpečnostná doména predstavuje sieť, ktorá je riadená jedným správnym orgánom. Väčšinou sa zhoduje s hranicami operátora. SEG je umiestnená na hranici bezpečnostnej domény a vnúti bezpečnostnú politiku bezpečnostnej domény ostatným SEG v cieľovej bezpečnostnej doméne. V IMS je celá prevádzka v rámci IMS smerovaná cez SEG hlavne vtedy, keď sa jedná o prevádzku medzi doménami, čo znamená, že bezpečnostná doména, z ktorej pochádza je iná ako doména, kde je prijatá. Pri ochrane IMS prevádzky medzi doménami je nariadená dôvernosť ako aj integrita údajov a autentifikácia [SGPP TS 33.203].

Funkčnosť THIG by mohla byť použitá pre ukrytie konfigurácie, kapacity a topológie siete mimo siete operátora. Ak operátor chce použiť funkčnosť ukrývania, musí operátor umiestniť funkciu THIG na smerovaciu cestu, keď prijíma požiadavky alebo odpovede z iných IMS sietí. THIG musí byť umiestnená v smerovacej ceste aj pri posielaní požiadaviek alebo odpovedí iným IMS sieťam. THIG vykonáva zakódovanie a dekódovanie všetkých hlavičiek, ktoré odhaľujú informácie o topológii o IMS sieti operátora.

2.2.7 GPRS entity

Obslužný podporný uzol GPRS (Serving GPRS Support Node – SGSN)

Obslužný podporný uzol GPRS (Serving GPRS Support Node – SGSN) spája RAN s paketovou základnou sieťou. Zodpovedá za vykonávanie kontroly a funkcií riadenia prevádzky pre PS doménu. Kontrolná zložka obsahuje dve základné funkcie: správa mobility a správa relácie. Správa mobility sa zaoberá umiestnením a stavom UE a autentifikuje účastníka UE. Kontrolná zložka správy relácie sa zaoberá kontrolou prijatia spojenia a akýmikoľvek zmenami v existujúcich dátových spojeniach. Kontroluje tiež služby a zdroje 3G siete. Riadenie prevádzky je tou zložkou správy relácie, ktorá je vykonávaná. SGSN funguje ako brána pre tunelovanie užívateľských údajov: inými slovami, prenáša užívateľskú prevádzku medzi UE a GGSN. V rámci tejto funkcie SGSN tiež zaisťuje, že je pre spojenia zabezpečená príslušná QoS. Okrem toho SGSN generuje účtovacie informácie.

Stykový podporný uzol GPRS (Gateway GPRS Support Node – GGSN)

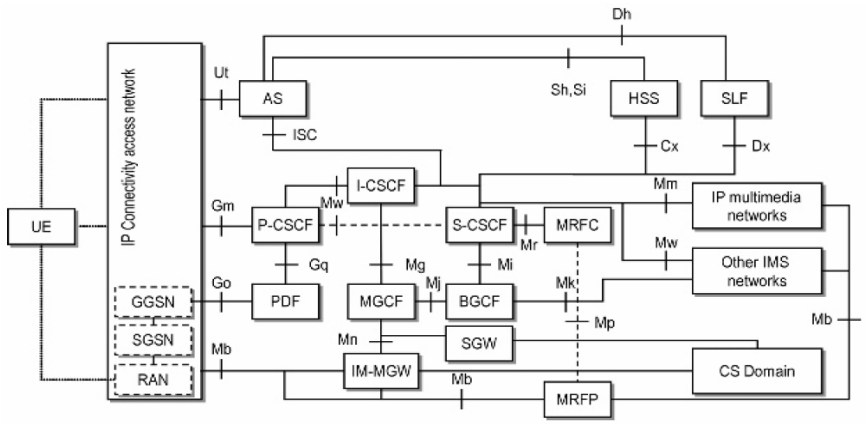
Stykový podporný uzol GPRS (Gateway GPRS Support Node – GGSN) poskytuje spoluprácu s externými paketovými sieťami. Základnou funkciou GGSN je spojiť UE s externými dátovými sieťami, kde sídlia aplikácie a služby na báze IP. Externou dátovou sieťou by mohol byť napríklad IMS alebo internet. Inými slovami, GGSN smeruje IP pakety obsahujúce SIP signalizáciu z UE do P-CSCF a naopak. Okrem toho má GGSN na starosti smerovanie IMS mediálnych IP paketov k cieľovej sieti (napr. GGSN v koncovej sieti). Poskytnutá vzájomne komunikujúca služba je realizovaná vo forme prístupových bodov, ktoré sa vzťahujú k rôznym sieťam, na ktoré sa chce účastník pripojiť. Vo väčšine prípadov má IMS svoj vlastný prístupový bod. Keď UE aktivuje nosič (PDP kontext) k prístupovému bodu (IMS), GGSN pridelí UE dynamickú IP adresu. Táto pridelená IP adresa sa použije v IMS registrácii a keď UE spustí reláciu ako kontaktná adresa UE. Okrem toho GGSN dohliada a kontroluje použitie PDP kontextu pre IMS mediálnu prevádzku a generuje účtovacie informácie.

2.3 Referenčné body IMS

Táto časť vysvetľuje akým spôsobom sú popísané sieťové jednotky spojené medzi sebou a aký protokol je použitý; okrem toho vykresľuje architektúru IMS (Obrázok 2.11). Nájdete tu tiež prehľad referenčných bodov na báze SIP (t.j. kde je použitý SIP a sú zahrnuté hlavné procedúry).

Aby bola zachovaná prehľadnosť, nie je možné zahrnúť všetko do jedného obrázku; venujte preto prosím pozornosť nasledovným veciam:

- Obrázok 2.11 neznázorňuje funkcie alebo referenčné body súvisiace s účtovaním.
- Obrázok neznázorňuje rôzne typy AS.
- Obrázok neznázorňuje spojenia na užívateľskej rovine medzi rôznymi IMS sieťami a AS.
- Obrázok neznázorňuje SEG v referenčných bodoch Mm, Mk, Mw.
- Bodkovaná čiara medzi entitami znázorňuje priame spojenie.
  IMS kontrola služby (IMS Service Control), Cx, Dx, Mm, Mw končia v S-CSCF a v I-CSCF.



Obrázok 2.11 Architektúra IMS.

IP Connectivity Access network – Prístupová sieť s IP konektivitou
IP multimedia networks – IP multimediálne siete
Other IMS networks – Iné IMS siete
CS Domain—CS doména

2.3.1 Referenčný bod Gm

Referenčný bod Gm spája UE a IMS. Používa sa na prenos všetkých SIP signalizačných správ medzi UE a IMS. Protipólom IMS je P-CSCF. Procedúry v referenčnom bode GM môžu byť rozdelené do troch hlavných kategórií: registrácia, kontrola relácie a transakcie:

- V registračnej procedúre UE používa referenčný bod Gm na zaslanie registračnej požiadavky s uvedením podporovaných bezpečnostných mechanizmov funkcii P-CSCF. Počas registračného procesu UE vymieňa potrebné parametre pre vlastnú autentifikáciu a autentifikáciu siete, získa implicitné registračné užívateľské identity, vyjedná potrebné parametre pre SA s P-CSCF a prípadne začne SIP kompresiu. Okrem toho sa referenčný bod Gm používa pre informovanie UE, ak dôjde k sieťou iniciovanému zrušeniu registrácie alebo sieťou iniciovanej opätovnej autentifikácii.
- Procedúry kontroly relácie obsahujú mechanizmy pre mobilne iniciované relácie a mobilne ukončené relácie. V mobilne iniciovaných reláciách sa referenčný bod Gm používa na preposlanie požiadaviek z UE do P-CSCF. V mobilne ukončených reláciách sa referenčný bod používa na preposlanie požiadaviek z P-CSCF do UE.
- Transakčné procedúry sa používajú pre odoslanie samostatných požiadaviek (napr. MESSAGE) a prijatie všetkých odpovedí (napr. 200 OK) na túto požiadavku cez referenčný bod Gm. Rozdiel medzi transakčnými procedúrami a procedúrami správy relácií je, že nie je vytvorený dialóg.

2.3.2 Referenčný bod MW

Referenčný bod Gm spája UE a IMS (hlavne s P-CSCF). Ďalej je potrebný referenčný bod na báze SIP medzi rôznymi CSCF. Tento referenčný bod sa nazýva Mw. Procedúry v referenčnom bode Mw môžu byť rozdelené do troch hlavných kategórií – registrácia, správa relácie a transakcia.

- V registračnej procedúre P-CSCF používa referenčný bod Mw na preposlanie registračnej požiadavky od UE funkcii I-CSCF. I-CSCF potom použije referenčný bod Mw pre postúpenie požiadavky funkcii S-CSCF. Nakoniec odpoveď od S-CSCF

prechádza naspäť cez referenčný bod Mw. Okrem toho S-CSCF používa referenčný bod v sieťou iniciovaných procedúrach zrušenia registrácie pre informovanie UE o sieťou iniciovanom zrušení registrácie a sieťou iniciovanej opätovnej autentifikácii pre informovanie S-CSCF, že by mala uvoľniť zdroje týkajúce sa konkrétneho užívateľa.

- Procedúry kontroly relácie obsahujú mechanizmy pre mobilne iniciované relácie a mobilne ukončené relácie. V mobilne iniciovaných reláciách sa referenčný bod Mw používa na preposielanie požiadaviek od P-CSCF do S-CSCF a od S-CSCF do I-CSCF. V mobilne ukončených reláciách sa referenčný bod Mw používa na preposielanie požiadaviek od I-CSCF do S-CSCF a od S-CSCF do P-CSCF. Tento referenčný bod sa tiež používa pre uvoľnenie sieťou iniciovaných relácií: napríklad P-CSCF by mohla iniciovať uvoľnenie relácie smerom k S-CSCF ak dostane indikáciu od PDF, že mediálne nosič(e) je(sú) stratený(é). Okrem toho sú informácie týkajúce sa účtovania prepravené cez referenčný bod Mw.
- Transakčné procedúry sa používajú pre postúpenie samostatnej požiadavky (napr. MESSAGE) a prijatie všetkých odpovedí (napr. 200 OK) na túto požiadavku cez referenčný bod Mw. Ako to už bolo uvedené, rozdiel medzi transakčnými procedúrami a procedúrami správy relácií je, že nie je vytvorený dialóg.

2.3.3 Referenčný bod IMS kontroly služby (IMS Service Control – ISC)

V architektúre IMS sú AS entity, ktoré hosťujú a vykonávajú služby ako prístupnosť, posielanie správ a preposielanie relácií. Musí teda existovať referenčný bod pre posielanie a prijímanie SIP správ medzi CSCF a jedným AS. Tento referenčný bod sa nazýva referenčný bod IMS kontroly služby (IMS Service Control – ISC) a vybraný protokol je SIP. Procedúry ISC môžu byť rozdelené na dve hlavné kategórie – smerovanie počiatočnej SIP požiadavky na AS a požiadavky iniciované AS:

- Keď S-CSCF príjme počiatočnú SIP požiadavku analyzuje ju. Na základe analýzy sa S-CSCF rozhodne smerovať požiadavku na AS pre ďalšie spracovanie. AS môže ukončiť, presmerovať alebo oprávniť požiadavku od S-CSCF.
- AS môže iniciovať požiadavku (napr. v prospech užívateľa).

2.3.4 Referenčný bod Cx

Účastnícke a servisné údaje sú trvalo uložené v HSS. Tieto centralizované údaje musí použiť I-CSCF a S-CSCF, keď sa užívateľ zaregistruje alebo príjme reláciu. Musí teda existovať referenčný bod medzi HSS a CSCF. Tento referenčný bol sa nazýva referenčný bod Cx a vybraným protokolom je priemer. Procedúry môžu byť rozdelené do troch hlavných kategórií: správa umiestnenia, riadenie užívateľských údajov a užívateľská autentifikácia. V Tabuľke 2.1 je uvedený prehľad dostupných Cx príkazov.

Procedúry správy umiestnenia

Procedúry správy umiestnenia sa môžu ďalej rozdeliť do dvoch skupín: registrácia a zrušenie registrácie a vyhľadanie umiestnenia.

Keď I-CSCF príjme požiadavku SIP REGISTER od P-CSCF cez referenčný bod Mw, vyvolá dotaz o stave užívateľskej registrácie alebo, ako je to špecifikované v štandardoch, príkaz na vyžiadanie užívateľskej autorizácie (User-Authorization-Request - UAR). Po prijatí UAR príkazu HSS pošle príkaz na odpoveď na užívateľskú autorizáciu (User-Authorization-Answer – UAA). Obsahuje Názov S-CSCF a/alebo Schopnosti S-CSCF (ak príkaz UAR nezlyhá napríklad z dôvodu, že súkromné a verejné identity prijaté v požiadavke nepatria tomu istému užívateľovi), v závislosti od súčasného stavu registrácie. S-CSCF schopnosti sú vrátené ak užívateľ ešte nemá pridelený Názov S-CSCF v HSS alebo ak I-CSCF výslovne požaduje Schopnosti S-CSCF. V opačnom prípade je vrátený názov S-CSCF. Ak sú vrátené schopnosti, I-CSCF musí vykonať výber S-CSCF.

Vyššie v texte sme vysvetlili, ako I-CSCF nájde S-CSCF, ktorá bude slúžiť užívateľovi. Keď to zrealizuje, I-CSCF prepošle požiadavku SIP REGISTER funkcii S-CSCF. Keď S-CSCF príjme požiadavku SIP REGISTER od I-CSCF, použije príkaz na vyžiadanie pridelenia servera (Server-Assignment-Request – SAR) pre komunikáciu s HSS. SAR príkaz sa použije pre informovanie HSS o tom, ktorá S-CSCF bude slúžiť užívateľovi, keď hodnota expirácie nie je rovná nule. Rovnako aj v prípade, keď je hodnota expirácie rovná nule sa príkaz SAR použije pre oznámenie skutočnosti, že S-CSCF už neslúži užívateľovi. Predpokladom pre odoslanie SAR príkazu je, že S-CSCF úspešne autentifikovala užívateľa. Po prijatí príkazu SAR HSS odpovie pomocou príkazu na odpoveď na pridelenie servera (Server-Assignment-Answer – SAA). Obsahuje

užívateľský profil založený na hodnotách nastavených v SAR požiadavke a prípadne adresy účtovacích funkcií.

Doteraz sme popísali ako sú procedúry registrácie iniciovanej užívateľom a procedúry zrušenia registrácie (iniciovaného užívateľom alebo iniciovaného S-CSCF) riadené cez referenčný bod Cx. Stále sú potrebné dodatočné operácie pre uskutočnenie sieťovo iniciovaného zrušenia registrácie (napr. z dôvodu krádeže UE alebo ukončenia prihlásenia). V tomto prípade HSS začne sieťovo iniciované zrušenie registrácie pomocou príkazu s názvom Požiadavka na ukončenie registrácie (Registration-Termination-Request – RTR). Príkaz RTR je potvrdený príkazom Odpoveď na ukončenie registrácie (Registration-Termination-Answer - RTA), ktorý jednoducho určí výsledok operácie.

V predchádzajúcom texte sme popísali ako I-CSCF používa dotaz o stave užívateľskej registrácie (príkaz UAR) pre nájdenie S-CSCF, keď príjme požiadavku SIP REGISTER. Musí teda existovať príslušná procedúra pre nájdenie S-CSCF, keď je metóda SIP iná ako REGISTER. Požadovaná procedúra by mala využívať príkaz na vyžiadanie informácie o umiestnení (Location-Info-Request - LIR). HSS odpovie príkazom na odpoveď na informáciu o umiestnení (Location-Info-Answer – LIA). Odpoveď obsahuje Názov S-CSCF a Schopnosti S-CSCF – tieto sú vrátené, ak užívateľ nemá pridelený Názov S-CSCF, v opačnom prípade je vrátené SIP URI funkcie S-CSCF.

Procedúry riadenia užívateľských údajov

Počas registračného procesu budú užívateľské údaje a údaje súvisiace so službou stiahnuté z HSS do S-CSCF cez referenčný bod Cx pomocou príkazov SAR a SAA, ako to bolo popísané v predchádzajúcom texte. Tieto údaje je však možné neskôr zmeniť, ak S-CSCF stále slúži užívateľovi. Pre aktualizáciu údajov v S-CSCF HSS iniciuje príkaz na vyžiadanie pretlačenie profilu (Push-Profile-Request – PRP). Aktualizácia prebehne hneď po zmene s jednou výnimkou: keď S-CSCF slúži neregistrovanému užívateľovi alebo S-CSCF je rezervovaná pre neregistrovaného užívateľa, a v registrovanej zložke užívateľského profilu došlo k zmene, HSS pošle príkaz PRR. Príkaz PRR je potvrdený príkazom na odpoveď na pretlačenie profilu (Push-Profile-Anwser – PPA), ktorý jednoducho určí výsledok operácie.

Tabuľka 2.1 Cx príkazy.

Názov príkazu	Účel	Skratka	Zdroj	Určenie
Požiadavka/Odpoveď na užívateľskú registráciu	Príkazy na požiadavku/odpoveď na užívateľskú registráciu (User-Authorizatio—Request/Answer (UAR/UAA) sa používajú medzi I-CSCF a HSS počas SIP registrácie pre získanie názvu SCSF alebo schopností S-CSCF pre výber S-CSCF a počas zrušenia SIP registrácie pre získanie názvu S-CSCF, keď je SIP metódou REGISTER	UAR	I-CSCF	HSS
		UAA	HSS	I-CSCF
Požiadavka/Odpoveď na pridelenie servera	Príkazy na požiadavku/odpoveď na pridelenie servera (Server-Assignment-Request/Answer - SAR/SAA) sa používajú medzi S-CSCF a HSS pre aktualizáciu názvu S-CSCF na HSS a stiahnutie údajov užívateľského profilu do S-CSCF	SAR	S-CSCF	HSS
		SAA	HSS	S-CSCF
Požiadavka/Odpoveď na informácie o umiestnení	Príkazy na požiadavku/odpoveď na informácie o umiestnení (Location-Info-Request/Answer – LIR/LIA) sa používajú medzi I-CSCF a HSS počas nastavenia SIP relácie pre získanie názvu funkcie S-CSCF, ktorá slúži užívateľovi alebo schopností S-CSCF pre výber S-CSCF	LIR	I-CSCF	HSS
		LIA	HSS	I-CSCF
Požiadavka/Odpoveď na autorizáciu multimédií	Príkazy na požiadavku/odpoveď na autorizáciu multimédií (Multimedia-Auth-Request/Answer – MAR/MAA) sa používajú medzi S-CSCF a HSS pre výmenu informácií na podporu autentifikácie medzi koncovým užívateľom a domácou sieťou IMS	MAR	S-CSCF	HSS
		MAA	HSS	S-CSCF
Požiadavka/Odpoveď na ukončenie registrácie	Príkazy na požiadavku/odpoveď na ukončenie registrácie (Registration-Termination-Request/Answer – RTR/RTA) sa používajú medzi S-CSCF a HSS, keď HSS administratívne zruší registráciu jednej alebo viacerých verejných identít užívateľa	RTR	HSS	S-CSCF
		RTA	S-CSCF	HSS
Požiadavka/Odpoveď na pretlačenie profilu	Príkazy na požiadavku/odpoveď na pretlačenie profilu (Push-Profile-Request/Answer – PPR/PPA) sa používajú medzi HSS a S-CSCF, keď sú údaje užívateľského profilu zmenené riadiacou operáciou v HSS a údaje musia byť aktualizované do S-CSCF	PPR	HSS	S-CSCF
		PPA	S-CSCF	HSS

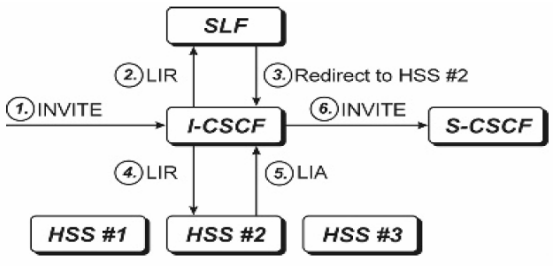
Autentifikačné procedúry

Užívateľská autentifikácia IMS je založená na predkonfigurovanom zdieľanom tajomstve. Zdieľané tajomstvá a sekvenčné čísla sú uložené v identifikačnom module IP multimediálnych služieb (IP Multimedia Services Identity Module - ISIM) v UE a v HSS na sieti. Keďže S-CSCF má na starosti užívateľskú autorizáciu, je potrebné presunúť bezpečnostné údaje cez referenčný bod Cx. Keď S-CSCF potrebuje autentifikovať užívateľa, pošle príkaz na vyžiadanie autorizácie multimédií (Multimedia-Auth-Request - MAR) serveru HSS. HSS odpovie príkazom na odpoveď na autorizáciu multimédií (Multimedia-Auth-Answer – MAA). Odpoveď obsahuje okrem iných informácií autentifikačné údaje. Zahŕňa autentifikačný vektor, ktorý je zložený z autentifikačnej schémy (napr. Digest-AKAv1-MD5), autentifikačných informácií (autentifikačná výzva RAND a známka AUTN), autorizačných informácií (očakávaná odpoveď alebo XRES), kľúča integrity a prípadne kľúča dôvernosti. Okrem toho obsahuje číslo položky, ktoré určuje poradie, v akom majú byť autentifikačné vektory použité, keď sú vrátené viaceré vektory.

2.3.5 Referenčný bod Dx

Keď boli na sieti nasadené viaceré a samostatne adresovateľné servery HSS, ani I-CSCF ani S-CSCF nevie, ktorý HSS majú kontaktovať. Musia však kontaktovať funkciu SLF ako prvú. Z tohto dôvodu bol zavedený referenčný bod Dx. Referenčný bod Dx sa vždy používa spoločne s referenčným bodom Cx. Protokol použitý pre tento referenčný bod je založený na priemere. Jeho funkčnosť je zavedená prostredníctvom smerovacieho mechanizmu poskytnutého zdokonaleným činiteľom presmerovania priemeru.

Pre získanie adresy HSS funkcia I-CSCF alebo S-CSCF pošle funkcii SLF požiadavky Cx určené pre HSS. Po prijatí adresy HSS od SLF funkcia I-CSCF alebo S-CSCF pošle požiadavky Cx serveru HSS. Obrázok 2.12 zobrazuje, akým spôsobom sa používa SLF pre nájdenie správneho HSS, keď I-CSCF príjme požiadavku INVITE a boli nasadené tri servery HSS.



Obrázok 2.12 Riešenie HSS pomocou SLF.

Redirect to HSS #2 – Presmerovať na HSS #2

2.3.6 Referenčný bod Sh

AS (SIP AS alebo OSA SCSC) môže potrebovať užívateľské údaje alebo informácie o tom, ktorému S-CSCF poslať požiadavku. Tento typ informácie je uložený v HSS. Musí teda existovať referenčný bod medzi HSS a AS. Tento referenčný bod sa nazýva referenčný bod Sh a protokolom je priemer. Procedúry sú rozdelené do dvoch hlavných kategórií: riadenie údajov a prihlásenie/upozornenie. Tabuľka 2.2 poskytuje prehľad dostupných Sh príkazov. HSS vedie zoznam serverov AS, ktoré môžu získať alebo ukladať údaje.

Riadenie údajov

Procedúry riadenia údajov zahŕňajú možnosť získať užívateľské údaje z HSS. Takéto užívateľské údaje môžu obsahovať údaje súvisiace so službou (transparentné alebo netransparentné), registračné informácie, identity, počiatočné filtračné kritéria, Názov funkcie S-CSCF slúžiacej užívateľovi, adresy účtovacích funkcií a dokonca aj informácie o umiestnení z CS a PS domén. Transparentné údaje server HSS chápe syntakticky, nie sémanticky. Sú to údaje, ktoré môže AS ukladať v HSS na podporu svojej servisnej logiky. Naopak netransparentné údaje server HSS chápe syntakticky aj sémanticky. AS používa príkaz na vyžiadanie užívateľských údajov (User-Data-Request - UDR) pre vyžiadanie údajov. Požiadavka obsahuje informácie o požadovaných údajoch. HSS odpovie odpoveďou na užívateľské údaje (User-Data-Answer – UDA).

AS môže aktualizovať transparentné údaje na HSS pomocou príkazu na vyžiadanie aktualizácie profilu (Profile-Update-Request - PUR), ktorý obsahuje údaje, ktoré majú byť aktualizované. Príkaz PUR je potvrdený príkazom na odpoveď na

aktualizáciu profilu (Profile-Update-Answer – PUA), ktorý jednoducho určí výsledok operácie.

Prihlásenie/Upozornenie

Procedúry prihlásenia/upozornenia umožňujú AS získať upozornenie, keď sú určité údaje konkrétneho užívateľa aktualizované na HSS. AS pošle príkaz na vyžiadanie upozornení o prihlásení (Subscribe-Notifications-Request – SNR), aby dostal upozornenie, keď budú užívateľské údaje uvedené v SNR príkaze zmenené na HSS. HSS potvrdí požiadavku na prihlásenie príkazom na odpoveď na upozornenia o prihlásení (Subscribe-Notifications-Answer – SNA), ktorý jednoducho určí výsledok operácie.

Ak AS odoslal SNR príkaz a vyžiadal upozornenie s typom požiadavky na prihlásenie, HSS pošle príkaz na vyžiadanie presunu upozornenia (Push-Notification-Request – PNR) serveru AS, keď došlo k zmene určitých údajov, s uvedením podrobností o zmenených údajoch. Príkaz PNR je potvrdený príkazom na odpoveď na presun upozornenia (Push-Notification-Answer – PNA), ktorý jednoducho určí výsledok operácie.

Tabuľka 2.2 Sh príkazy.

Názov príkazu	Účel	Skratka	Zdroj	Určenie
Požiadavka/Odpoveď na užívateľské údaje	Príkazy na požiadavku/odpoveď na užívateľské údaje (User-Data—Request/Answer (UAR/UAA) sa používajú pre dodanie užívateľských údajov konkrétneho užívateľa	UDR	AS	HSS
		UDA	HSS	AS
Požiadavka/Odpoveď na aktualizáciu profilu	Príkazy na požiadavku/odpoveď na aktualizáciu profilu (Profile-Udpate-Request/Answer - SAR/SAA) sa používajú pre aktualizáciu transparentných údajov v HSS	PUR	AS	HSS
		PUA	HSS	AS
Požiadavka/Odpoveď na upozornenia o prihlásení	Príkazy na požiadavku/odpoveď na upozornenia o prihlásení (Subscribe-Notifications-Request/Answer) sa používajú pre prihlásenie/odhlásenie užívateľských údajov, pre ktoré sa vyžadujú upozornenia o zmene	SNR	AS	HSS
		SNA	HSS	AS
Požiadavka/Odpoveď na presun upozornenia	Príkazy na požiadavku/odpoveď na presun upozornenia (Push-Notification-Request/Answer – MAR/MAA) sa používajú na odoslanie zmenených údajov AS	PNR	AS	HSS
		PNA	HSS	AS

2.3.7 Referenčný bod Si

Keď je AS server typu CAMEL AS (IM-SSF), používa referenčný bod Si pre komunikáciu s HSS. Referenčný bod Si sa používa pre prenos informácií CAMEL vrátane spúšťacích mechanizmov z HSS na IM-SSF. Použitý protokol je zložka mobilnej aplikácie (Mobile Application Part – MAP).

2.3.8 Referenčný bod Dh

Keď boli na sieti nasadené viaceré a samostatne adresovateľné servery HSS AS nemôže vedieť, ktorý HSS má kontaktovať. AS však musí kontaktovať funkciu SLF ako prvú. Z tohto dôvodu bol v Release 6 zavedený referenčný bod Dh. V Release 5 je správny HSS nájdený pomocou proprietárnych prostriedkov. Referenčný bod Dh sa vždy používa spoločne s referenčným bodom Sh. Protokol použitý pre tento referenčný bod je založený na priemere. Jeho funkčnosť je zavedená prostredníctvom smerovacieho mechanizmu poskytnutého zdokonaleným činiteľom presmerovania priemeru.

Pre získanie adresy HSS, AS pošle funkcii SLF požiadavku Sh určenú pre HSS. Po prijatí adresy HSS od funkcie SLF, AS pošle požiadavku Sh serveru HSS.

2.3.9 Referenčný bod Mm

Pre komunikáciu s ostatnými multimediálnymi IP sieťami je potrebný referenčný bod medzi IMS a ostatnými multimediálnymi IP sieťami. Referenčný bod Mm umožňuje funkcii I-CSCF prijať požiadavku na reláciu od iného SIP servera alebo terminálu. Podobne S-CSCF používa referenčný bod Mm na preposlanie IMS požiadavky pochádzajúcej od UE do ostatných multimediálnych sietí. V čase písania nebola poskytnutá detailná špecifikácia referenčného bodu Mm. Je však veľmi pravdepodobné, že by protokolom bol SIP.

2.3.10 Referenčný bod Mg

Referenčný bod Mg spája funkciu CS edge, MGCF s IMS (hlavne s I-CSCF). Referenčný bod umožňuje MGCF preposlať prichádzajúcu signalizáciu relácie z CS

domény do I-CSCF. Použitý protokol pre referenčný bod Mg je SIP. MGCF zodpovedá za konvertovanie prichádzajúcej signalizácie ISUP na SIP.

2.3.11 Referenčný bod Mi

Keď S-CSCF zistí, že relácia musí byť presmerovaná do CS domény, použije referenčný bod Mi na preposlanie relácie funkcii BGCF. Protokol použitý pre referenčný bod Mi je SIP. Časť 3.13 obsahuje podrobnosti o vzájomnej komunikácii IMS-CS .

2.3.12 Referenčný bod Mj

Keď BGCF príjme signalizáciu relácie cez referenčný bod Mi vyberie CS doménu, v ktorej dôjde k prepnutiu. Ak dôjde k prepnutiu v tej istej sieti, prepošle reláciu funkcii MGCF cez referenčný bod Mj. Protokol použitý pre referenčný bod Mj je SIP. Časť 3.13 obsahuje podrobnejšie informácie o vzájomnej komunikácii IMS-CS.

2.3.13 Referenčný bod Mk

Keď BGCF príjme signalizáciu relácie cez referenčný bod Mi vyberie CS doménu, v ktorej dôjde k prepnutiu. Ak dôjde k prepnutiu v tej istej sieti, prepošle reláciu funkcii BGCF v druhej sieti cez referenčný bod Mk. Protokol použitý pre referenčný bod Mk je SIP. Časť 3.13 obsahuje podrobnejšie informácie o vzájomnej komunikácii IMS-CS.

2.3.14 Referenčný bod Mn

Rozhranie Mn je kontrolný referenčný bod medzi MGCF a IMS-MGW. Rozhranie Mn kontroluje užívateľskú rovinu medzi IP prístupom a IMS-MGW (referenčný bod Mb). Kontroluje tiež užívateľskú rovinu medzi Cs prístupom (rozhrania Nb a TDM) a IMS-MGS. Rozhranie Mn je založené na H.248 a je rovnocenné s použitím (zakódovanie, odkódovanie, atď.) rozhrania Mc špecifikovaného pre kontrolu CS-MGW. Rozdiel medzi týmito dvoma rozhraniami je, že rozhranie Mn zavádza nové procedúry H.248 pre riadenie ukončenia konca IP prístupu a tiež niektoré dodatočné procedúry pre

riadenie ukončenia konca CS. H.248 sa používa predovšetkým pre vykonávanie nasledujúcich úloh:

- zaistiť alebo pripojiť ukončenia;
- pripojiť alebo odpojiť rušič ozveny k ukončeniam;
- pripojiť alebo odpojiť tóny a upozornenia k ukončeniam;
- poslať/prijať DTMF tóny.

2.3.15 Referenčný bod Ut

Referenčný bod Ut je referenčný bod medzi UE a AS. Umožňuje užívateľom bezpečne riadiť a konfigurovať ich sieťové služby súvisiace s informáciami hosťovanými na AS. Užívatelia môžu použiť referenčný bod Ut pre vytvorenie identít verejnej služby (Public Service Identities – PSIs), ako napríklad zoznam zdrojov a riadiť autorizačné politiky, ktoré používa služba. Príkladmi služieb, ktoré používajú referenčný bod Ut sú prístupnosť, Push to talk cez mobilný telefón a vedenie konferencií. AS môže poskytovať zabezpečenie pre referenčný bod Ut.
Hypertextový prenosový protokol (Hypertext Transfer Protocol – HTTP) je protokol vybraný pre referenčný bod Ut. Akýkoľvek protokol vybraný pre aplikáciu, ktorá využíva referenčný bod Ut musí byť založený na HTTP. Tento referenčný bod je štandardizovaný v Release 6. Použitie referenčného bodu Ut.

2.3.16 Referenčný bod Mr

Keď S-CSCF potrebuje aktivovať služby súvisiace s nosičom, postúpi SIP signalizáciu funkcii MRFC cez referenčný bod Mr. Funkčnosť referenčného bodu Mr nie je plne štandardizovaná: napríklad nie je špecifikované, ako S-CSCF informuje MRFC, aby prehrala konkrétne oznámenie. Použitý protokol pre referenčný bod Mr je SIP.

2.3.17 Referenčný bod Mp

Keď MRFC potrebuje kontrolovať mediálne toky (napr. vytvoriť pripojenia pre konferenčné médiá alebo zastaviť médiá v MRFP) použije referenčný bod Mp. Tento referenčný bod je v úplnom súlade so štandardmi H.248. IMS služby však môžu

vyžadovať rozšírenia. Tento referenčný bod nie je štandardizovaný v Release 5 ani v Release 6.

2.3.18 Referenčný bod Go

Je v záujme operátorov zaistiť, že QoS a zdrojové a cieľové adresy plánovanej IMS mediálnej prevádzky sa zhodujú s vyjednanými hodnotami na úrovni IMS. To vyžaduje komunikáciu medzi IMS (riadiaca rovina) a GPRS sieťou (užívateľská rovina). Referenčný bod G bol pôvodne definovaný pre tento účel. Neskôr bola pridaná účtovacia korelácia ako prídavná funkčnosť. Použitý protokol je protokol spoločnej služby otvorenej politiky (Common Open Policy Service - COPS). Procedúry Go môžu byť rozdelené do dvoch hlavných kategórií:

- Autorizácia média - čo sa týka prístupu, bod presadzovania politiky (Policy Enforcement Point – PEP) (napr. GGSN) používa referenčný bod Go pre zistenie, či požadovaná aktivácia nosiča môže byť prijatá zo strany PDF, ktorá plní funkciu bodu rozhodovania politiky (Policy Decision Point - PDP). PEP používa referenčný bod Go tiež pre oboznámenie PDF s potrebnou úpravou nosiča a uvoľneniami nosiča (napr. PDP kontext). Čo sa týka IMS, PDF používa referenčný bod Go pre výslovné stanovenie, či nosič môže alebo nemôže byť použitý; môže tiež požadovať, aby PEP inicioval uvoľnenie nosiča.
- Účtovacia korelácia – cez referenčný bod Go je IMS schopný postúpiť účtovací identifikátor IMS (IMS Charging Identifier – ICID) GPRS sieti (užívateľská rovina). Podobne je GPRS sieť schopná postúpiť účtovací identifikátor GPRS IMS. Pomocou tejto procedúry je neskôr možné zlúčiť účtovacie informácie GPRS a IMS v účtovnom systéme.

2.3.19 Referenčný bod Gq

Keď je nasadená samostatná PDF, referenčný bod Gq sa používa pre prenos informácií o nastavení politiky medzi aplikačnou funkciou a PDF. Výraz "aplikačná funkcia“ sa používa, pretože sa predpokladá, že by PDF by mohla autorizovať prevádzku

inú ako IMS. V prípade IMS funkcia P-CSCF plní úlohu aplikačnej funkcie. Tento referenčný bod bol štandardizovaný v Release 6 a zvolený protokol je priemer.

P-CSCF pošle PDF informácie o politike pre každú SIP správu, ktorá zahrňuje nasadenie SPD. To zaistí, že PDF postúpi správne informácie pre vykonanie autorizácie média pre všetky možné scenáre nastavenia IMS relácie. P-CSCF poskytuje PDF nasledujúce informácie súvisiace s politikou, pre použitie v SBLP [3GPP TS 23.207, 29.207, 29.209]:

- Informácie o mediálnom toku. Zahrňujú napríklad nasledovné:
  - smer prevádzky (dvojsmerný, uplink/downlink);
  - zdrojová/cieľová IP adresa a číslo portu;
  - prenosový protokol;
  - maximálna požadovaná šírka pásma uplink/downlink;
  - stav každého mediálneho komponentu (aktivovaný/deaktivovaný pre smer uplink/downlink);
  - informácie o pravidlách zoskupovania mediálnych komponentov;
  - typ média (audio, video, dáta, aplikácia, kontrola, text, správa, iné).
- Politika zaistenia zdrojov. Obsahuje informácie o tom, či P-CSCF chce byť kontaktovaná pri každej autorizácii nosiča, alebo či môže PDF použiť dostupné informácie pre samostatné rozhodnutie.
- Politika preposielania indikácie. Používa sa pre informovanie PDF, či P-CSCF chce dostávať indikácie o strate nosiča, obnove nosiča alebo uvoľnení nosiča.
- Účtovací identifikátor IMS (IMS Charging Identifier – ICID). Túto informáciu dodáva PDF prístupovej sieti s cieľom umožniť účtovaciu koreláciu.
- Informácie o použitej aplikácii. Tieto informácie môže PDF použiť pre rozlíšenie QoS pre rôzne služby aplikácie.
- Informácie o rozdvojení SIP. Táto informácia je potrebná, aby bola funkcia PDF schopná vypočítať správnu autorizáciu, keďže PDF by mala autorizovať maximálnu šírku pásma požadovanú ktorýmkoľvek z SIP dialógov, ale nie súčet šírok pásiem požadovaných všetkými SIP dialógmi (zaistenie niektorých šírok pásiem by viedlo k zníženiu kapacity a výkonu v prístupových sieťach).

P-CSCF je ďalej schopná požadovať, aby PDF odstránila dovtedy autorizované zdroje. PDF používa referenčný bod Gq pre dodanie autorizačnej známky, účtovacieho identifikátora GPRS, IP adresy GGSN a plnenie iných požiadaviek od P-CSCF, ako je to uvedené vyššie v texte.

2.3.20 Účtovacie referenčné body

Referenčné body súvisiace s účtovaním Rf, Ro, Rx sú popísané v Častiach 3.10.5, 3.10.5 a 3.10.5.

Tabuľka 2.3 Prehľad referenčných bodov.

Názov referenčného bodu	Zapojené entity	Účel	Protokol
Gm	UE, P-CSCF	Tento referenčný bod sa používa pre výmenu správ medzi UE a funkciami CSCF	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	Tento referenčný bod sa používa pre výmenu správ medzi funkciami CSCF	SIP
ISC	S-CSCF, I-CSCF, AS	Tento referenčný bod sa používa pre výmenu správ medzi CSCF a AS	SIP
Cx	I-CSCF, S-CSCF, HSS	Tento referenčný bod sa používa pre komunikáciu medzi I-CSCF/S-CSCF a HSS	Priemer
Dx	I-CSCF, S-CSCF, SLF	Tento referenčný bod používa I-CSCF/S-CSCF pre nájdenie správneho HSS v prostredí s viacerými HSS	Priemer
Sh	SIP AS, OSA SCS, HSS	Tento referenčný bod sa používa pre výmenu informácií medzi SIP AS/OSA SCS a HSS	Priemer
Si	IM-SSF, HSS	Tento referenčný bod sa používa pre výmenu informácií medzi IM-SSF a HSS	MAP
Dh	SIP AS, OSA, SCF, IM-SSF, HSS	Tento referenčný bod používa AS pre nájdenie správneho HSS v prostredí s viacerými HSS	Priemer
Mm	I-CSCF, S-CSCF, externá IP sieť	Tento referenčný bod bude použitý pre výmenu správ medzi IMS a externými IP sieťami	Nešpecifikované
Mg	MGCF → I-CSCF	MGCF konvertuje ISUP signalizáciu na SIP signalizáciu a prepošle SIP signalizáciu funkcii I-CSCF	SIP
Mi	S-CSCF → BGCF	Tento referenčný bod sa používa pre výmenu správ medzi S-CSCF a BGCF	SIP
Mj	BGCF → MGCF	Tento referenčný bod sa používa pre výmenu správ medzi BGCF a MGCF v rovnakej IMS sieti	SIP
Mk	BGCF → BFCF	Tento referenčný bod sa používa pre výmenu správ medzi BGCF v rôznych IMS sieťach	SIP
Mr	S-CSCF, MRFC	Tento referenčný bod sa používa pre výmenu správ medzi S-CSCF a MRFC	SIP

Mp	MRFC, MRFP	Tento referenčný bod sa používa pre výmenu správ medzi MRFC a MRFP	H.248
Mn	MGCF, IMS-MGW	Tento referenčný bod umožňuje kontrolu zdrojov užívateľskej roviny	H.248
Ut	UE, AS (SIP AS, OSA SCS, IM-SSF)	Tento referenčný bod umožňuje UE riadiť informácie súvisiace s jeho službami	http
Go	PDF, GGSN	Tento referenčný bod umožňuje operátorom kontrolovať QoS na užívateľskej rovine a vymieňať účtovacie korelačné informácie medzi sieťou IMS a GPRS	COPS
Gq	P-CSCF, PDF	Tento referenčný bod sa používa pre výmenu informácií súvisiacich s rozhodnutiami o politike medzi P-CSCF a PDF	Priemer
Ro	AS, MRCF, S-CSCF, OCS	Tento referenčný bod používa AS/MRFC/S-CSCF pre online účtovanie pre OCS. Poznámka: môže existovať vzájomne komunikujúca funkcia medzi S-CSCF a OCS	Priemer
Rf	P-CSCF, S-CSCF, I-CSCF, BGCF, MGCF, AS, MRFC, CDF	Tento referenčný bod používajú IMS entity pre offline účtovanie pre CDF.	Priemer
Rx	P-CSCF, AS, Funkcia účtovacích pravidiel	Tento referenčný bod umožňuje výmenu informácií o dynamickej službe súvisiacej s účtovaním medzi funkciou účtovacích pravidiel (Charging Rules Function - CRF) a IMS entitami. Túto informáciu použije CFR pre výber a splnenie účtovacích pravidiel.	Priemer

3 Koncepty IMS

Táto kapitola začína prvotným popisom registrácie a vytvorenia relácie IP multimediálneho subsystému (IP Multimedia Subsystem – IMS). Popisuje zapojené IMS entity. Zámerom nie je ukázať plne rozvinuté riešenie; cieľom je poskytnúť prehľad a pomôcť čitateľovi pochopiť rôzne koncepty IMS vysvetlené v tejto kapitole.

3.1 Registrácia

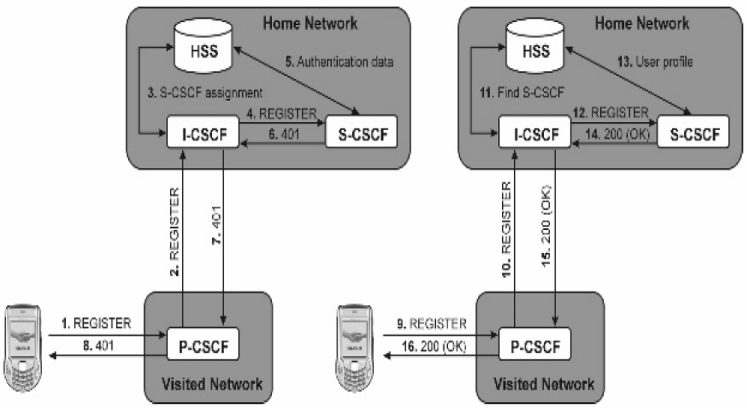
Pred registráciou IMS, ktorá umožní UE použiť IMS služby, musí UE získať nosič IP konektivity a zistiť vstupný bod IMS (napr. P-CSCF): napríklad v prípade prístupu všeobecnej paketovej rádiovej služby (General Packet Radio Service - GPRS) UE vykoná procedúru pripojenia GPRS a aktivuje kontext protokolu paketových údajov (Packet Data Protocol - PDP) pre SIP signalizáciu.

IMS registrácia obsahuje dve fázy: časť úplne vľavo na Obrázku 3.1 zobrazuje prvú fázu – ako sieť vyzve UE. Časť úplne vpravo na Obrázku 3.1 zobrazuje druhú fázu – ako UE odpovie na výzvu a dokončí registráciu.

Najprv UE pošle požiadavku SIP REGISTER odhalenej funkcii P-CSCF. Táto požiadavka bude obsahovať napríklad registrovanú identitu a názov domácej domény (adresa dotazovacej-CSCF, alebo I-CSCF). P-CSCF spracuje požiadavku REGISTER a použije poskytnutý názov domácej domény pre preloženie IP adresy funkcie I-CSCF. I-CSCF kontaktuje domáci účastnícky server (Home Subscriber Server – HSS) pre výber požadovaných schopností pre výber S-CSCF. Po výbere S-CSCF, funkcia I-CSCF prepošle požiadavku REGISTER funkcii S-CSCF. S-CSCF zistí, že užívateľ nie je autorizovaný a získa teda autentifikačné údaje z HSS a vyzve užívateľa Neautorizovanou odpoveďou 401. Potom UE vypočíta odpoveď na výzvu a pošle ďalšiu požiadavku REGISTER funkcii P-CSCF. P-CSCF opäť nájde I-CSCF a I-CSCF zas nájde I-CSCF. Nakoniec S-CSCF skontroluje odpoveď, a ak je správna, stiahne užívateľský profil z HSS a príjme registráciu odpoveďou 200 OK. Po úspešnej autorizácii UE, UE je schopné iniciovať a prijímať relácie. Počas registračnej procedúry EU aj P-CSCF zistia, ktorá funkcia S-CSCF bude slúžiť UE. Tabuľka 3.1 uvádza prehľad o ukladaní informácií pred, počas a po registračnom procese.

UE zodpovedá za udržiavanie svojej registrácie v aktívnom stave jej pravidelným obnovovaním. Ak UE neobnoví registráciu, S-CSCF potichu zruší registráciu, keď

uplynie stanovená doba časovača registrácie. Ak UE chce zrušiť registráciu v IMS, nastaví časovač registrácie na 0 a odošle požiadavku REGISTER.



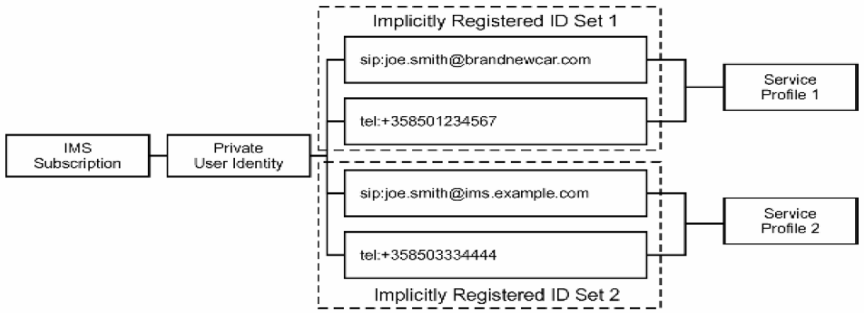
Obrázok 3.1 Registrácia IMS na vysokej úrovni.

Tabuľka 3.1 Uložené informácie pred, počas a po registračnom procese.

Uzol	Pred registráciou	Počas registrácie	Po registrácii
UE	Adresa P-CSCF, názov domácej domény, súkromné údaje, verejná užívateľská identita, súkromná užívateľská identita	Adresa P-CSCF, názov domácej domény, súkromné údaje, verejná užívateľská identita, súkromná užívateľská identita, bezpečnostná asociácia	Adresa P-CSCF, názov domácej domény, súkromné údaje, verejná užívateľská identita (a implicitne registrované verejné užívateľské identity), súkromná užívateľská identita, bezpečnostná asociácia, informácia o smerovaní služby (S-CSCF)
P-CSCF	Žiadna informácia o stave	Počiatočný sieťový vstupný bod, adresa UE IP, verejné a súkromné užívateľské identity, bezpečnostné asociácie	Koncový sieťový vstupný bod (S-CSCF), adresa UE, registrovaná verejná užívateľská identita (a implicitne registrované verejné užívateľské identity), súkromná užívateľská identita, bezpečnostná asociácia, adresa CDF
I-CSCF	Adresa HSS alebo SLF	Vstup HSS alebo SLF, adresa P-CSCF, adresa S-CSCF	Adresa HSS alebo SLF
S-CSCF	Adresa HSS alebo SLF	Adresa/názov HSS, užívateľský profil (obmedzený - podľa sieťového scenára), adresa/názov proxy, verejná/súkromná užívateľská identita, adresa UE IP	Adresa/názov HSS, užívateľský profil (obmedzený - podľa sieťového scenára), adresa/názov proxy, verejná/súkromná užívateľská identita, adresa UE IP
HSS	Užívateľský profil, výberové parametre S-CSCF	Užívateľský profil, výberové parametre S-CSCF, informácie o navštívenej sieti, ak užívateľ využíva roaming	Užívateľský profil, výberové parametre S-CSCF, informácie o tom, ktoré užívateľské identity sú registrované, názov S-CSCF pridelenej užívateľovi

3.2 Mechanizmus pre súbežnú registráciu viacerých užívateľských identít

SIP umožňuje registráciu len jednej verejnej užívateľskej identity naraz; ak má teda užívateľ viac ako jednu verejnú užívateľskú identitu, musí registrovať každú verejnú užívateľskú identitu samostatne. To môže byť frustrujúce a náročné na čas z pohľadu koncového užívateľa. Samozrejme, registrácia štyroch verejných užívateľských identít by zabrala štyrikrát viac rádiových zdrojov v prípade univerzálneho mobilného telekomunikačného systému (Universal Mobile Telecommunications System - UMTS) ako registrácia jednej verejnej užívateľskej identity. Z tohto dôvodu Projekt partnerstva tretej generácie (Third Generation Partnership Project - 3GPP) vyvinul mechanizmus pre registráciu viac ako jednej verejnej užívateľskej identity naraz. Tento koncept sa nazýva "implicitná registrácia".



Obrázok 3.2 Príklad sád implicitnej registrácie.

Implicitly Registered ID Set 1 - Implicitne registrovaná ID Sada 1
IMS Subscription – Prihlásenie IMS
Private User Identity - Súkromná užívateľská identita
Service Profile 1 – Profil služby 1
Service Profile 2 - Profil služby 2
Implicitly Registered ID Set 1 – Implicitne registrovaná ID Sada 2

Implicitná registračná sada je skupina verejných užívateľských identít, ktoré sú registrované prostredníctvom jedinej registračnej požiadavky. Keď je registrovaná jedna z verejných užívateľských identít v sade, všetky verejné užívateľské identity spojené so sadou implicitnej registrácie sú registrované naraz. Podobne, keď je pre jednu z verejných užívateľských identít v rámci sady zrušená registrácia, pre všetky verejné užívateľské

identity, ktoré boli implicitne registrované je registrácia zrušená naraz. Verejné užívateľské identity, ktoré patria do implicitnej registračnej sady, môžu smerovať na rôzne profily služieb. Niektoré z týchto verejných užívateľských identít môžu smerovať na rovnaký profil služby [3GPP TS 23.228].

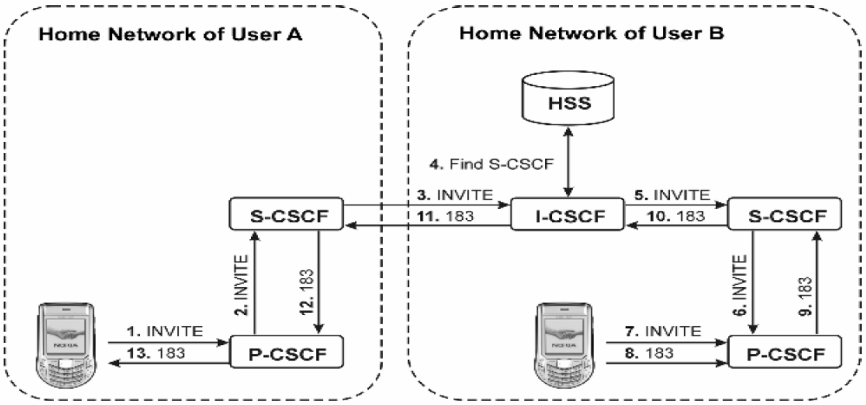
Pre získanie implicitne registrovaných verejných identít, musí UE poslať funkcii S-CSCF požiadavku SUBSCRIBE na balík registračnej udalosti. Keď S-CSCF príjme požiadavku SUBSCRIBE, vráti implicitne registrovanú verejnú užívateľskú identitu s požiadavkou NOTIFY. Napríklad, užívateľ má štyri verejné užívateľské identity, ktoré sú zoskupené do dvoch implicitných registračných sád (Obrázok 3.2). Prvá sada obsahuje *joe.smith@brandnewcar.com* a *tel.+358501234567*. Druhá sada obsahuje *joe.smith@brandnewcar.com* a *tel.+358503334444*. Keď Joe pošle požiadavku REGISTER obsahujúcu ako registrovanú identitu, pridelená funkcia S-CSCF vykoná normálnu registračnú procedúru a po úspešnej autorizácii S-CSCF stiahne profily služieb, ktoré sú spojené s verejnými užívateľskými identitami, ktoré patria do implicitnej registračnej sady (profil služby 1). Pre získanie implicitne registrovaných užívateľských identít Joeove UE pošle funkcii S-CSCF požiadavku SUBCRIBE. Keď S-CSCF príjme požiadavku SUBSCRIBE automaticky vráti implicitne registrovanú užívateľskú identitu, *tel.+358501234567*, v rámci *NOTIFY*.

3.3 Iniciácia relácie

Keď chce Užívateľ A vytvoriť reláciu s Užívateľom B, UE A generuje požiadavku SIP INVITE a pošle ju cez referenčný bod GM funkcii P-CSCF. P-CSCF spracuje požiadavku: napríklad dekomprimuje požiadavku a overí identitu užívateľa, od ktorého požiadavka pochádza pred preposlaním požiadavky cez referenčný bod Mw funkcii S-CSCF. S-CSCF spracuje požiadavku, vykoná kontrolu služby, ktorá môže zahŕňať interakciu s aplikačnými servermi (Application Servers (ASs)) a nakoniec určí vstupný bod domáceho operátora Užívateľa B na základe identity Užívateľa B v požiadavke SIP INVITE. I-CSCF príjme požiadavku cez referenčný bod Mw a kontaktuje HSS cez referenčný bod Cx, aby zistil S-CSCF, ktorý slúži Užívateľovi B. Požiadavka je postúpená funkcii S-CSCF cez referenčný bod Mw. S-CSCF zodpovedá za spracovanie ukončovacej relácie, ktorá môže zahŕňať interakcie s ASs a nakoniec doručí požiadavku funkcii P-CSCF cez referenčný bod Mw. Po ďalšom spracovaní (napr. kompresia a kontrola ochrany súkromia), P-CSCF použije referenčný bod Gm pre

doručenie požiadavky SIP INVITE UE B. UE B vytvorí odpoveď – 183 Postup relácie – ktorá prechádza naspäť do UE A po ceste, ktorá bola vytvorená smerom z UE A (napr. UE B → P-CSCF → S-CSCF → I-CSCF → S-CSCF → P-CSCF → UE A) (Obrázok 3.3). Po niekoľkých ďalších spiatočných cestách, obidve sady UE dokončia vytvorenie spojenia a sú schopné spustiť aktuálnu aplikáciu (napr. šachová partia). Počas vytvárania relácie môže operátor kontrolovať použite nosičov určených pre mediálnu prevádzku.

Len pre predstavu toho , čo nasleduje v knižke, v Tabuľke 3.2 je uvedený obsah vysokej úrovne požiadavky SIP INVITE. Každý stĺpec uvádza informačné prvky, ktoré sú vložené, odstránené alebo zmenené.



Obrázok 3.3 Tok vytvorenia relácie IMS vysokej úrovne.

Home Network of User A – Domáca sieť Užívateľa A

Home Network of User B – Domáca sieť Užívateľa B

Tabuľka 3.2 Obsah vyššej úrovne požiadavky SIP INVITE počas vytvorenia relácie.

UE (A)	P-CSCF (A)	S-CSCF (A)
Identita Užívateľa A Identita Užívateľa B Kontaktná adresa Prístupové informácie Smerovacie informácie (Hlavičky trasy a cesty) Podpora dôveryhodných odpovedí Podpora predpokladov Bezpečnostné informácie Indikácia ochrany súkromia Indikácia kompresie SPD náklad odrážajúci schopnosti terminálu užívateľa a užívateľské preferencie pre reláciu, subtyp MIME „telefónna udalosť“, informácia o šírke pásma	*Vložené informácie* Jedna smerovacia informácia (Hlavička záznamu cesty) Účtovacie informácie IMS Overená identita strany A *Odstránené informácie* Bezpečnostné informácie Navrhnutá identita strany A *Zmenené informácie* Smerovacie informácie (Cesta, Trasa)	*Vložené informácie* Interoperačný identifikátor *Odstránené informácie* Jedna smerovacia informácia (Hlavička cesty) Prístupové informácie *Zmenené informácie* Smerovacie informácie (Záznam cesty a Trasa) Overená identita strany A, tiež zahŕňa typ Tel-URL identity odteraz platnej
I-CSCF (B)	S-CSCF (B)	P-CSCF (B)
Vložené informácie Jedna smerovacia informácia (Hlavička cesty) *Odstránené informácie* Žiadne *Zmenené informácie* Smerovacia informácie (Trasa)	*Vložené informácie* Žiadne *Odstránené informácie* Interoperačný identifikátor *Zmenené informácie* Smerovacie informácie (R-URI, Cesta, Trasa, Záznam cesty)	*Vložené informácie* Autorizačná známka *Odstránené informácie* IMS účtovacie informácie Jedna smerovacia informácia (Hlavička cesty) Identita strany je odstránená, ak je požadovaná ochrana súkromia *Zmenené informácie* Smerovacie informácie (Trasa, Záznam cesty)

3.4 Identifikácia

3.4.1 Identifikácia užívateľov

Súkromná užívateľská identita

Súkromná užívateľská identita je jedinečná globálna identita definovaná operátorom domácej siete, ktorá môže byť použitá v rámci domácej siete pre jedinečnú identifikáciu užívateľa z hľadiska siete [3GPP TS 23.228]. Neidentifikuje samotného užívateľa, ale identifikuje prihlásenie užívateľa. Používa sa teda hlavne pre autentifikačné účely. Súkromné užívateľské identity je možné použiť aj pre fakturačné a administratívne

účely. IMS architektúra stanovuje nasledujúce požiadavky pre súkromnú užívateľskú identitu [3GPP TS 23.228, TS 23.003]:

- Súkromná užívateľská identita bude mať podobu identifikátora sieťového prístupu (Network Access Identifier - NAI) definovaného v [RFC2486].
- Súkromná užívateľská identita bude obsiahnutá vo všetkých registračných požiadavkách postúpených z UE domácej sieti.
- Súkromná užívateľská identita bude autentifikovaná len počas registrácie užívateľa (vrátane opätovnej registrácie a zrušenia registrácie).
- S-CSCF bude musieť získať a uložiť súkromnú užívateľskú identitu pri registrácii alebo neregistrovanom ukončení.
- Súkromná užívateľská identita nebude použitá pre smerovanie SIP správ.
- Súkromná užívateľská identita bude trvale pridelená užívateľovi a bezpečne uložená v aplikácii modulu identity IMS (IMS Identity Module - ISIM). Súkromná užívateľská identita bude platná po dobu trvania prihlásenia užívateľa v rámci domácej siete.
- UE nebude mať možnosť zmeniť súkromnú užívateľskú identitu.
- HSS bude musieť uložiť súkromnú užívateľskú identitu.
- Súkromná užívateľská identita bude súčasťou účtovacích záznamov založených na politikách operátora.

Príklad NAI	form_user@realm

Verejná užívateľská identita

Užívateľské identity v sieťach IMS sa nazývajú verejné užívateľské identity. Sú to identity používané pre vyžiadanie komunikácie s ostatnými užívateľmi. Verejné identity môžu byť zverejnené (napr. v telefónnych zoznamoch, web stránkach, firemných vizitkách).

Ako už bolo uvedené v predchádzajúcom texte, IMS užívatelia budú schopní iniciovať relácie a prijímať relácie z mnohých rôznych sietí, ako siete GSM a internet. Aby bola verejná užívateľská identita dostupná zo strany CS, musí byť v súlade s číslovaním telecom (napr. *+358501234567*). Podobným spôsobom pri vyžadovaní

komunikácie s internetovými klientmi, musí byť verejná užívateľská identita v súlade s internetovým pomenovaním (napr. *joe.doe@example.com*).

Architektúra IMS stanovuje nasledujúce požiadavky pre verejné užívateľské identity [3GPP TS 23.228, TS 23.003]:

- Verejná užívateľská identita/identity budú mať buď formu formátu jednotného identifikátora zdroja SIP (Uniform Resource Identifier – URI) alebo telefónneho jednotného lokalizátora zdroja (Uniform Resource Locator - tel URL).
- Aspoň jedna verejná užívateľská identita bude bezpečne uložená v ISM aplikácii.
- UE nebude schopné zmeniť verejnú užívateľskú identitu.
- Verejná užívateľská identita bude registrovaná predtým, ako môže byť identita použitá pre vytvorenie IMS relácií a procedúr nesúvisiacich s IMS reláciou (napr. MESSAGE, SUBSCRIBE, NOTIFY).
- Verejná užívateľská identita bude registrovaná pred ukončením IMS relácií a ukončenie procedúr nesúvisiacich s IMS reláciou bude doručené UE užívateľa, ktorému patrí verejná užívateľská identita. To nebráni výkonu služieb na sieti neregistrovanými užívateľmi.
- Bude možné registrovať viacnásobné verejné identity prostredníctvom jedinej UE požiadavky.
- Sieť neautentifikuje verejné užívateľské identity počas registrácie.

Schéma tel URL sa používa pre vyjadrenie tradičných E.164 čísel v syntaxe URL. Tel URL je popísaný v [RFC2806] a SIP URI je popísaný v [RFC3261] a [RFC2396]. Príklady verejných užívateľských identít sú uvedené nižšie.

Príklad SIP URI	*sip:joe.doe@ims.example.com*

Príklad tel URL	*tel:+358 50 1234567*

Odvodená verejná užívateľská identita a súkromná užívateľská identita

Boli vysvetlené koncepty súkromnej užívateľskej identity a verejnej užívateľskej identity. Bolo uvedené, že tieto identity sú uložené v aplikácii ISIM. Keď bude nasadený IMS, bude na trhu veľa UE, ktoré nepodporujú aplikáciu ISIM; bol teda vyvinutý mechanizmus pre prístup k IMS bez ISIM.

V tomto modeli sú súkromná užívateľská identita, verejná užívateľská identita a názov domácej domény odvodené z medzinárodnej identity mobilného účastníka (International Mobile Subscriber Identity (IMSI)). Tento mechanizmus je vhodný pre UE, ktoré má aplikáciu modulu univerzálnej identity účastníka (Universal Subscriber Identity Module - USIM).

Súkromná užívateľská identita

Súkromná užívateľská identita odvodená z IMSI je vytvorená v súlade s nasledujúcimi krokmi[3GPP TS 23.003]:

1. Zložka užívateľa súkromnej užívateľskej identity je nahradená celým reťazcom číslic z IMSI.
2. Zložka domény súkromnej užívateľskej identity je zložená z hodnôt MCC a MNC z IMSI a má preddefinovaný názov domény, *IMSI.3gppnetwork.org.*. Tieto tri časti sú zlúčené a oddelené bodkami v nasledujúcom poradí: kód mobilnej siete (Mobile Network Code – MNC, číslica alebo kombinácia číslic jedinečne identifikujúca verejnú pozemnú mobilnú sieť). Mobilný kód krajiny (MCC, kód jedinečne identifikujúci krajinu trvalého bydliska mobilného účastníka) a preddefinovaný názov domény.

Napríklad:

Použitá IMSI: 234150999999999; kde:
MMC: 234;
MNC: 15;
MSIN: 0999999999; a
Súkromná užívateľská identita je:
234150999999999990234.15.IMSI.3gppnetwork.org

Dočasná verejná užívateľská identita

Ak neexistuje ISIM aplikácie pre hosťovanie verejnej užívateľskej identity, bude odvodená dočasná verejná užívateľská identita na základe IMS. Dočasná verejná užívateľská identita bude mať formu SIP URI: *„sip:user@domain*. Zložka užívateľa a domény sú odvodené rovnakou metódou, ako pre súkromnú užívateľskú identitu [3GPP

TS 23.003]. Podľa nášho predchádzajúceho príkladu by príslušná dočasná verejná užívateľská identita bola:

sip:234150999999990234.15.IMSI.3gppnetwork.org

Architektúra IMS stanovuje nasledujúce požiadavky pre dočasnú verejnú užívateľskú identitu [3GPP TS 23.228]:

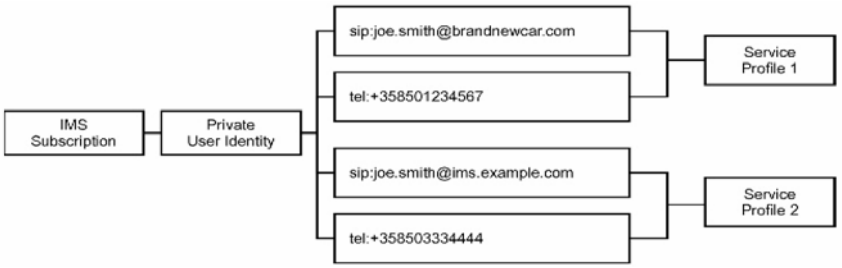
- Výrazne sa odporúča, aby dočasná verejná užívateľská identita bola nastavená ako "neprístupná“ pre neregistračné procedúry IMS, aby mohla byť použitá pre komunikáciu IMS. Nasledujúce dodatočné požiadavky sú platné, ak je dočasná verejná užívateľská identita "neprístupná":
  - dočasná verejná užívateľská identita nebude zobrazená užívateľovi a nebude použitá pre verejné účely (napr. zobrazená na navštívenke);
  - dočasná verejná užívateľská identita bude použitá len počas registrácie pre získanie implicitne registrovaných verejných užívateľských identít.
- Implicitne registrované verejné užívateľské identity budú použité pre riadenie relácie, v iných SIP správach a pre ďalších registračných procesoch.
- Po počiatočnej registrácii bude implicitne registrovanú(é) verejnú(é) užívateľskú(é) identitu(y) používať len UE.
- Dočasná verejná užívateľská identita bude dostupná len pre CSCF a HSS uzly.

Vzťah medzi súkromnou a verejnou užívateľskou identitou

Nasledujúci základný príklad ukazuje, ako sú rôzne identity vzájomne prepojené. Joe pracuje pre spoločnosť predávajúcu autá a používa jeden terminál pre svoj osobný aj pracovný život. Pre riadenie záležitostí súvisiacich s prácou má dve verejné užívateľské identity: *sip:joe.smith@brandnewcar.com* a *tel:+358501234567*. Keď nepracuje, používa dve dodatočné verejné užívateľské identity pre riadenie svojho osobného života: *sip:joe.smith@ims.example.com* a *tel:+358503334444*. Tým, že má dve sady verejných užívateľských identít, mohol by mať úplne iné spracovanie pre prichádzajúce relácie: napríklad, môže presmerovať všetky prichádzajúce relácie súvisiace s prácou do systému pre posielanie správ po 17.00 a počas víkendov a sviatkov.

Joeove užívateľské údaje a údaje súvisiace so službou sú udržiavané v dvoch rôznych profiloch služby. Profil služby obsahuje informácie o identitách jeho pracovného života a sťahuje sa do S-CSCF z HSS v prípade potreby: to znamená, keď Joe registruje pracovnú verejnú užívateľskú identitu, alebo keď S-CSCF potrebuje vykonať neregistrované služby pre pracovnú verejnú užívateľskú identitu. Podobne, ďalší profil služby obsahuje informácie o identitách jeho osobného života a sťahuje sa do S-CSCF z HSS v prípade potreby.

Obrázok 3.4 znázorňuje, ako sú Joeove súkromná užívateľská identita, verejné užívateľské identity a profily služieb prepojené.



Obrázok 3.4 Vzťah medzi užívateľskými identitami.

IMS Subscription – Prihlásenie IMS
Private User Identity – Súkromná užívateľská identita
Service Profile 1 – Profil služby 1
Service Profile 2 – Profil služby 2

3.4.2 Identifikácia služieb (verejné služobné identity)

So zavedením štandardizovanej prístupnosti, posielania správ, vedenia konferencií a schopností skupinových služieb začalo byť zrejmé, že musia existovať identity pre identifikáciu služieb a skupín, ktoré hosťujú ASs. Identity pre tento účel sú vytvárané aj priebežne: to znamená, že môžu byť vytvorené užívateľom podľa potreby v AS a nie sú pred použitím registrované. Bežné súkromné užívateľské identity jednoducho neboli dosť dobré: Release 6 teda zaviedlo nový typ identity, verejnú služobnú identitu. Verejné služobné identity majú formu SIP URI alebo sú vo formáte tel URL: napríklad v službách posielania správ existuje verejná služobná identita pre službu zoznamu pre posielanie

správ (napr. *sip:messaginglist_joe@ims.example.com*), ktorej užívatelia posielajú správy a potom sú správy distribuované ostatných členom na zozname pre posielanie správ serverom zoznamu pre posielanie správ. To isté platí pre konferenčné služby (napr. audio/video a relácie posielania správ), kde je vytvorené URI pre konferenčnú službu.

3.4.3 Identifikácia sieťových entít

Okrem užívateľov musia byť identifikovateľné aj sieťové uzly, ktoré riadia smerovanie SIP pomocou platného SIP URI. Tieto SIP URI sa použijú pri identifikácii týchto uzlov v poliach hlavičiek SIP správ. To však nevyžaduje, aby tieto URI boli globálne zverejnené v systéme doménových názvov (Domain Name System – DNS) [3GPP TS 23.228]. Operátor by mohol nazvať svoju S-CSCF nasledovne:

Príklad pomenovania sieťovej entity	*sip:finland.scscf1@ims.example.com*

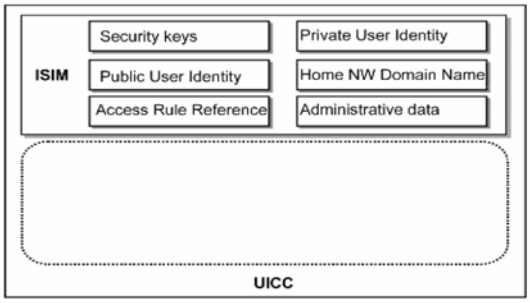
3.5 Moduly identity

3.5.1 Modul identity IP multimediálnych služieb (IP Multimedia Services Identity Module – ISIM)

Modul identity IP multimediálnych služieb (IP Multimedia Services Identity Module – ISIM) je aplikácia sídliaca v univerzálnej karte na báze integrovaných obvodov (Universal Integrated Circuit Card - UICC), čo je fyzicky bezpečné zariadenie, ktoré môže byť vložené do UE a vybrané z UE. V UICC môže byť jedna alebo viac aplikácií. Samotný ISIM ukladá IMS-špecifické účastnícke údaje poskytnuté operátorom IMS. Uložené údaje môžu byť rozdelené do šiestich skupín, ako je to znázornené na Obrázku 3.5. Väčšina údajov je potrebná, keď užívateľ vykonáva IMS registráciu [3GPP TS 31.103]:

- Bezpečnostné kľúče sa skladajú z kľúčov integrity, šifrovacích kľúčov a kľúčových identifikátorov sady. Kľúče integrity sa používajú na preukázanie ochrany integrity SIP signalizácie. Šifrovacie kľúče sa používajú na poskytnutie dôvernej ochrany SIP signalizácie. Dôverná ochrana sa nepoužíva v Release 5; v Release 6 by však malo byť možné použiť dôvernú ochranu. V dobe písania existovala potreba kľúčových identifikátorov sady.

- Súkromná užívateľská identita jednoducho obsahuje súkromnú užívateľskú identitu užívateľa. Používa sa v registračnej požiadavke na identifikáciu prihlásenia užívateľa.
- Verejná užívateľská identita obsahuje jednu alebo viac verejných užívateľských identít užívateľa. Používa sa v registračnej požiadavke pre identifikáciu registrovanej identity a používa sa pre vyžiadanie komunikácie s ostatnými užívateľmi.
- Názov domény domácej siete tvorí názov vstupného bodu domácej siete. Používa sa v registračnej požiadavke pre smerovanie požiadavky do domácej siete užívateľa.
- Administratívne údaje zahŕňajú rôzne údaje, ktoré by mohli byť použité napríklad účastníkmi IMS operácií alebo výrobcami pre vykonanie proprietárnych auto-testov.
- Referencia prístupového pravidla sa používa na uloženie informácií, pre ktoré musí byť overené osobné identifikačné číslo pre získanie prístupu k aplikácii.



Obrázok 3.5 Moduly identity IP multimediálnych služieb

Security keys – Bezpečnostné kľúče

Public User Identity – Verejná užívateľská identita

Acces Rule Referencia - Referencia prístupového pravidla

Private User Identity – Súkromná užívateľská identita

Home NW Domain Name – Názov domény domácej NW

Administrative data – Administratívne údaje

3.5.2 Modul univerzálnej identity účastníka (Universal Subscriber Identity Module - USIM)

Modul univerzálnej identity účastníka (Universal Subscriber Identity Module - USIM) je požadovaný pre prístup k PS doméne (GPRS) a jednoznačne identifikuje konkrétneho účastníka. Rovnako, ako pre ISIM, USIM aplikácia sídli v UICC ako úložisko pre prihlásenie a informácie súvisiacich s účastníkom. Okrem toho, môže obsahovať aplikácie, ktoré využívajú vlastnosti definované v USIM Aplikačnom toolkite.

USIM obsahuje nasledovné typy údajov: bezpečnostné parametre pre prístup k PS doméne, IMSI, zoznam povolených názvov prístupových bodov, informácie súvisiace so službou multimediálnych správ (Multimedia Message Service – MMS) [3GPP TS 31.102, TS 22.101, TS 21.111].

3.6 Zdieľanie jednej užívateľskej identity medzi viacerými zariadeniami

Tradične má v CS každý užívateľ vlastné medzinárodné ISDN číslo mobilnej stanice (Mobile Station International ISDN – MSISDN), ktoré sa používa pre zastihnutie užívateľa. Nie je možné, aby jeden užívateľ naraz používal viaceré terminály s rovnakým MSISDN. Dve mobilné stanice s identickými číslami MSISDN by spôsobili významné konflikty na sieti. V súčasnosti môžu mať užívatelia viac ako jedno UE s úplne odlišnými schopnosťami: malá/veľká obrazovka, s fotoaparátom/bez fotoaparátu, plná klávesnica atď. Rôzne UE môžu slúžiť na rôzne účely (napr. jeden na hranie, druhý na bežné hlasové a video relácie). S hľadiska užívateľa, by mal byť užívateľ zastihnuteľný s rovnakou identitou bez ohľadu na počet UE, ktoré súbežne používa. IMS túto schopnosť umožňuje.

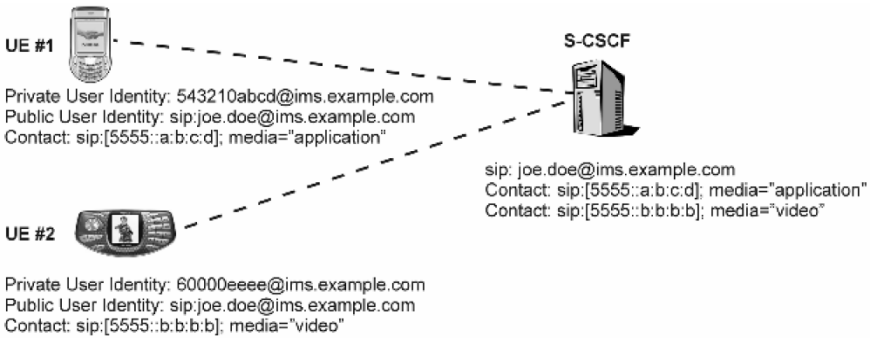
Release 6 IMS umožňuje užívateľom zaregistrovať rovnakú verejnú užívateľskú identitu z viacerých UE. Okrem toho, užívateľ je schopný určiť svoje preferencie ohľadom jedného UE v registračnej fáze. Rôzne registrácie môžu byť rozlíšené prostredníctvom súkromnej užívateľskej identity a IP adresy. Obrázok 3.6 znázorňuje príklad, kde má užívateľ dve UE: jedno pre video relácie a druhé pre aplikácie na internetový rozhovor a hry. Keď niekto zavolá užívateľovi, napr. Joeovi - jeho S-CSCF rozhodne, ktoré UE kontaktuje ako prvé. Toto rozhodnutie je vykonané na základe preferencií určených počas registračnej fázy: napríklad ak prichádzajúca relácia obsahuje video zložku, potom S-CSCF môže vybrať UE #2, ktoré je Joeovou primárnou

preferenciou pre video relácie. Okrem smerovania založeného na preferenciách, môže S-CSCF vykonať rozdvojenie. Existujú dva typy rozdvojenia:

- sekvenčné rozdvojenie;
- paralelné rozdvojenie.

Sekvenčné rozdvojenie znamená, že rôzne UE sú kontaktované po jednom: napríklad S-CSCF najprv pošle požiadavku UE #2 a ak Joe neodpovie do určitého časového limitu, S-CSCF sa pokúsi zastihnúť Joea cez UE #1.

Paralelné rozdvojenie znamená, že rôzne UE sú kontaktované naraz: napríklad keď zvonia dve UE, Joe sa môže rozhodnúť, ktoré UE použije pre prichádzajúcu reláciu; nakoniec však môže byť relácia pripojená len k jednému UE.



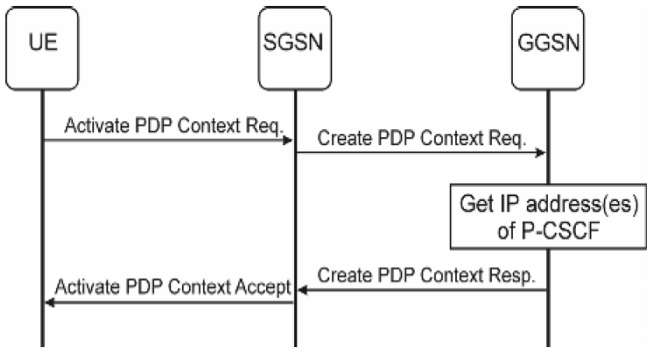
Obrázok 3.6 Zdieľanie jednej užívateľskej identity medzi viacerými zariadeniami.
Private User Identity – Súkromná užívateľská identita
Public User Identity – Verejná užívateľská identita
Contact - Kontakt

3.7 Odhalenie vstupného bodu IMS

Pre komunikáciu s IMS musí jedno UE poznať aspoň jednu IP adresu P-CSCF. Mechanizmus, pomocou ktorého UE získava tieto adresy, sa nazýva "odhalenie P-CSCF". V 3GPP boli štandardizované dva dynamické mechanizmy pre zistenie P-CSCF: DNS procedúra protokolu pre dynamickú konfiguráciu hostiteľov (Dynamic Host Configuration Protocol - DHCP) a GPRS procedúra. Okrem toho, je v UE možné konfigurovať buď názov P-CSCF alebo IP adresu P-CSCF.

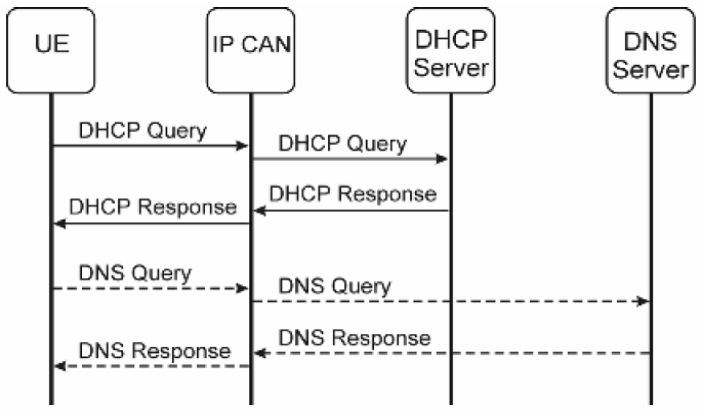
V GPRS procedúre (Obrázok 3.7) UE zahŕňa príznak požiadavky na adresu P-CSCF v požiadavke na aktiváciu PDP kontextu (alebo druhotná požiadavka na aktiváciu PDP kontextu) a v odpovedi získa IP adresu(y) P-CSCF. Táto informácia je prenesená v informačnom prvku možností konfigurácie protokolu [3GPP TS 24.008]. Mechanizmus stykového podporného uzla GPRS (Gateway GPRS Support Node - GGSN) použitý pre získanie IP adresy(adries) funkcie(í) P-CSCF nie je štandardizovaný. Tento mechanizmus však nefunguje v GGSNs v pre-Release 5.

V procedúre DHCP DNS (Obrázok 3.8) UE pošle DHCP dotaz prístupovej sieti s IP konektivitou (napr. GPRS), ktorá prenesie správu serveru DHCP. V súlade [RFC3319] a [RFC3315], UE môže požadovať buď zoznam názvov domén SIP servera funkcie(í) P-CSCF alebo zoznam adries SIP servera IPv6 funkcie(í) P-CSCF. Keď sú vrátené názvy domén, UE musí vykonať DNS dotaz (NAPTR/SRV) pre nájdenie IP adresy funkcie P-CSCF. Mechanizmus DHCP DNS je spôsob odhalenia P-CSCF nezávislý od prístupu.



Obrázok 3.7 Mechanizmus pre odhalenie P-CSCF špecifický pre GPRS.

Activate PDP Context Req. - Požiadavka na aktivovanie PDP kontextu
Create PDP Context Req. – Požiadavka na vytvorenie PDP kontextu
Get IP address(es) of P-CSCF – Získanie IP adresy(adries) P-CSCF
Activate PDP Context Accept – Prijatie požiadavky na aktivovanie PDP kontextu
Create PDP Context Resp. – Odpoveď na vytvorene PDP kontextu



Obrázok 3.8 Všeobecný mechanizmus pre odhalenie P-CSCF.

DHCP Query – DHCP dotaz
DHCP Response – DHCD odpoveď
DNS Query – DNS dotaz
DNS Response – DNS odpoveď

3.8 Priradenie S-CSCF

Bolo vysvetlené, ako UE odhalí vstupný bod IMS – t.j. P-CSCF. Ďalšou entitou na ceste signalizácie relácie je S-CSCF. Existujú tri prípady, kedy je S-CSCF priradená:

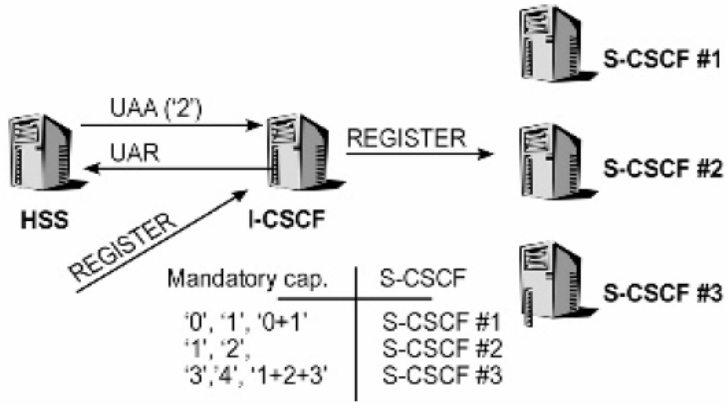
- keď sa užívateľ registruje na sieti;
- keď neregistrovaný užívateľ príjme SIP požiadavku;
- keď predtým priradená S-CSCF neodpovedá.

3.8.1 Priradenie S-CSCF počas registrácie

Keď sa užívateľ registruje na sieti, UE pošle požiadavku REGISTER odhalenej P-CSCF, ktorá nájde domácu sieťovú entitu užívateľa—t.j I-CSCF. Potom si I-CSCF vymení správy s HSS (UAR a UAA). Výsledkom je, že I-CSCF získa schopnosti S-CSCF, pokiaľ nebola predtým priradená S-CSCF. Na základe získaných schopností I-CSCF vyberie vhodnú S-CSCF. Informácie o schopnostiach sú prenesené medzi HSS a I-CSCF v rámci páru hodnota atribútu (Attribute Value Pair - AVP) schopností servera. AVP schopností servera obsahuje [3GPP TS 29.229]:

- AVP povinnej schopnosti - typ tohto AVP je neoznačený a obsahuje povinné schopnosti S-CSCF. Pre každú povinnú schopnosť, dostupnú v individuálnej sieti operátora, bude priradená unikátna hodnota.
- AVP voliteľnej schopnosti - typ tohto AVP je neoznačený a obsahuje povinné schopnosti S-CSCF. Pre každú povinnú schopnosť, dostupnú v individuálnej sieti operátora, bude priradená unikátna hodnota.
- AVP názvu servera - tento AVP obsahuje SIP URI používaný pre identifikáciu SIP servera.

Na základe AVP povinnej a voliteľnej schopnosti môže operátor rozdeliť užívateľov medzi funkcie S-CSCF v závislosti od rôznych schopností (požadované schopnosti pre užívateľské služby, preferencie operátora pre jednotlivých užívateľov, atď.), ktoré konkrétna S-CSCF má. Operátor je zodpovedný za definovanie (na základe funkčnosti ponúkanej každou S-CSCF nainštalovanou na sieti) presného významu povinných a voliteľných schopností. I-CSCF najprv vyberie S-CSCF, ktorá má všetky povinné a voliteľné schopnosti pre užívateľa. Ak to nie je možné, I-CSCF aplikuje "metódu najlepšieho výberu". Žiadna z metód výberu nie je štandardizovaná (napr. riešenia sú závislé od implementácie). Na obrázku 3.9 je uvedený príklad.



Obrázok 3.9 Príklad priradenia S-CSCF.

Pomocou AVP názvu servera má operátor možnosť naviesť užívateľov na určité S-CSCF; napríklad tým, že má jednu S-CSCF určenú pre tú istú spoločnosť/skupinu pre zavedenie služby VPN alebo podstatným zjednodušením priradenie S-CSCF.

3.8.2 Priradenia S-CSCF pre neregistrovaného účastníka

Časť 3.3 a Obrázok 3.3 vysvetlili na vysokej úrovni, akým spôsobom je relácia smerovaná z UE A do UE B. Z obrázku je zrejmé, že I-CSCF je kontaktným bodom v rámci siete operátora. Boli vysvetlené procedúry získania umiestnenia (napr. prichádzajúca SIP požiadavka spustí príkazy LIR/LIA s cieľom zistiť, ktorá S-CSCF slúži Užívateľovi B). Ak HSS nevie o žiadnej predtým priradenej S-CSCF, vráti informácie o schopnostiach S-CSCF a procedúra priradenia S-CSCF sa uskutoční v I-CSCF.

3.8.3 Priradenie S-CSCF v chybových prípadoch

Štandardy 3GPP umožňujú opätovné priradenie S-CSCF počas registrácie, keď priradená S-CSCF neodpovedá: to je vtedy, keď I-CSCF zistí, že nemôže dosiahnuť priradenú S-CSCF, pošle príkaz UAR serveru HSS a explicitne nastaví typ autorizačného informačného prvku na hodnotu registrácia_a_schopnosti. Po získaní schopností S-CSCF, I-CSCF vykoná priradenie S-CSCF.

3.8.4 Zrušenie priradenia S-CSCF

Priradenie S-CSCF je zrušené, keď užívateľ zruší registráciu na sieti alebo sa sieť rozhodne zrušiť registráciu užívateľovi (napr. pretože stanovená doba registrácie uplynula alebo prihlásenie vypršalo). S-CSCF zodpovedá za vymazanie názvu uloženej S-CSCF zo servera HSS.

3.8.5 Udržiavanie priradenia S-CSCF

Keď užívateľ zruší registráciu na sieti alebo časovač registrácie uplynie v S-CSCF, operátor sa môže rozhodnúť, či chce zachovať pre neregistrovaného užívateľa priradenú rovnakú S-CSCF. S-CSCF zodpovedá za informovanie HSS, že registrácia užívateľa bola zrušená; S-CSCF môže určiť, či chce zachovať užívateľský profil. To optimalizuje zaťaženie referenčného bodu Cx, pretože nie je potrebné prenášať užívateľský profil, keď sa užívateľ znovu zaregistruje alebo príjme relácie, pričom má so službami súvisiaci neregistrovaný stav.

3.9 Mechanizmus kontroly prevádzky nosičov

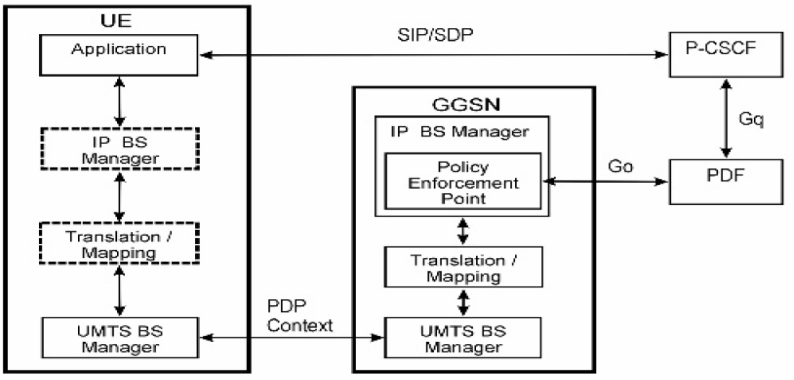
Oddelenie riadiacej roviny a užívateľskej roviny bolo možno jedným s najdôležitejších aspektov dizajnu IMS. Úplná nezávislosť vrstiev nie je reálna, pretože bez interakcie medzi užívateľskou rovinou a riadiacou rovinou operátori nie sú schopní kontrolovať kvalitu služieb (Quality of Service – QoS), zdroj/cieľ IMS mediálnej prevádzky a kedy budú média spustené a ukončené. Bol teda vytvorený mechanizmus pre autorizáciu a kontrolu použitia prevádzky nosičov určený pre IMS mediálnu prevádzku; bol založený na parametroch protokolu popisu relácie (Session Description Protocol – SDP) vyjednaných v relácii IMS. Táto celková interakcia medzi GPRS a IMS sa nazýva kontrola lokálnej politiky založenej na službe (Service-Based Local Policy - SBLP). Neskôr bola špecifikovaná účtovacia korelácia ako prídavná schopnosť. Obrázok 3.10 znázorňuje funkčné entity zahrnuté v SBLP. Obrázok zobrazuje model architektúry založený na Release 6, kde je použitá samostatná funkcia rozhodovania politiky (Policy Decision Function - PDF) a referenčný bod Gq. V architektúre Release 5 je PDF integrovaná s P-CSCF. Príklad v tejto časti nevysvetľuje ako P-CSCF mapuje informácie SIP/SDP na priemerové informačné prvky, ani ako sú informácie prenášané do PDF pomocou priemerových príkazov cez referenčný bod Gq. Naopak, príklad sa sústredí na základné skutočnosti: aké informácie sú potrebné zo signalizácie relácie SIP/SDP a akým spôsobom sú použité v PDF. Použitie referenčného bodu Gq:

- Správca služby IP nosiča (Bearer Service -BS) – riadi IP BS pomocou štandardného IP mechanizmu. Sídli v GGSN a prípadne v UE.
- Prekladacia/mapovacia funkcia – poskytuje vzájomnú komunikáciu medzi mechanizmom a parametrami použitými v rámci UMTS BS a parametrami použitými v rámci IP BS. Sídli v GGSN a prípadne v UE.
- Správca UMTS BS – riadi požiadavky na rezerváciu zdrojov z UE. Sídli v GGSN a v UE.
- Bod presadzovania politiky – je logická entita, ktorá presadzuje rozhodnutia politiky prijaté PDF. Sídli v GGSN a v UE.
- Funkcia rozhodovania politiky – je logický prvok rozhodovania politiky, ktorý používa štandardné IP mechanizmy pre zavedenie SBLP v IP mediálnej vrstve. V Release 5 sídli v P-CSCF. V Release 6 je to samostatná entita. Podľa [RFC2753] je

PDF efektívne bod rozhodovania politiky, ktorý definuje rámec pre prijímaciu kontrolu na základe politiky.

Existuje sedem funkcií SBLP. Týchto sedem funkcií je popísaných v nasledujúcich pododdieloch:

- autorizácia nosiča;
- schválenie odovzdanej QoS;
- odstránenie odovzdanej QoS;
- indikácia uvoľnenia nosiča;
- indikácia straty/obnovy nosiča;
- odobratie autorizácie;
- výmena účtovacích identifikátorov.



Obrázok 3.10 Entity SBLP.

3.9.1 Autorizácia nosiča

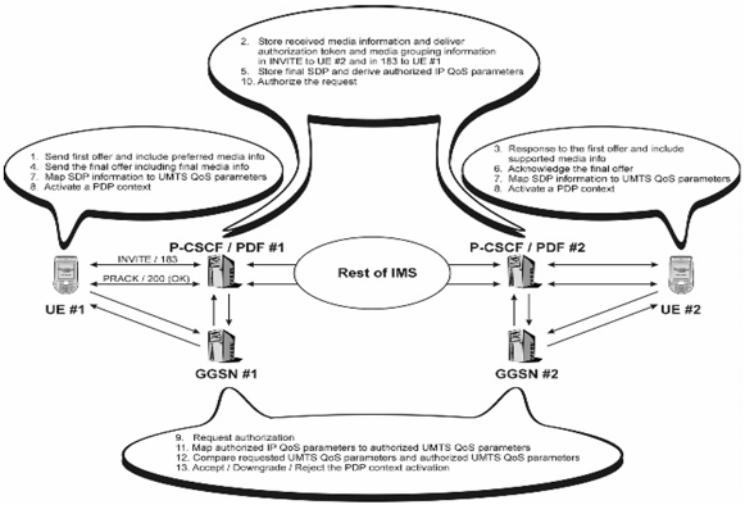
Vytvorenie a zmena relácie v IMS zahŕňa výmenu správ medzi koncovými zariadeniami pomocou SIP a SDP. Počas výmeny správ UE vyjednajú sadu mediálnych charakteristík (napr. spoločný(é) kodek(y)). Ak operátor použije SBLP, P-CSCF odošle relevantné SPD informácie funkcii PDF spolu s indikáciou pôvodcu. PDF zaznamená a autorizuje IP toky vybraných mediálnych komponentov mapovaním SPD parametrov na autorizované IP QoS parametre pre prenos na GGSN cez rozhranie Go.

Keď UE aktivuje alebo mení PDP kontext pre médiá, musí vykonať vlastné mapovanie, z SPD parametrov a aplikačných požiadaviek na niektoré UMTS QoS parametre. Aktivácia alebo zmena PDP kontextu bude tiež obsahovať prijatú autorizačnú známku a tokové identifikátory ako záväzné informácie.

Po prijatí aktivácie alebo zmeny PDP kontextu GGSN požiada PDF o autorizačné informácie. PDF porovná prijaté záväzné informácie s uloženými informáciami a vráti autorizačné rozhodnutie. Ak sú záväzné informácie potvrdené ako správne, PDF oznámi GGSN detaily o autorizácii média v rozhodnutí. Tieto detaily obsahujú IP QoS parametre a paketové klasifikátory súvisiace s PDP kontextom.

GGSN namapuje autorizované IP QoS parametre na autorizované UMTS QoS parametre a nakoniec GGSN porovná UMTS QoS parametre s autorizovanými UMTS QoS parametrami PDP kontextu. Ak sa UMTS QoS parametre z požiadavky na PDP kontext nachádzajú v rámci limitov autorizovaných funkciou PDF, aktivácia alebo zmena PDP kontextu bude prijatá. Obrázok 3.10 zobrazuje túto funkčnosť a pre zjednodušenie je PDF zobrazená ako časť P-CSCF. Keď existuje samostatná PDF, P-CSCF musí namapovať SIP/SDP signalizačné informácie na príslušné Priemerové informačné prvky a poslať príslušnú Priemerovú požiadavku funkcii PDF cez referenčný bod Gq.

Na Obrázku 3.11 môžeme vidieť dve rôzne fázy: autorizáciu QoS zdrojov (Kroky 1-6) a rezervácia zdrojov (Kroky 7-14). Ďalej sa budeme podrobnejšie venovať týmto obom krokom a potom je popísaný záverečný krok autorizácie nosiča - t.j. schválenie odovzdanej QoS.



Obrázok 3.11 Autorizácia nosiča pomocou SBLP.

1. Send first offer and include preferred media info – Poslať prvú ponuku a zahrnúť informácie o preferovanom médiu
2. Store received media information and deliver authorization token and media grouping information in INVITE to UE #2 and in 183 to UE #1 - 1. Uložiť prijaté mediálne informácie a dodať autorizačnú známku a informácie o zoskupení médií v INVITE pre UE #2 a v 183 pre UE #1
3. Response to the first offer and include supported media info – Odpovedať na prvú ponuku a zahrnúť informácie o podporovanom médiu
4. Send the final offer including final media info – Poslať konečnú ponuku vrátane konečných informácií o médiu
5. Store final SDP and derive authorized IP QoS parameters – Uložiť konečný SDP a odvodiť autorizované IP QoS parametre
6. Acknowledge the final offer – Potvrdiť konečnú ponuku
7. Map SDP information to UMTS QoS parameters – Namapovať SPD informácie na UMTS QoS parametre
8. Activate a PDP context – Aktivovať PDP kontext
9. Request authorization – Vyžiadať autorizáciu
10. Authorize the request – Autorizovať požiadavku
11. Map authorized IP QoS parametres to authorized UMTS QoS parameters – Namapovať autorizované IP QoS parametre na autorizované UMPTS QoS parametre
12. Compare requested UMTS QoS parameters and authorized UMTS QoS parameters – Porovnať požadované UMTS QoS parametre a autorizované UMTS QoS parametre
13. Accept/Downgrade/Reject the PDP context activation – Prijať/Oslabiť/Odmietnuť aktiváciu PDP kontextu
Rest of IMS – Zostatok IMS

Autorizovať GoS zdroje

Kroky 2 a 5 na Obrázku 3.11 zodpovedajú procedúre autorizácie QoS zdrojov. Počas nastavenia relácie PDF zhromažďuje IP QoS autorizačné údaje. Tieto údaje zahŕňajú:

- Identifikátor toku – používaný pre identifikáciu IP tokov, ktoré sú popísané v rámci mediálneho komponentu spojeného s SIP reláciou. Identifikátor toku sa skladá z dvoch častí: (1) poradové číslo polohy popisu mediálneho komponentu

v informáciách popisu SPD relácie a (2) poradové číslo IP toku(ov) v rámci priradeného popisu mediálneho komponentu (vo vzostupnom poradí čísel portov).

- Rýchlosť prenosu údajov - táto informácia je odvodená z parametrov šírky pásma SPD. Rýchlosť prenosu údajov zahrnie všetky režijné náklady prichádzajúce z IP vrstvy a vyšších vrstiev (napr. UDP, RTP alebo RTCP), Ak je v relácii odsúhlasené použitie viacerých kodekov pre médium, potom je autorizovaná rýchlosť prenos údajov nastavená podľa kodeku vyžadujúceho najväčšiu šírku pásma.
- Trieda QoS - informácie QoS triedy predstavujú najvyššiu triedu, ktorá môže byť použitá pre mediálny komponent. Je odvodený z SPD popisu média.

Povedzme, že Tobias (UE #1 na Obrázku 3.11) chce hovoriť so svojou sestrou Terezou (UE #2). Okrem bežného hlasového hovoru chce Tobias aktivovať dvojsmerné a jednosmerné video prúdy. Jeho terminál teda zostaví SIP INVITE obsahujúci SDP, ktorý odráža preferencie Tobiasa a schopnosti jeho UE. SDP obsahuje podporované kodeky, požiadavky na šírku pásma (plus charakteristiky každého) a priradené čísla lokálnych portov pre každý možný mediálny tok. V tejto časti sa sústredíme len na tie parametre, ktoré sú potrebné pre SBLP. SDP odoslané z UE #1 by vyzeral nasledovne:

```
v = 0
o =- 3262464865 3262464868 IN IP6 5555::1:2:3:4
t = 3262377600 3262809600
m = video 50230 RTP/AVP 31
c = IN IP6 5555::1:2:3:4
b = AS:35
b = RS:700
b = RR:700
m = video 50240 RTP/AVP 31
c = IN IP6 5555::1:2:3:4
b = AS:32
b = RS:640
b = RR:640
a = sendonly
m = audio 3456 RTP/AVP 97 96
c = IN IP6 5555::1:2:3:4
b = AS:25.4
b = RS:500
b = RR:500
```

Keď PDF #1 na Obrázku 3.11 získa informácie založené na vyššie uvedených údajoch, je schopný formulovať autorizačné údaje pre downlink smer (z GGSN #1 do UE #1). Keď

Terezine UE odpovie, PDF #1 je schopné formulovať autorizačné údaje pre uplink smer (z UE #1 do GGSN #1). Všimnite si, že Tereza nechce prijímať jednosmerné video, príslušné číslo portu je teda nastavené na nulu:

v = 0
o = - 3262464865 3262464868 IN IP6 5555::1:2:3:4
t = 3262377600 3262809600
m = video 60230 RTP/AVP 31
c = IN IP6 5555::5:6:7:8
b = AS:35
b = RS:700
b = RR:700
m = video 0 RTP/AVP 31
c = IN IP6 5555::5:6:7:8
b = AS:32
b = RR:640
b = RS:640
a = recvonly
m = audio 3550 RTP/AVP 0
c = IN IP6 5555::5:6:7:8
b = AS:25.4
b = RS:500
b = RR:500

Na základe týchto informácií sú PDF #1 a PDF #2 schopné zhotoviť potrebné identifikátory toku. Tabuľka 3.3 zobrazuje identifikátory toku v PDF #1.

Rýchlosť prenosu údajov PDF odvodzuje hodnotu rýchlosti prenosu údajov pre mediálne IP tok(y) z "b=AS“ SPD parametra. Pre prípadné priradené IP toky protokolu kontroly prenosu v reálnom čase (RTCP) PDF použije SDP parametre „b=AS“,“b=RR“ a „b=RS“, ak sú dostupné. Keď SPD "b=RR" alebo b="RS" chýbajú, rýchlosť prenosu údajov pre RTCP IP toky je odvodená z dostupných parametrov, tak ako je to popísané v [3GPP TS 29.208]. Popis šírky pásma RTCP:

- Ak b = RS a b = RR exitujú, potom šírka pásma RTCP pre uplink (UL) a downlink (DL) = (bRS + bRR)/1,000].
- Ak chýba buď b = RS alebo b = RR, potom šírka pásma RTCP pre UP a DL = MAX(0.05 * bAS, bRS/1,000 alebo bRR/1,000].
- Ak b = RS aj b = RR chýbajú, šírka pásma RTCP pre UL a DL = 0.05 * bAS.

Tabuľka 3.3 Informácie o identifikátore toku v PDF #1.

Poradie „m“ riadku	Typ IP toku	Cieľová IP adresa	Číslo portu IP tokov	Identifikátor toku
1	RTP (video) DL	5555::1:2:3:4	50230	<1,1>
1	RTP (video) UL	5555::5:6:7:8	60230	<1,1>
1	RTP DL	5555::1:2:3:4	50231	<1,2>
1	RTP UL	5555::5:6:7:8	60231	<1,2>
3	RTP (audio) DL	5555::1:2:3:4	3456	<3,1>
3	RTP (audio) UL	5555::6:7:8:9	3550	<3,1>
3	RTP DL	5555::1:2:3:4	3457	<3,2>
3	RTP UL	5555::6:7:8:9	3551	<3,2>

Tabuľka 3.4 Maximálne rýchlosti prenosu pre typy média

Typ média (m-linka v SDP)	Maximálna autorizovaná trieda QoS
Dvojsmerné audio a video	A
Jednosmerné audio a video	B
Aplikácia	A
Údaje	E
Kontrola	C
Iné	F

Tabuľka 3.5 Maximálne rýchlosti prenosu a QoS trieda podľa identifikátoru toku v PDF #1.

	Identifikátor toku			
	<1,1>	<1,2>	<3,1>	<3,2>
Maximálna rýchlosť prenosu údajov downlink (kbps)	35	0.7	25.4	0.5
Maximálna rýchlosť prenosu údajov uplink (kbps)	35	0.7	25.4	0.5
Maximálna trieda QoS	A	A	A	A

QoS trieda PDF namapuje informácie o type média na najvyššiu triedu QoS, ktorá môže byť použitá pre médium. PDF použije rovnakú QoS triedu pre uplink aj downlink smer, keď sú použité obidva smery [3GPP TS 29.207]. [3GPP TS 29.208] obsahuje detailné pravidlá pre odvodenie (prehľad je uvedený v Tabuľke 3.4). Tabuľka 3.5 ukazuje, ako sú informácie z Tabuľky 3.5 použité v našom príklade. Maximálna autorizovaná trieda QoS pre RTCP IP tok je rovnaká, ako pre príslušný RTP IP mediálny tok.

Autorizovaná IP QoS bola vytvorená a uložená vo funkciách PDF počas krokov 2 a 5 v Obrázku 3.11 (autentifikácia nosiča). Autorizovaná IP QoS obsahuje triedu QoS a rýchlosť prenosu údajov. Zároveň PDFs vytvorili identifikátory toku, ktoré budú neskôr

použité na vytvorenie klasifikátorov paketov v GGSN. Tabuľka 3.5 uvádza prehľad doteraz uvedených skutočností.

Autorizačná známka Na Obrázku 3.11, Krok 2 uvádza: "dodať autorizačnú známku UE #1 a UE #2". Ale čo je to autorizačná známka?:

- Je to jedinečný identifikátor PDP kontextov spojených s názvom prístupového bodu.
- Je vytvorená v PDF, keď sú vytvorené autorizačné údaje.
- Tvorí ju identifikátor IMS relácie a PDF identifikátor.
- Jej syntax je v súlade s [RFC3520].
- Je dodaná do UE prostredníctvom [RFC3313].
- UE ju zahŕňa v požiadavku na aktiváciu/zmenu PDP kontextu.
- GGSN používa PDF identifikátor v rámci autorizačnej známky pre nájdenie PDF, ktorá má autorizované informácie o IP QoS.
- PDF používa autorizačnú známku pre nájdenie správnych autorizačných údajov po prijatí požiadaviek od GGSN.

Zoskupovanie médií SIP a IMS umožňujú nastavenie multimediálnych relácií, ktoré môžu zahrňovať rôzne komponenty, ako audio a video. Každá účastnícka strana môže pridať alebo odobrať mediálny komponent z prebiehajúcej relácie. Všetky komponenty by mali byť individuálne identifikovateľné pre účely účtovania a musí byť umožnené účtovať každý z týchto komponentov v relácii oddelenie.

Nanešťastie, Release 5 GGSN je schopné vytvoriť len jeden záznam o detaile hovoru GGSN (Call Detail Record - CDR) pre PDP kontext. Je teda nemožné oddeliť prevádzku pre každý mediálny komponent v rámci toho istého PDP kontextu. Keďže súčasný model účtovania tvorby údajov a koreláciu neumožňuje multiplexovanie mediálnych tokov v rovnakom sekundárnom PDP kontexte pre každý mediálny komponent, musí existovať mechanizmus na IMS úrovni, ktorý donúti UE otvoriť samostatné PDP kontexty pre každý mediálny komponent. Pre tento účel bola definovaná indikácia pre zachovanie oddelenia.

Keď P-CSCF príjme úvodnú požiadavku INVITE na ukončovacie nastavenie relácie alebo odpoveď 183 (postup relácie) na požiadavku INVITE na počiatočné nastavenie relácie, P-CSCF môže zmeniť SPD v súlade s [RFC3524] pre indikáciu UE, že

konkrétny(e) mediálny(e) prúd(y) bol(i) zoskupený(é) v súlade s lokálnou politikou [3GPP TS 24.229]. [RFC3524] definuje typ skupiny jediného rezervačného toku (Single Reservation Flow -SFR) (a = skupina:SRF). SRF skupiny sa používajú nasledovných spôsobom:

- Ak sieť chce prenášať konkrétne médium v rovnakom PDP kontexte, P-CSCF nastaví rovnakú hodnotu SRF pre tieto mediálne komponenty.
- Ak sieť chce prenášať konkrétne médium v rôznych PDP kontextoch, P-CSCF nastaví rôzne hodnoty SRF pre každý mediálny komponent.
- Ak sieť nenastaví indikáciu SRD, UE môže zoskupiť mediálne prúdy podľa svojho uváženia.

Nasledujúce ďalšie obmedzenia a smernice sú uvedené v štandardoch [3GPP TS 23.228] a [3GPP TS 24.229]:

- P-CSCF aplikuje a dodrží tú istú politiku počas celej relácie SIP.
- Ak je pridaný mediálny prúd a v počiatočnej INVITE alebo 183 (postup relácie) odpovedi bolo uvedené zoskupenie mediálnych tokov, P-CSCF zmení SPD v súlade s [RFC3524] pre indikáciu UE, že pridaný(é) mediálny(e) prúd(y) bude(ú) zoskupené buď v novej skupine alebo v jednej z existujúcich skupín.
- P-CSCF neaplikuje [RFC3524] na SDP pre dodatočný(é) mediálny(e) tok(y), ak zoskupenie mediálneho toku(ov) nebolo uvedené v počiatočnej požiadavke INVITE alebo 183 (postup relácie) odpovedi.
- P-CSCF oznámi preskupenie mediálneho toku(ov) v rámci SDP.
- Pre všetky pridružené IP toky (napr. RTP/RTCP) používané UE pre podporu jedného mediálneho komponentu sa predpokladá, že budú prenášané v rámci rovnakého PDP kontextu.
- V Release 5 sa predpokladá, že mediálne komponenty z rôznych IMS relácií nie sú prenášané v rámci rovnakého PDP kontextu. Táto požiadavka neplatí v Release 6, keďže Release 6 pridáva schopnosť účtovať na báze IP toku.

Podľa nášho príkladu P-CSCF # 1 vynúti samostatný PDP kontext pre všetky typy médií v odpovedi 183 (postup relácie) nasledujúcim spôsobom (183 smerom k UE #1):

v = 0
o =- 3262464865 3262464868 IN IP6 5555::1:2:3:4
t = 3262377600 3262809600
a = skupina:SRF 1
a = skupina:SRF 2
a = skupina:SRF 3
m = video 60230 RTP/AVP 31
a = mid: 1
c = IN IP6 5555::5:6:7:8
b = AS:35
b = RS:700
b = RR:700
m = video 0 RTP/AVP 31
a = mid: 2
c = IN IP6 5555::5:6:7:8
b = AS:32
b = RS:640
b = RR:640
a = recvonly
m = audio 3550 RTP/AVP 0
a = mid:3
c = IN IP6 5555::5:6:7:8
b = AS:25.4
b = RS:500
b = RR:500

Problematika rozdvojenia Keď P-CSCF príjme rozdvojenú odpoveď, postúpi informácie PDF. Keď PDF príjme rozdvojovaciu indikáciu, tiež priradí predtým pridelenú autorizačnú známku rozdvojenej odpovedi. Okrem toho PDF autorizuje akékoľvek dodatočné mediálne komponenty a akékoľvek zvýšené požiadavky QoS pre predtým autorizované mediálne komponenty, ako je to požadované v rozdvojenej odpovedi. QoS autorizovaná pre mediálny komponent je teda rovná najvyššej požadovanej QoS pre tento mediálny komponent ktoroukoľvek z rozdvojených odpovedí [3GPP TS 29.207].

Rezervovanie zdrojov

Funkcie UE

Keď UE príjme autorizačnú známku v rámci výmeny správ medzi koncovými zariadeniami vie, že SBLP je aplikovaná na sieti. Musí teda vytvoriť požadované QoS parametre a identifikátory toku pre požiadavku aktivácie (zmeny) PDP kontextu. Požadované parametre QoS zahŕňajú informácie uvedené v Tabuľke 3.6. Z hľadiska

SBLP prvé tri riadky v Tabuľke 3.6 uvádzajú hodnoty, ktoré sú zaujímavé. V prípade záujmu môžu čitatelia nájsť detailné popisy ostatných QoS parametrov v [3GPP TS 23.107]. Na tomto mieste je popísaná trieda prevádzky, garantovaná bitová rýchlosť prenosu a maximálna bitová rýchlosť prenosu:

- Trieda prevádzky - štyri rôzne triedy prevádzky definované pre UMTS sú konverzačná, prúdová, interaktívna a základná. Po zahrnutí triedy prevádzky môže UMTS definovať predpoklady o zdroji prevádzky a optimalizovať prenos pre všetky typy prevádzky.
- Garantovaná bitová rýchlosť (Guaranteed Bit Rate - GBR) – popisuje bitovú rýchlosť, ktorú služba nosiča UMTS garantuje užívateľovi alebo aplikácii.
- Maximálna bitová rýchlosť (Maximum Bit Gate – MBR) - popisuje hornú hranicu, ktorú môže užívateľ alebo aplikácia prijať alebo poskytnúť. To umožní použite rôznych rýchlostí pre prevádzku (napr. medzi GBR a MBR).

Tabuľka 3.6 Požadované QoS parametre.

Trieda prevádzky	Maximálna bitová rýchlosť pre downlink
Garantovaná bitová rýchlosť pre downlink	Maximálna bitová rýchlosť pre uplink
Garantovaná bitová rýchlosť pre uplink	
Informácia o SDU formáte	Maximálna veľkosť SDU
Chybový pomer SDU	Zvyškový BER
Dodanie chybných SDU	Priorita riadenia prevádzky
Oneskorenie prenosu	Priorita pridenia/zadržania
Deskriptor zdrojových štatistík	Poradie dodania

Hodnoty tried prevádzky – GBR pre downlink/uplink a MBR pre downlink/uplink – nemali by presiahnuť odvodené hodnoty maximálnej povolenej šírky pásma a maximálnej povolenej triedy prevádzku pre identifikátor toku. Maximálna povolená šírka pásma v autorizovanej triede prevádzky je odvodená podľa Tabuľky 3.7. Presné pravidlá pre odvodenie obidvoch parametrov sú popísané v [3GPP TS 29.208].

[3GPP TS 26.236] definuje odporúčania o tom, akým spôsobom by mali byť nastavené ostatné požadované QoS parametre pre konverzačné kodekové aplikácie.

Zodpovedajúcim spôsobom [3GPP TS 26.234] definuje odporúčania o tom, akým spôsobom by mali byť nastavené požadované QoS parametre pre prúdové kodekové aplikácie.

Tabuľka 3.7 Maximálna povolená trieda prevádzky podľa typu média v UE.

Typ média (m-linka v SPD)	Trieda prevádzky UMTS
Dvojsmerné audio a video	Konverzačná
Jednosmerné audio a video	Prúdová
Aplikácia	Konverzačná
Údaje	Interaktívna
Kontrola	Interaktívna
Iné	Základná

Tabuľka 3.8 Hodnoty maximálnych povolených UMTS QoS parametrov podľa identifikátora toku, napríklad tak, ako to vypočítalo EU #1 (Tobias) z príkladu.

	Identifikátor toku			
	<1,1>	<1,2>	<3,1>	<3,2>
Maximálna rýchlosť prenosu údajov do (DL) (kbps)	35	0.7	25.4	0.5
Maximálna rýchlosť prenosu údajov UL (kbps)	35	0.7	25.4	0.5
Maximálna trieda QoS	Konverzačná	Konverzačná	Konverzačná	Konverzačná

Identifikátory toku sú odvodené z UE rovnakým spôsobom ako v PDF. Tabuľka 3.8 uvádza maximálne povolené UMTS QoS parametre podľa identifikátora toku vypočítané UE.

UE sa ďalej musí rozhodnúť, koľko PDP kontextov je potrebných. Kľúčovými faktormi je charakter mediálnych prúdov (napr. požadovaná trieda prevádzky) a prijaté indikácia o zoskupené od P-CSCF. V našom príklade sú dva rôzne typy dvojsmerných médií: video a audio. Obidve médiá by požadovali vysokú QoS (malé oneskorenie a zachované časové spojenie); P-CSCF teda stanoví, že je potrebný samostatný PDP kontext pre každý mediálny komponent. UE #1 by malo teda aktivovať dva rôzne PDP kontexty. V opačnom prípade by aktivácia PDP kontextu zlyhala z dôvodu SBLP rozhodnutia vynúteného PDF. Keď P-CSCF nestanovila, že sú potrebné samostatné PDP kontexty, UE môže optimalizovať počet PDP kontextov. V našom príklade by UE mohlo otvoriť jeden nový PDP kontext pre video a audio. UE by okrem toho mohlo prenášať nové komponenty pomocou existujúceho PDP, ak vhodný PDP kontext existuje. V

Tabuľke 3.9 sú uvedené maximálne povolene UMST QoS parametre podľa PDP kontextu vypočítané UE #1.

UE teraz ukončilo Krok 7 z Obrázku 3.11. Po odvodení a vybraní vhodných požadovaných QoS parametrov, UE aktivuje potrebné PDP kontexty. Autorizačná známka a identifikátory toku sú vložené do informačného prvku šablóny toku prevádzky. Detailný popis o spôsobe prenášania autorizačnej známky a identifikátorov toku v informačnom prvku šablóny toku prevádzky sú uvedené v [3GPP TS 24.008]. Požadované QoS parametre sú vložené do QoS informačného prvku. Detailný popis spôsobu prenášania požadovaných QoS parametrov v informačnom prvku QoS je uvedený [3GPP TS 24.008].

Tabuľka 3.9 Maximálne povolené hodnoty UMTS QoS parametrov podľa PDP kontextu vypočítané EU #1 z príkladu.

	PDP kontext #	
	1	2
Maximálna povolená šírka pásma DL (kbps)	35.7	25.9
Maximálna povolená šírka pásma UL (kbps)	35.7	25.9
Maximálna povolená trieda prevádzky	Konverzačná	Konverzačná

Funkcie GGSN

Keď GGSN príjme požiadavku na aktiváciu sekundárneho PDP kontextu na názov prístupového bodu (Access Point Name – APN), pre ktorý je aktivovaný referenčný bod Go, GGSN:

- Identifikuje správnu PDF získaním PDF identity z poskytnutej autorizačnej známky. Ak autorizačná známka chýba, GGSN môže buď odmietnuť požiadavku alebo ju prijať v lehote stanovenej lokálne uloženou politikou QoS. Štandard Release 6 vyžaduje, aby GGSN prijal aspoň jednu požiadavku na aktiváciu sekundárneho PDP kontextu bez záväzných informácií alebo autorizácie SBLP, ak požadovaný PDP kontext nie je kontext v reálnom čase (trieda prevádzky UMTS „základná" alebo „interaktívna") a tento PDP kontext ešte nebol priradený UE pre ten istý APN [3GPP TS 29.207]. Tento druh funkčnosti je potrebný, keď operátor ponúka jediný IMS APN pre služby, ktoré nie sú stanovené pri SLBP (napr. Push to talk cez mobilný telefón alebo posielanie správ na báze relácie) a služby, ktorú sú stanovené pri SBLP (napr. hlasové a video relácie).

- Požaduje autorizačné informácie z PDF pre IP toky prenášané PDP kontextom. Táto požiadavka je požiadavkou služby spoločnej otvorenej politiky (Common Open Policy Service - COPS) a obsahuje poskytnutú autorizačnú známku a poskytnuté identifikátory toku.
- Vynucuje rozhodnutie po prijatí autorizačného rozhodnutia. Autorizačné rozhodnutie je vydané ako správa COPS autorizácia_rozhodnutia. Hlavné zložky rozhodnutia sú:
  - indikácia rozhodnutia - uplink, downlink;
  - autorizovaná IP QoS – rýchlosť prenosu údajov, maximálna povolená trieda QoS;
  - klasifikátory paketov (tiež nazývané popis brány) – zdrojová IP adresa a číslo(a) portu, cieľová IP adresa a číslo(a) portu, ID protokol.
- Mapuje autorizovanú IP QoS na autorizovanú UMTS QoS.
- Porovná požadované QoS parametre s autorizovanou UMST QoS. Ak sú všetky požadované parametre v rámci limitov, aktivácia PDP kontextu bude prijatá. Inými slovami, ak sú splnené nasledujúce kritéria[3GPP TS 29.208]:
  - požadované GBR DL/UL (ak je požadovaná trieda prevádzky konverzačná alebo prúdová) alebo MBR DL/UL (ak je požadovaná trieda prevádzky interaktívna alebo základná) je menšie alebo rovné maximálnej povolenej rýchlosti prenosu údajov DL/UL; a
  - požadovaná trieda prevádzky je menšia alebo rovná maximálnej požadovanej triede prevádzky.

  Ak požadovaná QoS presahuje autorizovanú UMTS QoS, úroveň informácií je znížená z informácií o požadovanej UMTS QoS na informácie o autorizovanej UMTS QoS.
- Vytvorí popis brány založený na prijatom klasifikátore paketov. Popis brány umožní vykonanie funkcie brány. Funkcia brány aktivuje alebo deaktivuje preposielanie IP paketov. Ak je brána zatvorená všetky pakety súvisiacich IP tokov sú zahodené. Ak je brána otvorená, potom pakety súvisiacich IP tokov môžu byť preposielané. Otvorenie brány môže byť súčasťou udalosti autorizačného rozhodnutia alebo to môže byť samostatné rozhodnutie. Zatvorenie brány môže byť súčasťou odvolania autorizačného rozhodnutia.
- Ukladá záväzné informácie.
- Môže ukladať údaje o rozhodnutí politiky z PDF rozhodnutí do vyrovnávacej pamäte.

Počas zmeny sekundárneho PDP kontextu GGSN môže použiť informácie predtým uložené do vyrovnávacej pamäte pre rozhodnutie o lokálnej politike v prípade, že požiadavka na zmenu nepresiahne predtým autorizovanú QoS. Ak GGSN nemá informácie uložené vo vyrovnávacej pamäti, vykoná vyššie popísané funkcie.

Funkcie PDF

Keď PDF príjme COPS požiadavku, PDF potvrdí, že:

- Autorizačná známka je platná.
- Príslušná SIP relácia existuje. Ak sú mediálne komponenty z rôznych relácií multiplexované v rovnakom PDP kontexte, existuje viac ako jedna autorizačná známka a PDF identifikuje jednu IMS reláciu pre každú známku. Táto schopnosť bola pridaná v Release 6.
- Záväzná informácia obsahuje platný(é) identifikátor(y) toku.
- Autorizačná známka nebola zmenená v požiadavke na zmenu autorizácie.
- UE dodržiava indikáciu o zoskupení.
- Ak je potvrdenie úspešné, PDF určí a oznámi autorizovanú IP QoS, klasifikátory paketov a stav brány použité pre GGSN. Keď záväzné informácie tvorí viac ako jeden identifikátor toku, informácie poslané späť GGSN budú zahŕňať agregovanú QoS pre všetky IP toky a vhodný filter(filtre) paketov pre tieto IP toky.

V našom príklad UE #1 potrebuje aktivovať dva PDP kontexty. Keď príde požiadavka na aktiváciu sekundárneho PDP kontextu pre prvý PDP kontext (dvojsmerné video) do GGSN #1, ktorý získa autorizačnú známku a identifikátory toku (1,1 a 1,2) zo šablóny toku prevádzky a pošle ich PDF #1, PDF #1 použije autorizačnú známku pre identifikáciu autorizovaných IP QoS parametrov a klasifikátorov paketov zodpovedajúcich identifikátorom toku (1,1, a 1,2). GGSN #1 namapuje autorizovanú IP QoS na autorizovanú UMTS QoS; porovná hodnoty a zistí, že všetko je OK. Nakoniec GGSN #1 príjme požiadavku a nainštaluje bránu, na základe prijatých klasifikátorov paketov. Rovnaký postup sa použije pre ostatné súvisiace PDP kontexty.

Okrem toho môže PDP poslať GGSN nové samostatné rozhodnutie, keď dostane od P-CSCF zmenené SDP informácie. To môže byť potrebné napríklad v prípade rozdvojenia.

3.9.2 Schválenie funkcie odovzdania QoS

Počas procedúry rezervácie zdrojov PDF pošle klasifikátory paketov do GGSN. Na základe klasifikátorov paketov GGSN formuluje kontrolu od brány k politike pre prichádzajúcu a odchádzajúcu prevádzku. PDF sa rozhodne, kedy otvorí bránu. Keď je brána otvorená, GGSN umožní prevádzke prechádzať cez GGSN. Otvorenie brány by mohlo byť poslané ako odpoveď na počiatočnú autorizačnú požiadavku z GGSN alebo môže byť rozhodnutie poslané ako samostatné rozhodnutie. Ak sa použije samostatné rozhodnutie, operátor môže zaistiť, že zdroje užívateľskej roviny nebudú použité pred konečným prijatím IMS relácie (napr. keď je prijatá správa SIP 200 OK). V tomto prípade koncoví užívatelia stratia všetky oznámenia, ktoré boli doručené pred ukončením relácie, keďže GGSN zahodí všetky prichádzajúce IP pakety užívateľskej roviny.

3.9.3 Odstránenie funkcie odovzdania QoS

Táto funkcia zatvára bránu v GGSN, keď PDF nepovolí prechod prevádzky cez GGSN. Táto funkcia sa použije napríklad keď je mediálny komponent určitej relácie zastavený z dôvodu opätovného vyjednávania média.

3.9.4 Indikácia funkcie uvoľnenia nosiča

Keď GGSN príjme požiadavku na zmazanie PDP kontextu a PDP kontext bol predtým autorizovaný cez referenčný bod Go, GGSN informuje PDF o uvoľnení nosiča súvisiaceho s SIP reláciou poslaním správy na zmazanie požiadavku na stav COPS. PDF odstráni autorizáciu pre príslušný(é) mediálny(e) komponent(y). Keď PDF príjme správu o tom, že nosič boľ uvoľnený, môže požiadať P-CSCF o uvoľnenie relácie(í) a odvolanie všetkých súvisiacich autorizácií médií pomocou procedúry popísanej v Časti 3.10.6.

3.9.5 Indikácia straty/obnovy nosiča

Keď je hodnota MBR rovná 0 kbit/s v požiadavke na aktualizáciu PDP kontextu, GGSN musí poslať COPS správu s hlásením PDF. Rovnako keď je MBR zmenené z 0 kbit/s, GGSN pošle COPRS správu s hlásením PDF po prijatí aktualizácie z obslužného GPRS podporného uzla (Serving GPRS Support Node - SGSN).

Pomocou tohto mechanizmu môže IMS zistiť, či UE stratilo/obnovilo svoj(e) rádiové(ý) nosič(e), keď je v GPRS systéme použitá prúdová alebo konverzačná trieda prevádzky. [3GPP TS 23.060] stanoví, že SGSN musí poslať požiadavku na aktualizáciu PDP kontextu, keď riadiaca jednotka rádiovej siete (Radio Network Controller - RNC) informuje SGSN o uvoľnení Iu alebo uvoľnení nosiča rádiového prístupu. Keď PDF dostane správu, že MBR sa rovná 0 kbit/s, môže požiadať P-CSCF o uvoľnenie relácie(í) a odvolanie všetkých súvisiacich autorizácií médií pomocou procedúry popísanej v Časti 3.10.6.

3.9.6 Odvolávacia funkcia

Táto funkcia sa používa pre vynútenie uvoľnenia predtým autorizovaných zdrojov nosiča v GPRS sieti. Pomocou tohto mechanizmu je PDF schopná napríklad zaistiť, že UE uvoľní PDP kontext, keď je SIP relácia ukončená, alebo že UE zmení PDP kontext, keď je mediálny komponent viazaný na PDP kontext odstránený z relácie. Ak to UE nespraví pred uplynutím lehoty vopred definovanej operátorom, PDF odvolá zdroje.

3.9.7 Výmenná funkcia účtovacích identifikátorov

Referenčný bod Go je spojenie medzi IMS a GPRS sieťami. Pre vykonanie účtovacej korelácie v súlade s popisom v Časti 3.11.6, IMS vrstva musí poznať príslušný účtovací identifikátor vrstvy GPRS a naopak. Tieto účtovacie identifikátory sú vymenené počas autorizačnej fázy nosiča. Účtovací identifikátor IMS je dodaný GGSN v rámci správy autorizačného rozhodnutia, zatiaľ čo účtovací identifikátor GPRS je dodaný PDF ako súčasť autorizačnej správy.

3.9.8 Použitie referenčného bodu Gq

Pomocou referenčného bodu Gq môže byť PDF nasadené ako samostatná sieťová entita. Keď je použitá samostatný PDF, P-CSCF musí postúpiť potrebné informácie odvodené z signalizácie relácie SIP/SDP funkcii PDF. PDF tiež používa Gq na poslanie odpovedí a nezávislých oznámení P-CSCF. Pre postúpenie informácií P-CSCF a PDF používajú Priemerové príkazy, v súlade s definíciou v RFC3588, NASREQ aplikácia

Priemeru a 3GPP TS 29.209. Táto časť poskytuje stručný prehľad týchto Priemerových príkazov a ich použitia medzi P-CSCF a PDF pre podporu rôznych SBLP funkcií.

V referenčnom bode Gq sú použité štyri páry požiadavky a odpovede:

- AA-Požiadavka/AA-Odpoveď (AA-Request/AA-Answer - AAR&AAA);
- Požiadavka na opätovnú registráciu/Odpoveď na opätovnú registráciu (Re-Auth-Request/Re-Auth-Answer - RAR&RAA);
- Požiadavka na ukončenie relácie/Odpoveď na ukončenie relácie (Session-Termination-Request/Session-Termination-Anwer - STR&STA);
- Požiadavka na prerušenie relácie/Odpoveď na prerušenie relácie (Abort-Session-Request/Abort-Session-Answer - ASR&ASA).

Autorizácia nosiča

Keď je na sieti použitá SBLP, P-CSCF musí poslať relevantné informácie získané zo signalizácie relácie SIP/SDP funkcii PDF. Tieto informácie PDF použije pre prijatie autorizačného rozhodnutia o požiadavke prijatej cez referenčný bod Go. Okrem toho P-CSCF potrebuje získať autorizačnú známku a GPRS účtovací identifikátor pre účely korelácie účtovania. Pre tento účel sa použijú páry Priemerových príkazov AAR&AAA a RAR&AAA.

Po prijatí SIP požiadavky alebo odpovede obsahujúcej SPD informácie, P-CSCF pošle PDF požiadavku AAR. AAR obsahuje okrem iných základných prvkov informácie o mediálnom prúde, politiku rezervácie zdrojov, politiku indikácie preposielania, IMS účtovací identifikátor, informácie o použitej aplikácii a informácie a SIP rozdvojení. Podľa nášho príkladu P-CSCF #1 na obrázku 3.11 najprv vydá príkaz AAR, keď dostane požiadavku SIP INVITE od Tobiasovho UE. Tento príkaz bude niesť potrebné informácie pre vytvorenie downlink informácií (identifikátory toku, výpočet maximálnej šírky pásma a odvodenie maximálnej povolenej triedy QoS) v PDF. P-CSCF # druhýkrát vydá príkaz AAR, keď dostane odpoveď 183 o postupe relácie od Terezinho UE. Druhý príkaz AAR bude niesť informácie potrebné pre vytvorenie uplink informácií. PDF je teraz pripravená na autorizáciu celej požiadavky na aktiváciu nosiča.

Prostredníctvom úvodného príkazu AAR môže P-CSCF tiež určiť, či P-CSCF chce byť kontaktovaná pri každej autorizácii nosiča alebo či PDF môže použiť dostupné informácie pre samostatné prijatie rozhodnutia (politika rezervácie zdrojov). Okrem toho

P-CSCF môže určiť, či chce dostávať indikácie o strate nosiča, obnove nosiča alebo uvoľnení nosiča (politika preposielania indikácií). V týchto prípadoch PDF pošle príkaz RAR funkcii P-CSCF po prijatí príslušnej správy z GGSN cez referenčný bod Go. Príkaz RAR je potvrdený príkazom RAA. Príkaz AAR je potvrdený príkazom AAA. Autorizačná známka a/alebo účtovací identifikátor GPRS a/alebo IP adresa GGSN pre P-CSCF sú dodané v rámci príkazu AAA.

Schválenie a zrušenie odovzdanej QoS

Schválenie a odstránenie odovzdanej QoS – t.j. otvorenie/zatvorenie/odstránenie príslušnej brány(brán) v GGSN - je realizované ako súčasť príkazu AAR. Pre tento účel bol vyvinutý AVP Priemer špecifický pre 3GPP (3GPP-specific Diameter AVP), nazývaný „AVP pre stav toku“ [3GPP TS 29.209]. Tento AVP môže mať päť rôznych hodnôt: aktivovať uplink, aktivovať downlink, aktivované (obidva smery), deaktivované alebo odstránené. Rôzne “aktivované“ hodnoty sa používajú pre otvorenie brán (napr. povolenie prechodu prevádzky na užívateľskej rovine). P-CSCF môže dať PDF pokyn na otvorenie príslušných brán buď v úvodnom AAR príkaze alebo v AAR príkaze, ktorý je spustený po prijatí SIP 200 OK v P-CSCF. P-CSCF používa „deaktivovanú“ hodnotu napríklad keď je SIP relácia alebo jeden z jej mediálnych komponentov zastavený. "Odstránená“ hodnota sa používa na odstránenie autorizácie IP toku(ov). K tomu môže dôjsť napríklad vtedy, keď sú určité komponenty odstránené z SIP relácie.

Indikácia funkcie uvoľnenia nosiča

Po prijatí oznámenia o uvoľnení nosiča z GGSN cez referenčný bod Go musí PDF oboznámiť P-CSCF, ak P-CSCF požaduje tento typ oznámenia. PDF používa príkaz ASR ak sú ovplyvnené všetky toky v rámci SIP relácie. V rámci príkazu ASR 3GPP definoval AVP špecifický pre 3GPP nazývaný "AVP pre dôvod prerušenia", pre uvedenie dôvodu uvoľnenia nosiča. Príkaz RAR sa použije ako alternatíva, ak nie sú ovplyvnené všetky IP toky v rámci SIP relácie. V rámci príkazu RAR 3GPP definoval AVP špecifický pre 3GPP nazývaný "AVP pre špecifickú akciu", pre uvedenie dôvodu uvoľnenia nosiča. K tomu by mohlo dôjsť napríklad vtedy, keď je zahodený len video komponent multimediálnej relácie.

Indikácia straty/obnovy nosiča

Keď GGSN oznámi stratu alebo obnovu nosiča cez referenčný bod GO, PDF musí oboznámiť P-CSCF, ak P-CSCF požaduje tento typ oznámenia. Pre tento účel PDF vydá príkaz RAR, vrátane AVP pre špecifickú akciu, pre indikáciu straty alebo obnovy nosiča.

Tabuľka 3.10 Príkazy Gq.

Názov príkazu	Účel	Skratka	Zdroj	Cieľ
AA-Požiadavka	P-CSCF používa AAR na pretlačenie informácie o SIP relácii a účtovacieho korelačného identifikátora IMS smerom k PDF	AAR	P-CSCF	PDF
AA-Odpoveď	AAA potvrdzuje AAR, dodáva autorizačnú známku a GPRS účtovací korelačný identifikátor funkcii P-CSCF	AAA	PDF	P-CSCF
Požiadavka na opätovnú autorizáciu	RAR dodáva správy (strata/obnova nosiča, uvoľnenie niektorého komponentu(ov) relácie) a obsahuje požiadavku na odoslanie informácií o relácii	RAR	PDF	P-CSCF
Odpoveď na opätovnú autorizáciu	RAA sa používa na potvrdenie príkazu RAR. Môže obsahovať napríklad informácie o SIP relácii.	RAA	P-CSCF	PDF
Požiadavka na ukončenie relácie	STR sa používa na zaistenie, že zdroje nosiča sú uvoľnené spolu s uvoľnením SIP relácie.	STR	P-CSCF	PDF
Odpoveď na ukončenie relácie	STA sa používa na potvrdenie príkazu STR.	STA	PDF	P-CSCF
Požiadavka na prerušenie relácie	ASR sa používa na informovanie P-CSCF, že všetky nosiče súvisiace s konkrétnou SIP reláciou boli uvoľnené.	ASR	PDF	P-CSCF
Odpoveď na prerušenie relácie	ASA sa používa na potvrdenie príkazu ASR.	ASA	P-CSCF	PDF

Odvolávacia funkcia

Pre spustenie uvoľnenia PDP kontextu(ov) spojených s SIP reláciou funkcia P-CSCF pošle príkaz STR. K tomu dôjde napríklad pri uvoľnení SIP relácie. Keď PDF príjme tento príkaz, pošle ďalšiu správu cez referenčný bod Go pre spustenie deaktivácie PDP kontextu iniciovanej GGSN, s cieľom predísť zneužitiu nosiča po ukončení SIP relácie.

3.10 Účtovanie

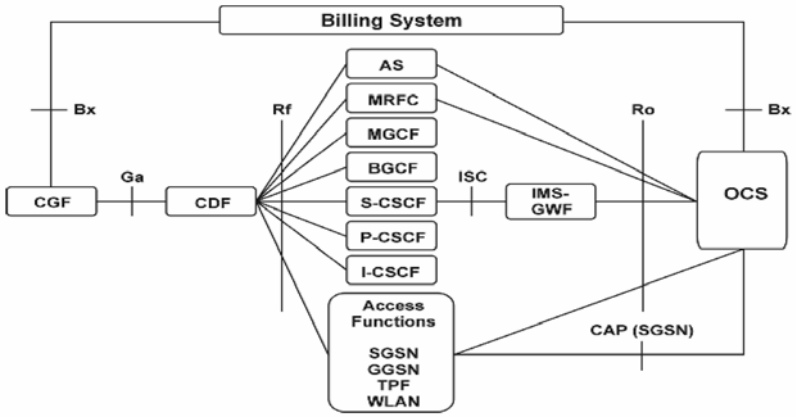
Nepaušálne schémy na báze objemu sú tradičné účtovacie modely v súčasných komunikačných sieťach na báze IP. IMS prináša nové účtovacie modely, ktoré zas prinášajú rôzne obchodné modely pre operátorov IMS. Schopnosť účtovať na základe relácie alebo udalosti alebo služby je jedna z kľúčových výhod, ktoré IMS prináša pre operátorov. Výhody sú plánované aj pre koncových užívateľov. Operátor je napríklad schopný ponúknuť peer-to-peer hry a o predplatenú službu (t.j. užívateľ potrebuje mať peniaze na účte pred využitím služieb) a iné multimediálne relácie ako služby platené po využití (t.j. užívateľ platí za služby pravidelne, napríklad jedenkrát mesačne), alebo okamžité správy by mohli byť dostupné ako nepaušálna služba a posielanie správ na báze relácie účtované odlišne (napr. na základe trvania relácie alebo na základe prenesených bytov).

Pre ponúknutie služby platenej po využití IMS musí podporovať mechanizmus pre offline účtovanie. Offline účtovanie je účtovací proces, kde sú účtovacie informácie zhromažďované hlavne po relácii a účtovací systém neovplyvňuje používanú službu v reálnom čase. V tomto podeli užívateľ typicky dostáva mesačnú faktúru, ktorá zobrazuje účtovateľné položky za určité časové obdobie. Predplatená služba vyžaduje podporu online účtovania. To znamená, že sieťové entity IMS sa musia informovať v online účtovacom systéme (Online Charging System – OCS) predtým, ako umožnia užívateľom využívať služby. OCS zodpovedá za interakciu s užívateľským účtom v reálnom čase a za kontrolu a monitorovanie poplatkov súvisiacich s použitím služby.

Sieťové entity IMS sú nakonfigurované tak, aby zistili, kedy je splnená spúšťacia požiadavka účtovania. Po detekcii entita zhromaždí potrebné informácie z SIP požiadavky a buď vyžiada povolenie z účtovacieho systému (online účtovanie) na pokračovanie v spracovaní SIP požiadavky , alebo pošle relevantné informácie do účtovacieho systému pre vytvorenie CDR pre konečné spracovanie (offline účtovanie) a povolí pokračovanie SIP požiadavky. Spúšťacím mechanizmus účtovania by mohla byť požiadavka na iniciáciu relácie, zmenu relácie, ukončenie relácie (účtovania na báze relácie), alebo by to mohla byť niektorá SIP transakcia – napr. požiadavky MESSAGE, PUBLISH, SUBSCRIBE (účtovanie na báze udalosti). Spúšťacím mechanizmom môže byť tiež prítomnosť SIP hlavičky alebo SPD informácie. Na základe získaných informácií účtovací systém buď zoberie kredit z účtu užívateľa (online účtovanie) alebo presunie CDR do fakturačného systému. Táto časť je založená na účtovacích riešeniach Release 6.

3.10.1 Účtovacia architektúra

Z dôvodu rozdielnej podoby účtovacích modelov boli definované rôzne riešenia architektúry pre offline a online účtovanie. Obrázok 3.12 znázorňuje vysoko úrovňovú účtovaciu architektúru IMS. Ľavá strana obrázku zobrazuje offline účtovanie a pravá strana ukazuje online účtovanie. Dopady účtovania na báze tokov nie sú v obrázku znázornené.



Obrázok 3.12 Účtovacia architektúra IMS

Billing System – Fakturačný systém
Access Functions – Prístupové funkcie

Na obrázku môžete vidieť, že všetky IMS entity riadiace SIP signalizáciu sú schopné komunikovať s offline účtovacou entitou - t.j. funkcia účtovacích údajov (Charging Data Functions - CDF) – pomocou jediného Rf referenčného bodu na báze Priemeru [3GPP TS 32.299]. CDF príjme Priemerovú požiadavku aj od prístupových sieťových entít a na základe informácii poskytnutých rôznymi entitami vytvorí CDRs, ktoré sú dodané funkcii účtovacej brány (Charging Gateway Function – CGF) cez referenčný bod Ga [3GPP TS 32.295]. Nakoniec CGF spracuje prijaté CDRs a presunie konečný(é) CDR(s) do fakturačného systému pomocou referenčného bodu Bx.

Na rozdiel od offline účtovania v online účtovaní sú zahrnuté len tri IMS entity (AS, MRFC a S-CSCF). Okrem toho S-CSCF nemôže komunikovať priamo s OCS kvôli zlému dizajnu časového rámca Release 5. Funkcia IMS brány (IMS-Gateway Function - IMS-GWF) sa požíva pre vykonanie potrebných konverzií protokolu. OCS podporuje dva

referenčné body z iných sieťových entít. SGSN používa CAMEL aplikačnú zložku (CAP) a zvyšné entity používajú referenčný bod Ro založený na Priemere. Rovnako ako CGF v offline účtovaní, OCS je tiež schopné vytvoriť CDRs okrem riadenia kontroly kreditu (schválenie zdrojov v reálnom čase).

3.10.2 Offline účtovanie

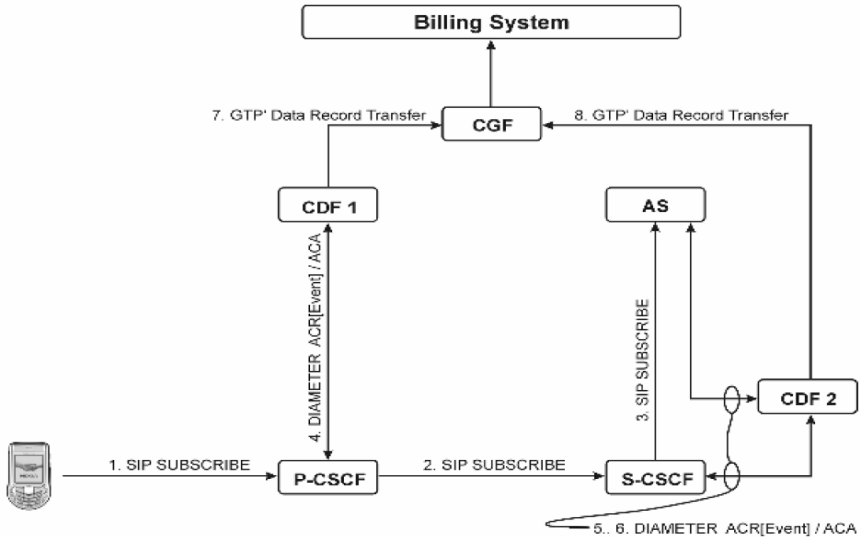
IMS signalizácia prechádza cez rôzne IMS entity a ako to bolo uvedené v predchádzajúcom texte, všetky entity sú schopné vytvoriť offline účtovacie informácie. Každá entita schopná offline účtovania obsahuje integrovanú funkciu nazývanú funkcia spustenia účtovania (Charging Trigger Function – CTF). CTF je informovaná o spúšťacích mechanizmoch účtovania (ako napríklad začiatok IMS relácie, zmena IMS relácie, ukončenie IMS relácie, poslanie správy, prihlásenie k udalosti, zverejnenie informácie o prístupnosti) a je schopná rozhodnúť, kedy musí kontaktovať CDF, centrálny bod v offline účtovacom systéme. Keď je splnená požiadavka spustenia, CFT zhromaždí účtovacie informácie zo signalizačnej správy a pošle informácie o offline účtovaní CDF pomocou Priemerových *účtovných požiadaviek* (*Accounting Requests* - ACRs) cez Rf rozhranie. Požiadavka obsahuje veľa informácií o udalosti, ktorá spustila spúšťací mechanizmus (napr. typ požiadavky INVITE/MESSAGE/SUBSCRIBE, adresu volajúcej strany, adresu volanej strany, časové razítka). CDF používa Priemerovú *účtovnú odpoveď* (*Accounting Answer* - ACA) pre potvrdenie prijatej požiadavky. V prípade IMS relácie sä poslané aspoň dva páry ACR/ACA (na začiatku relácie a na konci relácie). Môže(u) byť použitý(é) aj ďalší(e) ACR(s), ak boli zmenené vlastnosti relácie (napr. pridané alebo odobrané mediálne komponenty, kodeky mediálneho komponentu a šírka pásma sa zmenili, relácia je zastavená). V prípade jediného koncového užívateľa sieťovej transakcie (napr. poslanie okamžitej správy), stačí jeden ACR/ACA. Použitie Priemerových požiadaviek je bližšie popísané v Časti 3.11.5.1 (referenčný bod Rf).

Doteraz sme popísali, akým spôsobom sú účtovacie informácie dodané z IMS entity funkcii CDF. Na obrázku 3.12 môžeme vidieť, že nasledujú ďalšie kroky predtým, ako fakturačný systém môže poslať užívateľovi faktúru. Ďalším krokom je presun CDRs z CDF smerom k CGF. CGF je potrebná, keďže v jednej relačnej/nerelačnej udalosti môžu byť zahrnuté viaceré CDFs, pretože rôzne IMS entity môžu poslať účtovacie informácie rôznym CDFs (napr. z dôvodu roamingu alebo konfigurácie). CGF potvrdí, konsoliduje, predbežne spracuje prichádzajúci CDR (napr. filtruje nepotrebné polia

a pridá informácie špecifické pre užívateľa) a môže korelovať rôzne CDR pred ich postúpením do fakturačného systému. Tabuľka 3.11 uvádza prehľad kľúčových procedúr podporovaných rôznymi funkciami offline účtovania.

Tabuľka 3.11 Prehľad funkcií offline účtovania

Funkcia offline účtovania	Kľúčové procedúry
Funkcia spustenia účtovania (Charging Triggering Function – CTF)	Monitoruje SIP signalizáciu. Zisťuje podmienku spustenia Získava informácie z SIP signalizácie a zhromažďuje účtovacie informácie Posiela účtovacie informácie CDF
Funkcia účtovacích údajov (Charging Data Function - CDF)	Vytvára CDRs Dodáva CDRs funkcii CGF
Funkcia účtovacej brány (Charging Gateway Function – CGF)	Koreluje, konsoliduje, filtruje nepotrebné polia a pridáva informácie špecifické pre užívateľa do prijatých účtovných informácií Riadenie chýb CDR a ukladanie Dodáva CDRs do fakturačného systému Predbežne spracováva CDRs.
Fakturačný systém	Vytvára skutočnú faktúru



Obrázok 3.13 Príklad offline účtovania.

Billing system – Fakturačný sytém

7. GTP Data Record Transfer – 7. Prenos záznamu údajov GTP

4. DIAMETER ACR[Event]ACA – PRIEMER ACR[Udalosť]ACA

1. SIP SUBSCRIBE - SIP prihlásenie

Na Obrázku 3.13 je uvedený príklad offline účtovania. V tomto príklade užívateľ pošle požiadavku na prihlásenie serveru AS. Predpokladá sa, že S-CSCF a AS používajú rovnakú CDF (CDF #2 na obrázku) a P-CSCF používa inú CDF (CDF #1 na obrázku). Požiadavka na prihlásenie by mohla byť napríklad požiadavka na odhalenie, kto sú členovia konkrétnej skupiny Push to talk cez mobilný telefón. V krokoch 1-3 požiadavka SUBSCRIBE prechádza od UE k AS. V krokoch 4-6 funkcie CTF vnútri IMS entít zistia účtovateľnú udalosť, vytvoria ACR a pošlú ho funkcii CDF. V krokoch 7-8 CDFs pošlú príslušné CDRs od CDF k CGF, ktorá potom dodá CDR(s) do fakturačného systému. CDRs sú prenesené od CDF k CGF pomocou požiadavky na prenos záznamu údajov v GPRS tunelovacom protokole, ktorý zahŕňa funkcie pre účtovanie (GTP´) [3GPP TS 32.295]. Všimnite si, že CDF #2 môže vytvoriť jediný CDR z prijatých účtovacích informácií. Okrem toho CGF môže skonsolidovať prijaté CDRs a poslať jediný CDR do fakturačného systému.

Hoci sa v tomto príklade predpokladalo, že sa používajú viaceré CDFs, môže byť pre všetky IMS entity zahrnuté v SIP relácii alebo transakcii distribuovaná jediná adresa CDF. To umožní poslanie účtovacích informácií jedinej CDF.

3.10.3 Online účtovanie

Cieľom online účtovania je vykonať kontrolu kreditu pred použitím IMS služieb/zdrojov. Existujú dva rôzne modely: priame zaúčtovanie a rezervácia jednotiek. Pri priamom zaúčtovaní sieťová entita IMS kontaktuje OCS a vyžiada si povolenie pre umožnenie použitia služieb/zdrojov. OCS použije vnútornú vyhodnocovaciu funkciu pre nájdenie vhodného tarifu pre udalosť na základe prijatých informácií, ak nebola cena zadaná v požiadavke. Po vyriešení tarifu a ceny OCS skontroluje, či má užívateľ dostatočný kredit na jeho účte. Ak je kredit dostatočný, OCS odpočíta príslušnú peňažnú čiastku z účtu užívateľa a vyhovie požiadavke IMS entity. V modeli rezervácie jednotiek OCS príjme požiadavku na kontrolu kreditu od IMS entity a použije vnútornú vyhodnocovaciu funkciu pre stanovenie ceny požadovanej služby podľa informácií o službe poskytnutých entitou IMS, ak cena nebola zadaná v požiadavke. Potom OCS rezervuje príslušnú peňažnú čiastku na účte užívateľa a vráti zodpovedajúci počet zdrojov IMS entite, ktorá zadala požiadavku. Počet zdrojov by mohol zahŕňať napríklad čas alebo povolený objem údajov. Keď sú zdroje poskytnuté užívateľovi spotrebované alebo služba bola úspešne dodaná alebo ukončená, IMS entita informuje OCS o počte

spotrebovaných zdrojov. Nakoniec OCS odpočíta použité množstvo z účtu užívateľa. OCS môže tiež prijímať ďalšie požiadavky od IMS entity počas výkonu služby, ak boli všetky poskytnuté zdroje spotrebované. V tomto prípade OCS musí uskutočniť novú autorizáciu kreditu.

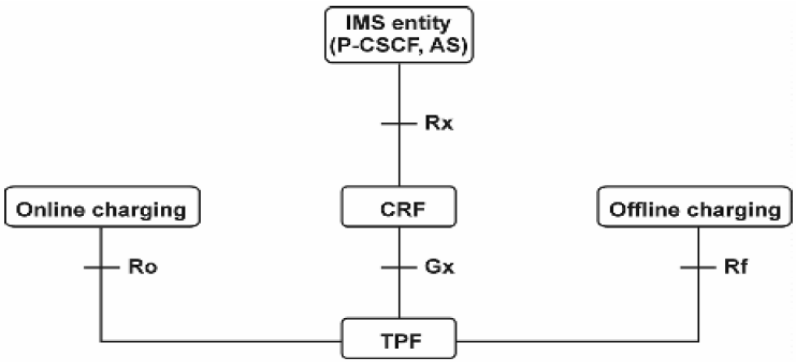
Model priameho zaúčtovania je vhodný, keď IMS entita vie, že by sama mohla dodať požadovanú službu užívateľovi. Napríklad herný AS môže poslať požiadavku na kontrolu kreditu a informovať OCS o službe a počte položiek, ktoré majú byť dodané. Potom OCS použije vyhodnocovaciu funkciu na vyriešenie tarifu a výpočet ceny na základe počtu dodaných jednotiek. Nakoniec je odpočítané z účtu užívateľa a OCS informuje AS, že boli poskytnuté jednotky v rámci odpovede na kontrolu kreditu.

Rezervovanie jednotiek je vhodné, keď IMS entita nie je schopná dopredu určiť, či môže byť služba dodaná alebo keď požadovaný počet zdrojov nie je známy pred použitím konkrétnej služby (napr. doba trvania multimediálnej relácie). Model rezervácie jednotiek sa väčšinou používa pre relácie, ale môže byť použitý aj pre nerelačné požiadavky.

3.10.4 Účtovanie založené na tokoch

Súčasné štandardizované účtovacie riešenia umožňujú účtovanie v užívateľskej rovine na úrovni APN a PDP. 3GPP Release 6 a Release 7 predstavia schopnosť účtovania detailnejším spôsobom. Model účtovania založený na tokoch zavádza schopnosť účtovať toky servisných údajov identifikovaných podľa filtrov servisných tokov na základe stanovených účtovacích pravidiel. Účtovacie pravidlá obsahujú informácie, ktoré umožňujú filtrovať prevádzku pre identifikáciu paketov patriacich konkrétnemu toku servisných údajov a umožňujú definovať akým spôsobom bude tok servisných údajov účtovaný. Účtovacie pravidlá sú bežne vyžiadané funkciou roviny prevádzky (Traffic Plane Function - TPF) pri vytvorení nosiča, pri špecifickej spúšťacej udalosti a pri ukončení nosiča. Táto požiadavka je uskutočnená použitím Gx referenčného bodu smerom k funkcii účtovacieho pravidla (Charging Rule Function - CRF). CRF je ďalej spojená s aplikačnou funkciou prostredníctvom Rx referenčného bodu (v prípade IMS je to väčšinou P-CSCF alebo AS). Rx referenčný bod umožňuje prenos informácií (napr. informácií dynamického mediálneho prúdu) z aplikačnej funkcie do CRF. Príkladom takejto informácie môže byť filtrovacia informácia učená pre identifikovanie

IMS relácie a jej parametrov pripojenia (napr. koncové body, popis média). Architektúra je znázornená na obrázku 3.14.
V súčasnosti sa v Release 7 pracuje na harmonizácii a zlúčení kontroly politiky (SBLP) a architektúry a postupov účtovania na báze tokov.



Obrázok 3.14 Architektúra účtovania založeného na tokoch

IMS entity (P-CSCF, AS) - IMS entita (P-CSCF, AS)
Online charging - Online účtovanie
Offline charging - Offline účtovanie

3.10.5 Účtovacie referenčné body

Pre účely účtovania existujú tri s IMS súvisiace referenčné body, Ro (online účtovanie), Rf (offline účtovanie) a Rx. Všetky referenčné body sú založené na Priemerovom protokole vyvinutom Operačnou skupinou internetového inžinierstva (Internet Engineering Task Force - IETF).

Referenčný bod Rf (offline účtovanie)

Na začiatku tejto kapitoly je vysvetlilené, že CTF v IMS entite má za úlohu zistiť, kedy je nevyhnutné nahlásiť účtovateľnú udalosť do CDF (účtovací systém vo všeobecnosti). Táto kritická úloha sa dosahuje zaslaním Priemerového ACR prostredníctvom Rf referenčného bodu do CDF. CDF odpovedá použitím ďalšieho Priemerového príkazu - účtovacou odpoveďou (Accounting Answer - ACA).

Základná funkčnosť Priemeru je popísaná v [RFC3588] a utvára základ Rf referenčného bodu. Okrem základného Priemerového protokolu 3GPP definovala aj sadu

vlastných rozšírení vo forme 3GPP AVP Priemerového účtovania, aby splnila účtovacie požiadavky 3GPP. AVP špecifické pre 3GPP obsahuje informácie považované za užitočné hlavne v 3GPP prostredí, nie nutne v celom Internete. Zahŕňa napríklad popisy médií v relácii (audio, video, správy, chat), autorizovanú kvalitu služby (QoS), zapojené ASs. ACR používané v 3GPP obsahuje vhodné AVP Priemerového protokolu a AVP 3GPP Priemerového účtovania. Použitie AVP je špecifikované pre každú IMS entitu a ACR typ: ACR vytvorené pomocou S-CSCF môže napríklad obsahovať informácie o kontaktovaných AS, kým ACR vytvorené pomocou P-CSCF môže obsahovať autorizované informácie o kvalite služby (QoS) [3GPP TS 32.299].

Offline účtovací systém musí podporovať účtovanie na báze relácií ako aj účtovanie na báze udalostí. IMS entity poznajú typ požiadavky, ktorá má byť určená pre CDF. To sa dosahuje použitím vhodnej hodnoty v AVP typu účtovacieho záznamu v ACR ("event" (udalosť) pre udalosti a "start" (štart), "interim" (medzifáza), "stop" pre relácie). ACR súvisiace s IMS reláciou sa nazývajú štart, medzifáza a stop a posielajú sa na začiatku, v strede a na konci relácie, ako to vyplýva z ich názvu. Nerelačné ACR sa nazývajú ACR udalostí. ACR udalostí spôsobujú, že CDF vygeneruje odpovedajúce CDR, zatiaľ čo ACR relácií spôsobujú, že CDF otvorí, aktualizuje a zatvorí zodpovedajúce CDRs. Nasledujúca časť bude venovaná dvom príkladom použitia Rf referenčného bodu, IMS relácie a okamžitej správy (nevzťahujúcej sa k relácii), aby sme vysvetlili použitie Priemerového ACR.

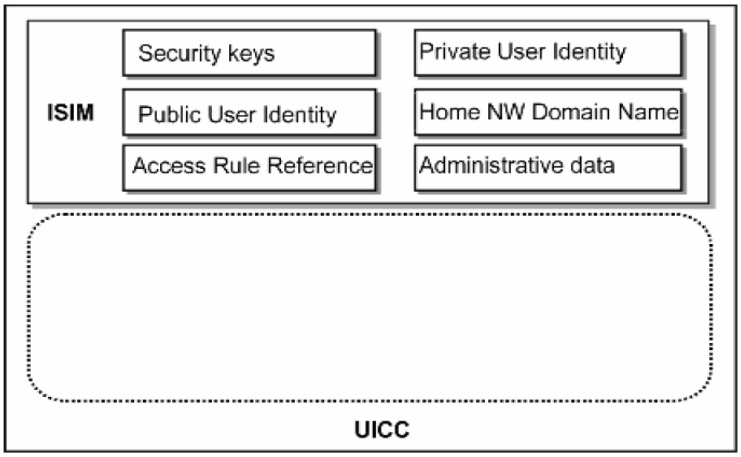
V IMS relácii môžeme rozlíšiť tri rôzne fázy (zahájenie relácie, zmena relácie a uvoľnenie relácie). Na začiatku relácie (prijatie 200 OK, potvrdenia INVITE), CTF vnútri IMS entity monitoruje signalizačnú prevádzku a detekuje spúšťací bod definovaný za účelom prijatia 200 OK, potvrdenia INVITE. Po kontakte so spúšťacím bodom CDF zhromaždí informácie zo signalizačnej správy (napr. adresu volajúcej strany, adresu volanej strany, časové razítka, mediálny komponent "audio" SDP), zostaví účtovaciu informáciu, ktorá zodpovedá zistenej účtovateľnej udalosti a prepošle účtovaciu informáciu smerom k CDF cez Rf referenčný bod pomocou ACR[Start] požiadavky. Použitie ACR[Start] vyzve CDF na otvorenie CDR pre túto reláciu. Keď sa táto relácia zmení (prijme sa RE-INVITE alebo UPDATE) - napr. keď je pridaný video komponent - CTF môže opäť vyvolať túto udalosť a získať potrebné informácie (napr. adresu volajúcej strany, adresu volanej strany, časové razítka, mediálny komponent "audio + video" SDP). Tieto zmenené účtovacie informácie sú opäť poslané do CDF, ale tento krát sa použije požiadavka ACR[Interim]. Konečne, keď relácia skončí (prijme sa BYE), CTF vytvorí

požiadavku ACR[Stop] na indikáciu ukončenia relácie. Na základe týchto troch účtovacích udalostí dokáže CDF vytvoriť jediné CDR obsahujúce celkový čas relácie, čas audio relácie a čas video relácie.

Po prijatí nerelačnej požiadavky (v tomto prípade MESSAGE) môže byť spúšťací bod opäť dosiahnutý. CTF zhromaždí z požiadavky potrebné informácie (napr. adresu volajúcej strany, adresu volanej strany, časové razítka, veľkosť obsahu) a tento krát vytvorí požiadavku ACR[Event] za účelom indikácie účtovania na báze udalostí. Výsledkom tohto ACR[Event] je, že CDF rozpozná nutnosť aplikácie účtovania na báze udalostí, okamžite vygeneruje CDR a postúpi ju CGF.

Operátor sa rozhodne, ktorá správa SIP metódy, užívateľskej zložky ISDN (ISDN User Part - ISUP) alebo kontroly volania nezávislej od nosiča (Bearer Independent Call Control - BICC) spustí posielanie ACR. Boli však definované dve povinné položky:

- Pri každom prijatí SIP 200 OK, potvrdení počiatočného SIP INVITE alebo keď MGCF príjme ISUP/BICC odpoveď, pošle sa ACR[Start] do CDF.
- Pri každom prijatí SIP BYE alebo keď riadiaca funkcia mediálnej brány (Media Gateway Control Function - MGCF) príjme uvoľnenie ISUP/BICC, pošle sa ACR[Stop] do CDF.



Obrázok 3.15 Príklad offline účtovania založeného na reláciách a na udalostiach

Session starts - Začiatok relácie

Session modification – Zmena relácie

Referenčný bod Ro (online účtovanie)

Pre vykonanie online účtovania OCS musí získať potrebné informácie z dotazovacej IMS entity. Pre tento účel bol definovaný Ro referenčný bod. Prenáša požiadavky a odpovede kontroly kreditu medzi OCS a tromi rôznymi IMS entitami, ktoré sú schopné vykonávať online účtovanie (AS, MRFC a S-CSCF skrz IMS-GWF). Za týmto účelom sa používajú *požiadavky na kontrolu kreditu a odpovede na kontrolu kreditu*. 3GPP okrem toho definovala 3GPP AVP páry kontroly kreditu za účelom zlepšenia riešenia IETF, pre splnenie požiadaviek na účtovanie 3GPP [3GPP TS 32.299].

Pre umožnenie priameho zaúčtovania IMS entita posiela požiadavku na kontrolu kreditu do OCS a používa hodnotu "EVENT_REQUEST" v AVP typu požiadavky na kontrolu kreditu a hodnotu "DIRECT_DEBITING" v AVP požadovanej akcie. AS umožňujúci posielanie správ môže napríklad prijať od užívateľa požiadavku, aby niekomu zaslal okamžitú správu (1). Server pre posielanie správ vie, že užívateľ je predplatiteľ a musí preto vyžiadať povolenie z OCS. Vytvorí *požiadavku na kontrolu kreditu*, nastaví správne *AVP typu požiadavky na kontrolu kreditu*, *AVP požadovanej akcie* a ďalšie požadované AVP a potom pošle požiadavku do OCS (2). OCS požiadavku príjme a ak táto neobsahuje informáciu o cene služby, OCS pred nahliadnutím na účet užívateľa použije vyhodnocovaciu funkciu. Tento príklad je zobrazený na Obrázku 3.15. Ak má užívateľ na účte dostatočný kredit, OCS vyhovie požiadavke pomocou *odpovede na kontrolu kreditu* (3). Server pre posielanie správ následne umožní realizáciu služby a pošle okamžitú správu smerom k cieľu (4). Tento príklad je zobrazený v ľavej hornej časti obrázku 3.16.

Pre umožnenie účtovania relácie prostredníctvom rezervácie jednotiek IMS entita pošle *požiadavku na kontrolu kreditu* do OCS a potom použije hodnoty "INITIAL_REQUEST", "UPDATE_REQUEST" a "TERMINATION_REQUEST" v *AVP typu požiadavky na kontrolu kreditu* nasledovným spôsobom:

- Hodnota "INITIAL_REQUEST" sa používa, keď IMS entita prijme prvú požiadavku na dodanie služby.
- Hodnota "UPDATE_REQUEST" sa používa, keď požiadavka IMS entity nahlási počet použitých jednotiek a stanoví požiadavku na ďalšie jednotky

- Hodnota “TERMINATION_REQUEST” sa používa, keď IMS entita hlási, že dodanie obsahu alebo služby bolo ukončené, alebo keď sa spotrebovali koncové pridelené jednotky.

Pre umožnenie účtovania udalostí prostredníctvom rezervácie jednotiek IMS entita pošle *požiadavku na kontrolu kreditu* do OCS a potom použije hodnoty “INITIAL_REQUEST” a “TERMINATION_REQUEST” v *AVP typu požiadavky na kontrolu kreditu* nasledovným spôsobom:

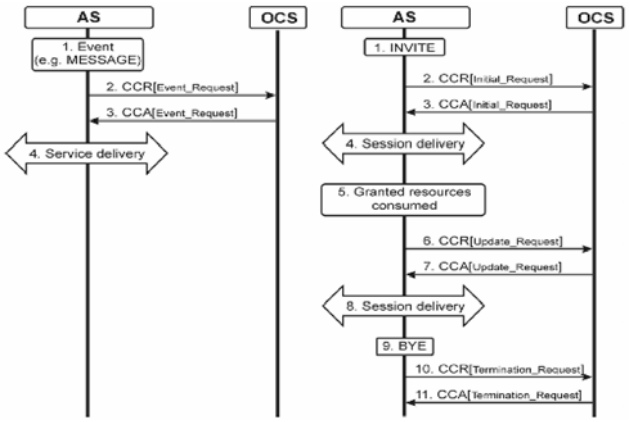
- Hodnota “INITIAL_REQUEST” sa používa, keď IMS entita prijme prvú požiadavku na dodanie služby.
- Hodnota “TERMINATION_REQUEST” sa používa, keď IMS entita hlási, že dodanie obsahu alebo služby bolo ukončené.

Napríklad operátor, ktorý svojim zákazníkom ponúka predplatené služby a chce aplikovať online účtovanie, musí smerovať celú signalizačnú prevádzku cez AS alebo IMS-GWF. V nasledujúcom príklade budeme predpokladať prístup založený na AS. V kroku (1) na obrázku 3.16 AS prijme požiadavku SIP relácie (INVITE). Vzhľadom na to, že toto je prvá požiadavka v tejto relácii, SIP INVITE spustí *požiadavku na kontrolu kreditu* zároveň s hodnotou “INITIAL_REQUEST” v *AVP typu požiadavky na kontrolu kreditu*. OCS príjme požiadavku (2) a na základe poskytnutých informácií sa rozhodne, či tejto požiadavke vyhovie alebo nevyhovie. *Odpoveď na kontrolu kreditu* (3) obsahuje počet poskytnutých jednotiek služby a na základe toho môže AS umožniť pokračovanie SIP (4). Keď je počet poskytnutých jednotiek vyčerpaný, alebo vznikla potreba pridelenia dodatočných jednotiek (napr. z dôvodu pridania mediálneho komponentu), AS pošle novú *požiadavku na kontrolu kreditu* ale tento krát je hodnota v *AVP typu požiadavky na kontrolu kreditu* odlišná (6). OCS opäť prijme rozhodnutie o kontrole kreditu a oznámi ho, na základe čoho môže SIP relácia pokračovať (7, 8). Keď je relácia ukončená, alebo sa spotrebujú všetky jednotky, AS pošle tretiu *požiadavku na kontrolu kreditu*, ktorou stanoví ukončenie relácie a použije príslušné hodnotu v *AVP typu požiadavky na kontrolu kreditu*. Tento príklad je zobrazený v pravej časti obrázku 3.16.

Rx referenčný bod

Keď sa v sieti používa účtovanie na báze tokov, IMS entity (v praxi P-CSCF a AS) pomáhajú CRF prenosom mediálnych informácií IMS relácie do CRF. CRF používa poskytnuté informácie na generovanie dynamických účtovacích pravidiel, ktoré sa odosielajú do prístupovej siete (TPF). Na Rx referenčnom bode existujú štyri rôzne procedúry: prenos informácií z IMS entít do CRF, požiadavka na informácie iniciovaná CRF, oznámenie uvoľnenia IMS relácie a oznámenie uvoľnenia nosiča.

Tabuľka 3.12 ukazuje, ktoré Priemerové požiadavky sa používajú v každej z procedúr. Odporúčame čitateľovi porovnať túto tabuľku s tabuľkou Gq príkazov (používané príkazy sú úplne rovnaké).



Obrázok 3.16 Príklad online účtovania založeného na reláciách a na udalostiach

1. Event (MESSAGE) – Udalosť (napr. SPRÁVA)
2. CCR(Event_Request) – CCR(Požiadavka na udalosť)
4. Service delivery – Dodanie služby
1. INVITE – POZVÁNKA
2. CCR(Initial_Request) – CCR(Počiatočná požiadavka)
4. Session delivery – Dodanie relácie
5. Granted resources consumed – Poskytnuté zdroje boli spotrebované
6. CCR(Update_request) – CCR(Požiadavka na aktualizáciu)
8. Session delivery – Dodanie relácie
9. BYE – POZDRAV
10. CCR(Termination_request) – CCR(Požiadavka na ukončenie)

3.10.6 Korelácia účtovacích informácií

Vzhľadom na to, že dizajn je založený na vrstvách, IMS entity nemajú prehľad o objemoch prevádzky na užívateľskej rovine súvisiacich s reláciami IMS a sieťové entity s IP konektivitou (napr. SGSN a GGSN) nemajú prehľad o stave signalizácie riadiacej roviny (napr. o stave IMS relácií). Z pohľadu operátora je vhodné mať možnosť korelovať účtovacie informácie vytvorené na užívateľskej rovine a riadiacej rovine. Zámena účtovacích identifikátorov – Účtovací identifikátor IMS (ICID) a Účtovací identifikátor GPRS (GCID) – prostredníctvom Go referenčného bodu umožňuje koreláciu účtovania medzi IMS a GPRS sieťami.
Počas fázy vytvárania relácie UE aktivuje potrebný sekundárny PDP kontext(y). Počas procesu autorizácie PDP kontextu sa u GGSN a PDF zamenia účtovacie identifikátory nasledovným spôsobom:

1. PDF predá identifikátor ICID entite GGSN v autorizačnom rozhodnutí.
2. GGSN predá identifikátor GCID funkcii PDF v hlásení o autorizačnom rozhodnutí.

PDF taktiež postúpi GCID funkcii P-CSCF, ktorá prepošle GCID IMS entitám vo svojej vlastnej sieti, kde sa GCID zahrnie do požiadaviek IMS CDR. GGSN zahrnie ICID vo svojej G-CDR (napr. záznam o účtovacích údajoch GGSN), ale nepostúpi ICID entite SGSN. V prípade, že samostatná IMS relácia vyžaduje niekoľko sekundárnych PDP kontextov, dôjde k namapovaniu jedného, alebo aj viacerých GCID identifikátorov na jeden ICID. GGSN tiež zodpovedá za aktualizáciu GCID informácií na úrovni IMS, keď dôjde k odstráneniu alebo pridaniu sekundárneho PDP kontextu alebo mediálnych tokov počas relácie. Ako posledný článok vytvorí SGSN S-CDR (napr. záznam o účtovacích údajoch SGSN), ktorý obsahuje adresy GCID a GGSN.

Vznikne takto unikátny identifikátor pre každý PDP kontext. Obrázok 3.17 zobrazuje príklad IMS relácie, ktorá obsahuje dva mediálne komponenty prenášané v samostatných PDP kontextoch.
Na uvedenom príklade môžeme vidieť, že 3GPP IMS architektúra definuje ICID a GCID za účelom korelácie účtovaných údajov a mechanizmus pre zámenu týchto identifikátorov medzi IMS a PS doménou.

Tabuľka 3.12 Rx príkazy

Názov príkazu	Účel	Skratka	Zdroj	Cieľ
AA požiadavka	Keď sa vytvára nová SIP relácia a v P-CSCF sú k dispozícii mediálne informácie o tejto relácii, alebo keď je relácia zmenená, P-CSCF pošle zodpovedajúce informácie o službe (napr. mediálne informácie) do CRF prostredníctvom zaslania správy AA požiadavky.	AAR	P-CSCF	CRF
AA odpoveď	AA odpoveď dodá potvrdenie na AAR.	AAA	CRF	P-CSCF
Požiadavka na opätovnú autorizáciu	Požiadavka na opätovnú autorizáciu dodá hlásenie (pri uvoľnení niektorých komponent relácie) a môže obsahovať požiadavku na odoslanie informácií o SIP relácii.	RAR	CRF	P-CSCF
Odpoveď na opätovnú autorizáciu	Tento príkaz sa používa na potvrdenie príkazu STR.	RAA	P-CSCF	CRF
Požiadavka na ukončenie relácie	Tento príkaz oznamuje uvoľnenie SIP relácie.	STR	P-CSCF	PDF
Odpoveď na ukončenie relácie	Tento príkaz sa používa na potvrdenie príkazu STR.	STA	PDF	P-CSCF
Požiadavka na prerušenie relácie	Tento príkaz informuje P-CSCF, že všetky nosiče vzťahujúce sa k špecifickej SIP relácii boli uvoľnené.	ASR	PDF	P-CSCF
Odpoveď na prerušenie relácie	Tento príkaz sa používa na potvrdenie príkazu ASR.	ASR	P-CSCF	PDF

3.10.7 Rozdelenie účtovacích informácií

Bolo vysvetlené, ako sú účtovacie informácie korelované. Táto časť poskytuje prehľad o spôsobe rozdelenia účtovacích informácií medzi rôznymi entitami IMS.

Prvá IMS entita na SIP signalizačnej ceste vytvorí ICID. Tento ICID je postúpený signalizačnou cestou všetkým zapojeným entitám, okrem UE: to znamená, že P-CSCF v ukončovacej sieti odstráni ICID. ICID sa používa pre koreláciu účtovacích údajov

medzi IMS komponentmi. ICID je platný po dobu trvania udalosti, s ktorou je spojený: napríklad ICID priradený pre vytvorenie relácie je platný do ukončenia relácie, atď. Na Obrázku 3.18 môžeme vidieť, že účtovacie identifikátory IMS a GRPS sú vymenené po autorizácii nosiča. Okrem toho Obrázok 3.18 znázorňuje, kedy sú účtovacie požiadavky poslané CDF. Adresa CDF je rozdelená počas registrácie, alebo je nakonfigurovaná v IMS entitách.

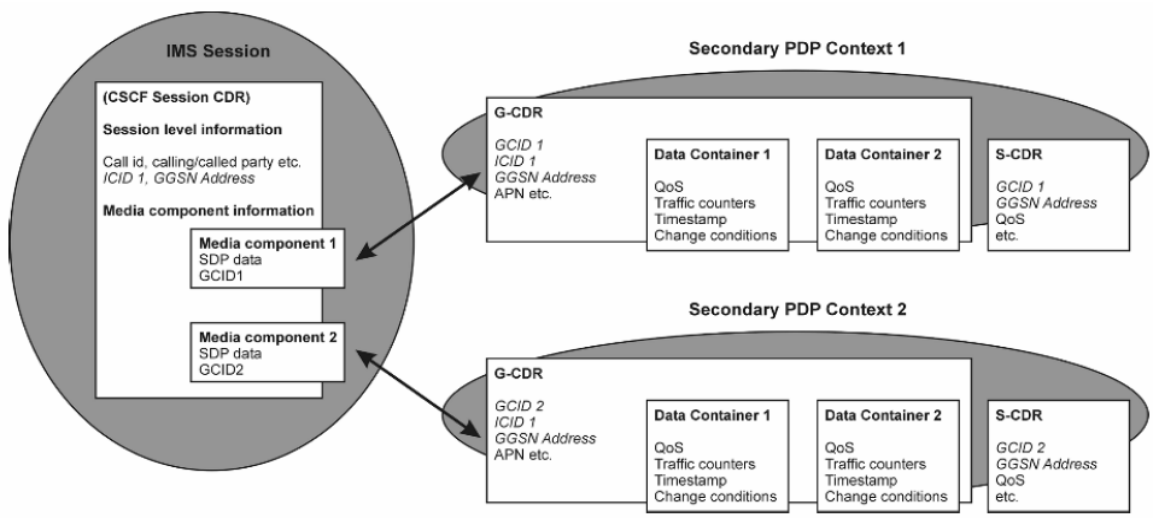
3.11 Užívateľský profil

Keď užívateľ získa IMS prihlásenie od operátora, operátor musí prideliť užívateľský profil. Užívateľský profil obsahuje aspoň jednu verejnú užívateľskú identitu a jeden profil služby. Obrázok 3.19 znázorňuje všeobecnú štruktúru užívateľského profilu. Súkromná užívateľská identita bola popísaná v Časti 3.4.1, ale malo by byť jasné, že užívateľský profil môže obsahovať viac ako jednu súkromnú užívateľskú identitu, ak užívateľ používa zdieľanú verejnú užívateľskú identitu. Obrázok 3.4 ukazuje, že jedno IMS prihlásenie môže obsahovať viaceré profily služieb; to umožňuje rôzne spracovanie pre rôzne verejné užívateľské identity.

3.11.1 Profil služby

Profil služby je súbor informácií špecifických pre užívateľa, ktoré sú trvalo uložené v HSS. Sú prenesené z HSS do pridelenej S-CSCF prostredníctvom dvoch operácií pre riadenie užívateľských údajov – odpoveď na pridelenie servera (Server-Assignment-Answer – SAA) a požiadavka na pretlačenie profilu (Push-Profile-Request – PPR). Profil služby je prenášaný v jednom Priemerovom AVP, kde je zahrnutý ako dokument rozšíriteľného značkovacieho jazyka (Extensible Markup Language – XML). Profil služby sa ďalej delí na tri časti:

- Verejná identifikácia;
- Autorizácia služby základnej siete;
- Počiatočné filtračné kritériá.



Obrázok 3.17 Účtovacia korelácia IMS.

Secondary PDP Context 1 – Sekundárny PDP kontext 1

Data Container 1 – Kontajner údajov 1

Traffic counters – Počítadlo prevádzky

Timestamp – Časové razítko

Change conditions—Podmienky zmeny

(CSCF Session CDR) – CDR relácie CSCF

Session level information – Informácie o úrovni služby

Call id. calling/called party etc. – Id. volania, volajúca/volaná strana, atď.

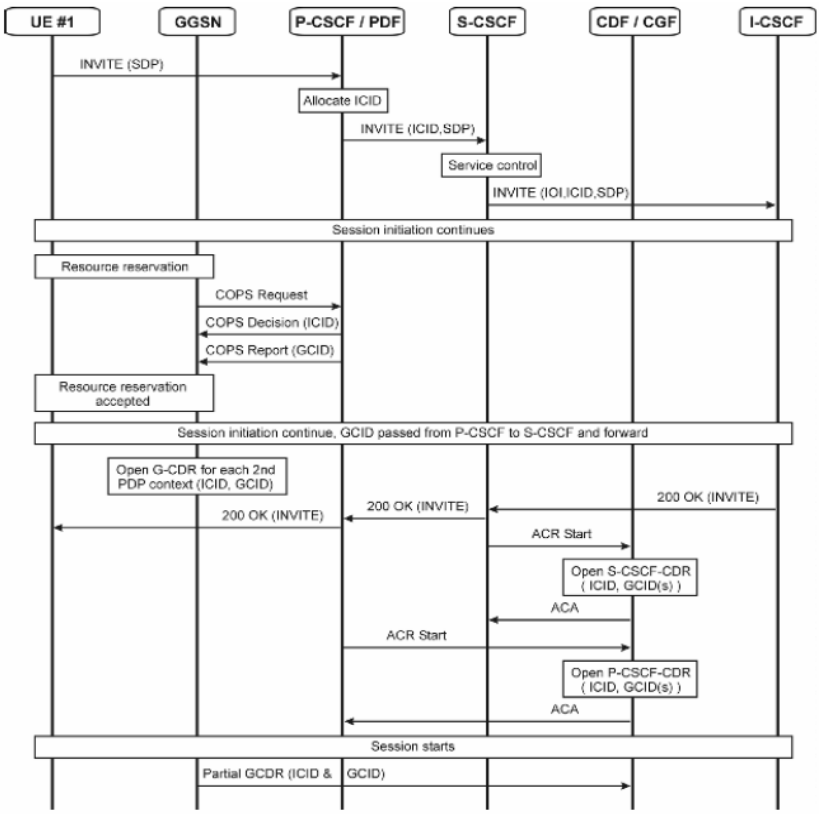
ICID 1, GGSN Address – ICID 1, Adresa GGSN

Media component information – Informácie o mediálnom komponente

Media component 1 – Mediálny komponent 1

SDP data – SDP údaje

Media component 2 – Mediálny komponent 2



Obrázok 3.18 Rozdelenie účtovacích informácií.

Allocate ICID – Prideliť ICID

Service control – Kontrola služby

Session initiation continues – Iniciácia relácie pokračuje

Resource reservation – Rezervácia zdroja

COPS Request – Požiadavka COPS

COPS Decision (ICID) – Rozhodnutie COPS (ICID)

COPS Report (GCID) – Správa COPS (GCID)

Resource reservation accepted – Rezervácia zdroja prijatá

Session initiation continues, GCID passed from P-CSCF to S-CSCF and forward – Iniciácia relácie pokračuje, GCID postúpený z P-CSCF do S-CSCF a ďalej

Open G-CDR for each 2nd PDP context (ICID, GCID) - Otvoriť G-CDR pre každý druhý PDP kontext (ICID, GCID)

Open S-CSCF-CSR (ICID, GCID(s)) – Otvoriť S-CSCF-CSR (ICID, GCID(s))

Session starts – Relácia začne

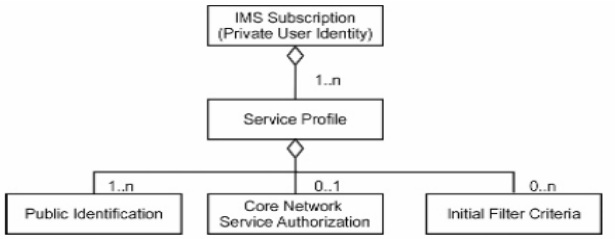
Partial GCDR (ICID & GCID) – Čiastočné GCDR (ICID & GCID)

Verejná identifikácia

Verejná identifikácia zahŕňa tie verejné užívateľské identity, ktoré sú spojené s profilom služby. Identity môžu byť buď SIP URI alebo tel URI. Každá verejná užívateľská identita obsahuje priradenú indikáciu blokovania. Keď je indikácia blokovania nastavená, S-CSCF zabráni použitiu verejnej užívateľskej identity (napr. dočasnej verejnej užívateľskej identity) v akejkoľvek IMS komunikácii inej ako registrácie a zrušenie registrácií.

Informácie o mediálnej politike

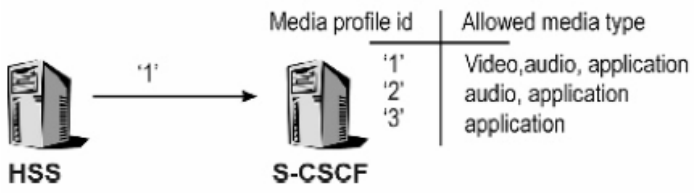
Informácia o mediálnej politiky je prenášaná v autorizácii služby základnej siete. Obsahuje celé číslo, ktoré identifikuje účastnícky mediálny profil v S-CSCF (napr. povolené SPD parametre). Táto informácia umožní operátorom definovať rôzne účastnícke profily v ich IMS sieťach. Môžu definovať rôzne triedy užívateľov, ako zlatá, strieborná a bronzová. Zlatá by mohla znamenať, že užívateľ môže uskutočniť video hovory a všetky bežné hovory. Strieborná by mohla znamenať, že užívateľ môže používať širokopásmovú prispôsobiteľnú viacnásobnú rýchlosť prenosu (Adaptive Multi-Rate – AMR) ako kodek hovoru, ale nemôže uskutočňovať video hovory a iné. Prenos len hodnoty celého čísla medzi HSS a S-CSCF ušetrí miesto v HSS a optimalizuje použitie Cx referenčného bodu.



Obrázok 3.19 Štruktúra užívateľského profilu IMS

IMS Subscription (Private User Identity) – IMS prihlásenie (Súkromná užívateľská identita)
Service Profile – Profil služby
Public Identification – Verejná identifikácia
Core Network Service Authorization – Autorizácia služby základnej siete
Initial Filter Criteria – Počiatočné filtračné kritériá

S-CSCF musí mať statickú databázu, ktorá obsahuje mapovanie medzi hodnotou celého čísla a prihláseným mediálnym profilom. Význam hodnoty celého čísla nie je štandardizovaný (t.j. je špecifický pre operátora). Na obrázku 3.20 je uvedený ilustračný príklad.



Obrázok 3.20 Autorizácia média v S-CSCF.

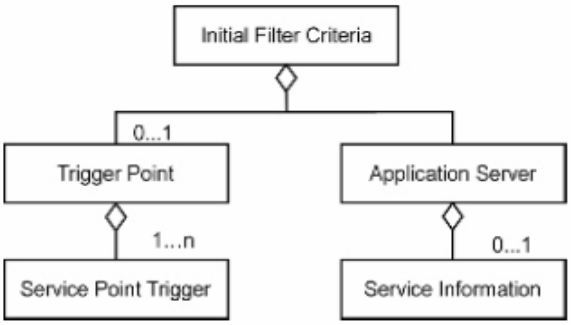
Media profile id – Id mediálneho profilu

Allowed media type – Povolený typ média

Video. audio, application – Video, audio, aplikácia

Informácia spúšťajúca službu

Informácia spúšťajúca službu je predstavená vo forme počiatočných filtračných kritérií. Počiatočné filtračné kritériá popisujú, kedy je prichádzajúca SIP správa presmerovaná ďalej na konkrétny AS. Obrázok 3.21 ukazuje, že počiatočné filtračné kritéria tvorí žiadna alebo jedna inštancia spúšťacieho bodu a jedna inštancia AS. Každé počiatočné filtračné kritérium v rámci profilu služby ma unikátnu hodnotu priority (celé číslo), ktoré sa používa v S-CSCF. Keď sú priradené viaceré počiatočné filtračné kritériá, S-CSCF ich zhodnotí v číselnom podarí: to znamená, že počiatočné filtračné kritérium s číslom s vyššou prioritou bude zhodnotené po kritériu s číslom s menšou prioritou.



Obrázok 3.21 Štruktúra počiatočných filtračných kritérií

Initial Filter Criteria – Počiatočné filtračné kritériá
Trigger Point – Spúšťací bod
Application Server – Aplikačný server
Service Point Trigger – Spúšťací mechanizmus servisného bodu
Service information – Informácie o službe

Spúšťací bod

Spúšťací bod popisuje podmienky, ktoré by mali byť skontrolované pre zistenie, či má byť stanovený AS kontaktovaný. Neprítomnosť spúšťacieho bodu indikuje nepodmienené spustenie pre AS. Každý spúšťací bod obsahuje jednu alebo viacej inštancií spúšťacieho mechanizmu servisného bodu. Spúšťacie mechanizmy servisných bodov môžu byť prepojené prostredníctvom logických výrazov (A, ALEBO, NIE).

Aplikačný server (AS)

Aplikačný server (AS) definuje AS, ktorý je kontaktovaný, ak sú dosiahnuté spúšťacie body. AS môže obsahovať informácie o predvolenom riadení relácie, ak kontakt s AS zlyhá. Predvolené riadenie buď skončí reláciu, alebo nechá reláciu pokračovať, na základe informácií v počiatočných filtračných kritériách. Okrem toho AS obsahuje žiadnu alebo jednu inštanciu informácie o službe. Informácie o službe umožňujú poskytnutie informácií, ktoré majú byť transparentne prenesené cez S-cSCF do AS, ak sú počas registrácie splnené podmienky počiatočných filtračných kritérií.

3.12 Poskytovanie služby

Samotný IMS nie je službou; naopak, je to architektúra založená na SIP, ktorá umožňuje pokročilú IP službu a aplikáciu nad PS sieťou. IMS poskytuje potrebné prostriedky pre vyvolanie služieb; táto funkčnosť sa nazýva "poskytovanie služby". Poskytovanie služby IMS tvoria tri základné kroky:

1. Definovať možnú službu alebo sady služieb.
2. Vytvoriť servisné údaje špecifické pre užívateľa v formáte počiatočných filtračných kritérií, keď užívateľ nariadi/zmení prihlásenie.
3. Postúpiť prichádzajúci počiatočnú požiadavku AS.

3.12.1 Vytvorenie filtračných kritérií

Kedykoľvek užívateľ získa IMS prihlásenie a jeho prihlásenie obsahuje služby s pridanou hodnotou, alebo operátor chce použiť servery AS ako súčasť jeho IMS infraštruktúry, musia vytvoriť údaje špecifické pre službu. Tieto údaje špecifické pre službu sú súčasťou užívateľského profilu užívateľa. Presnejšie, údaje špecifické pre službu sú znázornené ako počiatočné filtračné kritériá. V nasledujúcom texte sa sústredíme len na počiatočné filtračné kritériá. Časť 3.11 popisuje, akým spôsobom sú počiatočné filtračné kritériá zapadajú do profilu užívateľa. Pri vytváraní počiatočných filtračných kritérií musí operátor vziať do úvahy nasledujúce otázky:

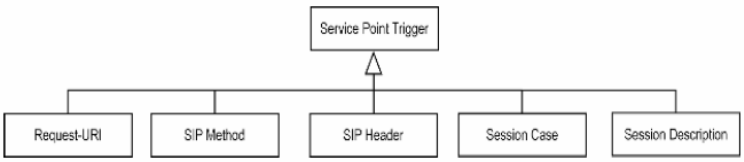
- Čo je to spúšťací bod?
- Ktorý je správny AS pri dosiahnutí spúšťacieho bodu?
- Čo je prioritou počiatočného filtračného kritéria?
- Čo je potrebné urobiť, keď AS neodpovedá?

Spúšťací bod sa používa pre rozhodnutie, či má byť AS kontaktovaný. Obsahuje jednu alebo viac inštancií spúšťacieho mechanizmu servisného bodu. Spúšťací mechanizmus servisného bod zahŕňa položky znázornené na Obrázku 3.22:

- Požiadavka-URI – identifikuje zdroj, ktorému je požiadavka adresovaná (napr. *sportnews@ims.example.com*).
- SIP metóda - určuje typ požiadavky (napr. INVITE alebo MESSAGE).
- SIP hlavička – obsahuje informácie súvisiace s požiadavkou. Spúšťací mechanizmus servisného bodu môže byť založený na prítomnosti alebo neprítomnosti SIP hlavičky alebo obsahu SIP hlavičky. Hodnota obsahu je reťazec, ktorý sa interpretuje ako regulárny výraz. Regulárny výraz môže byť jednoduchý, ako napr. podstatné meno (napr. John) v hlavičke FROM (OD), ktorá určuje pôvodcu požiadavky.
- Prípad relácie – môže mať jednu z troch možných hodnôt, Spúšťajúci, Ukončujúci alebo Ukončujúci_Neregistrovaný, ktoré určujú, či má byť požitý filter funkciou S-CSCF, ktorá riadi spúšťajúcu službu, ukončujúcu službu alebo ukončenie neregistrovanej služby pre koncového užívateľa. Spúšťajúci prípad sa vzťahuje

k prípadu, keď S-SSCF slúži volajúcemu užívateľovi. Ukončujúci prípad sa vzťahuje k prípadu, keď S-CSCF slúži volanému užívateľovi.

- Popis relácie – definuje spúšťací mechanizmus servisného bodu pre obsah akéhokoľvek SPD poľa v tele SIP metódy. Ako vyhovujúce výrazy pre spúšťací mechanizmus môžu byť použité regulárne výrazy.



Obrázok 3.22 Štruktúra spúšťacieho mechanizmu servisného bodu

Service Point Trigger – Spúšťací mechanizmus servisného bodu
Request-URI – Požiadavka-URI
SIP Method – SIP metóda
SIP Header – SIP hlavička
Session Case – Prípad relácie
Session Description – Popis relácie

Vyššie uvedení operátor vytvorí napríklad počiatočné kritéria pre riadenie neregistrovaných užívateľov, ako IMS užívateľ, ktorý neregistroval žiadnu z jeho verejných užívateľských identít. Nasledujúce počiatočné filtračné kritérium smeruje prichádzajúcu reláciu na server hlasovej pošty (*sip:wmail@ims.example.com*|, keď užívateľ nie je registrovaný. Za týmto účelom musí operátor nastaviť SIP metódu tak, aby sa zodpovedala INVITE a prípad relácie tak, aby zodpovedal hodnote Ukončujúci_Neregistrovaný. Ak nie je možné kontaktovať server hlasovej pošty, potom by predvoleným riadením malo byť ukončenie relácie. Počiatočné filtračné kritériá sú kódované v XML, ako je to zobrazené nižšie pre presné kódovacie pravidlá počiatočných filtračných kritérií):

```
Method="INVITE" AND SessionCase="2"
<?xml version="1.0" encoding="UTF-8”?>
<testDatatype xmlns:xsi=”http://www.w3.org/2001/XMLSchcema-instance”
xsi:noNamespaceSchemaLocation=”D:\ CxDataType.xsd”>
        <IMSSubscription>
```

```
            <PrivateID>privatexzyjoe@ims.example.com </Identity>
            <ServiceProfile>
                <PublicIdentity>
                    <Identity>sip: joe.doe@ims.example.com </Identity>
                </PublicIdentity>
                <PublicIdentity>
                    <Identity>tel:+358503334444</Identity>
                </PublicIdentity>
            <InitialFilterCriteria>
                <Priority>0</Priority>
                <TriggerPoint>
                    <ConditionNegated>0</ConditionTypeCNF>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <SessionCase>2</SessionCase>
                    </SPT>
                </TriggerPoint>
                    <ApplicationServer>
                        <ServerName>sip:vmail@ims.example.com
                        </ServerName>
                        <DefaultHandling>1</DefaultHandling/>
                    </ApplicationServer>
                </InitialFilterCriteria>
            </ServiceProfile>
        <IMSSubscription>
</testDatatype>
```

3.12.2 Výber AS

Počiatočné filtračné kritéria sa stiahnuté do S-CSCF pri registrácii užívateľa alebo pri ukončujúcej počiatočnej požiadavke pre neregistrovaného užívateľa. Po stiahnutí profilu užívateľa z HSS S-CSCF zhodnotí filtračné kritéria len pre počiatočnú požiadavku, v súlade s nasledujúcimi krokmi [3GPP TS 24.229]:

1. Skontrolujte, či je verejná užívateľská identita zablokovaná; ak nie, pokračujte ďalej.
2. Skontrolujte, či je táto požiadavka spúšťajúca požiadavka alebo ukončujúca požiadavka.
3. Vyberte počiatočné filtračné kritériá pre prípad relácie (spúšťajúci, ukončujúci alebo ukončujúci pre neregistrovaného koncového užívateľa).
4. Skontrolujte, či táto požiadavka zodpovedá počiatočnému filtračnému kritériu, ktoré má najvyššiu prioritu pre tohto užívateľa, porovnaním profilu služby s verejnou užívateľskou identitou, ktorá bola použitá pre zadanie tejto požiadavky:

- ak sa táto požiadavka zhoduje s počiatočným filtračným kritériom, S-CSCF prepošle túto požiadavku AS, aby skontroloval, či zodpovedá nasledujúcemu filtračnému kritériu s nižšou prioritou a aplikuje filtračné kritérium na SIP metódu prijatú od predtým kontaktovaného AS;
- ak sa táto požiadavka nezhoduje s počiatočným filtračným kritériom s najvyššou prioritou kontrolujte, či sa zhoduje s nasledujúcimi prioritami filtračného kritéria, pokiaľ nebude nájdená zhoda;
- ak už nie sú platné ďalšie (alebo žiadne) počiatočné filtračné kritériá, S-CSCF prepošle túto požiadavku na základe rozhodnutia o smerovaní.

Existuje jeden jasný rozdiel v spôsobe, akým S-CSCF riadi spúšťacie a ukončovacie počiatočné filtračné kritériá. Keď S-CSCF zistí, že AS zmenil Požiadavku-URI v prípade ukončovacieho počiatočného filtračného kritéria, zastaví kontrolu a smeruje požiadavku na základe zmenenej hodnoty Požiadavky-URI. V spúšťajúcom prípade S-CSCF bude ďalej hodnotiť počiatočné filtračné kritériá, kým nebudú zhodnotené všetky.

Ak kontaktovaný AS neodpovedá, S-CSCF sleduje postup predvoleného riadenia spojeného s počiatočnými filtračnými kritériami: to znamená, že buď ukončí reláciu alebo nechá reláciu pokračovať na základe informácií vo filtračných kritériách. Ak počiatočné filtračné kritériá neobsahujú pokyny pre S-CSCF ohľadom zlyhania kontaktu AS, S-CSCF nechá volanie pokračovať s predvoleným správaním [3GPP TS 24.229].

Podľa nášho príkladu počiatočných filtračných kritérií budú prichádzajúce požiadavky INVITE nasmerované na server hlasovej pošty, *vmail@ims.example.com*, keď Joe nie je registrovaný na sieti. Vo výnimočných prípadoch, keď server hlasovej pošty neodpovedá, S-CSCF dostane pokyn na uvoľnenie pokusu o reláciu.

3.12.3 Správanie AS

Časť 3.12.3 popísala, ako je požiadavka nasmerovaná na AS. Po prijatí požiadavky AS iniciuje aktuálnu službu. AS môže vykonať službu pomocou troch rôznych režimov:

- Ukončovací užívateľský zástupca (User Agent - UA) - AS funguje ako UE. Tento režim môže byť použitý pre poskytnutie služby hlasovej pošty.

- Presmerovací server – AS informuje pôvodcu o novom umiestnení užívateľa alebo o alternatívnych službách, ktoré môžu vyhovieť relácii. Tento režim by mohol byť použitý na presmerovanie pôvodcu na konkrétnu web stránku.
- SIP proxy – AS spracuje požiadavku a potom oprávni na požiadavku opäť funkciu S-CSCF. Počas spracovania môže AS pridať, odstrániť alebo zmeniť obsahy hlavičiek obsiahnuté v SIP požiadavke, v súlade s pravidlami pre oprávnenie špecifikovanými v [RFC3261].
- Kontrola volania tretej strany/UA na oboch koncoch - AS generuje novú SIP požiadavku pre iný SIP dialóg, ktorú pošle S-CSCF.

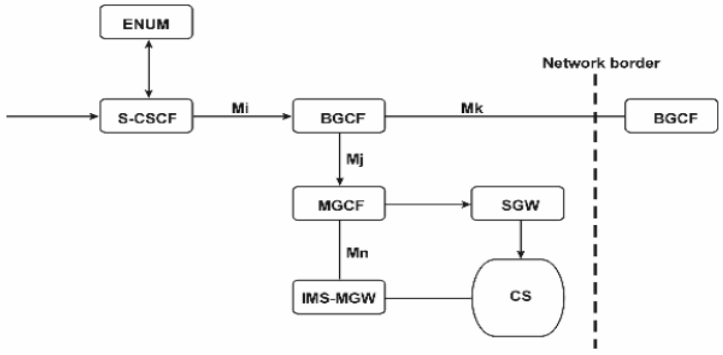
Okrem týchto režimov môže AS fungovať ako spúšťajúci UA. Keď aplikácia funguje ako spúšťajúci UA, je schopná posielať požiadavky užívateľom: napríklad konferenčný server môže poslať požiadavky SIP INVITE vopred definovanému počtu ľudí o 9.00 hod pre nastavenie konferenčného hovoru. Ďalším príkladom môže byť news server , ktorý pošle SIP MESSAGE futbalovému fanúšikovi, aby ho informoval, že jeho obľúbený tím dal gól.

3.13 Konektivita medzi tradičnými CS užívateľmi a IMS užívateľmi

V súčasnosti väčšina užívateľov používa tradičné CS UE: to znamená telefóny s pevnou linkou a rôzne druhy mobilných terminálov. Je teda žiaduce, aby IMS vzájomne komunikoval s CS sieťami nezaloženými na IP protokole (legacy CS networks), pre podporu základných hlasových hovorov medzi IMS užívateľmi a užívateľmi CS sietí. To vyžaduje vzájomnú komunikáciu na užívateľskej rovine a riadiacej rovine, keďže použité protokoly sú pre obidve roviny rôzne. Vzájomnou komunikáciou riadiacej roviny je poverená MGCF. Vykonáva mapovanie z SIP signalizácie na BICC, alebo ISUP použitými v CS sieťach nezaložených na IP protokole, a naopak. Mediálna brána IMS (IMS Media Gateway – IMS-MGW) zas prekladá protokoly na užívateľskej rovine. Ukončuje kanály nosičov zo sietí CS (PSTN/ISDN/GSM), ako aj mediálne prúdy z PS sietí na báze IP alebo ATM a poskytuje preklad medzi týmito ukončeniami. Môžu byť poskytnuté aj prídavné funkcie, ako vzájomná komunikácia kodekov, rušenie ozveny alebo kontrola kontinuity. Ukončenia kontroluje MGCF. Sieťové konfigurácie pre riadenie volaní vytvorených v IMS a volaní vytvorených v CS sú vysvetlené ďalej v texte.

3.13.1 Relácia vytvorená v IMS smerujúca k užívateľovi v CS základnej sieti

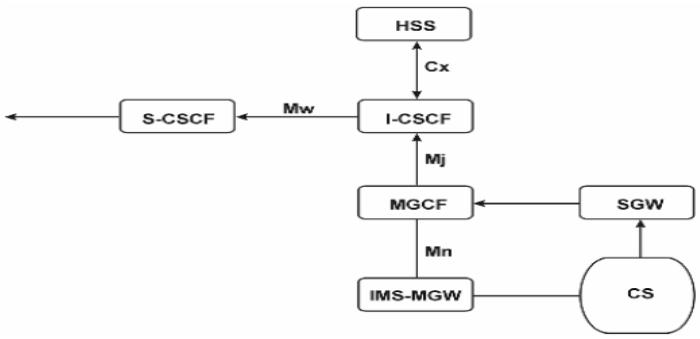
Keď užívateľ iniciuje reláciu, nemusí sa starať o to, či je volaný účastník IMS užívateľ alebo CS užívateľ. Jednoducho zavolá a IMS sa postará o nájdenie volanej strany. Požiadavka na reláciu od volajúceho užívateľa príde vždy funkcii S-CSCF slúžiacej volajúcemu užívateľovi, na základe cesty zistenej počas IMS registrácie. Keď S-CSCF príjme požiadavku na reláciu prostredníctvom tel URL typu užívateľskej identity (*tel:+358501234567*), musí vykonať ENUM dotaz pre konverziu tel URL na SIP URI, keďže princípy IMS nedovoľujú smerovanie s tel URL. Ak je S-CSCF schopná konvertovať identitu do SIP URI formátu, nasmeruje reláciu ďalej do cieľovej IMS siete a ak táto konverzia nie je úspešná, S-CSCF sa pokúsi zastihnúť užívateľa v CS sieti. Pre prepnutie do CS siete S-CSCF smeruje požiadavku na reláciu ďalej k riadiacej funkcii prepínacej brány (Breakout Gateway Control Function - BGCF) v tej istej sieti. Vybraná BGCF má dve možnosti: buď vybrať prepínací bod v tej istej sieti, alebo vybrať inú sieť na prepnutie do CS siete. V prvom prípade BGCF vyberie MGCF v tej istej sieti s cieľom konvertovať SIP signalizáciu na ISUP/BICC signalizáciu a riadiť IMS-MGW. V druhom prípade BGCF vyberie inú BGCF v odlišnej IMS sieti, aby mohla vybrať MGCF v jej vlastnej sieti na riadenie prepnutia. MGCF plní funkciu koncového bodu pre SIP signalizáciu; vyjednáva teda mediálne parametre s IMS US a tiež vyjednáva mediálne parametre spolu s CS entitou (napr. s MSC serverom). Obrázok 3.23 zobrazuje koncept vzájomnej komunikácie, keď je relácia vytvorená v IMS ukončená v CS sieti. Šípky na obrázku ukazujú, akým spôsobom prvá signalizačná správa prechádza od S-CSCF do CS siete.



Obrázok 3.23 Konfigurácia vzájomnej komunikácie IMS-CS, keď IMS užívateľ zavolá CS užívateľovi.

3.13.2 Relácia vytvorená v CS smerujúca k užívateľovi v IMS

Keď užívateľ vytočí číslo E.164, ktoré patrí IMS užívateľovi, bude spracované v CS sieti ako každé iné číslo E.16; po analýze smerovania však bude poslané do MGCF v domácej sieti IMS užívateľa. Po prijatí signalizačnej správy ISUP/BICC MGCF nadviaže vzájomnú komunikáciu s IMS-MQW pre vytvorenie spojenia na užívateľskej rovine, skonvertuje ISUP/BICC signalizáciu na SIP signalizáciu a pošle SIP INVITE funkcii I-CSCF, ktorá nájde S-CSCF pre volaného užívateľa s pomocou HSS. Následne S-CSCF vykoná potrebné kroky pre postúpenie SIP INVITE UE. Potom MGCF pokračuje v komunikácii s EU a CS sieťou pre nastavenie volania. Obrázok 3.24 znázorňuje, akým spôsobom funkcia vzájomne komunikuje, keď je volanie vytvorené v CS sieti ukončené v IMS sieti. Šípky na obrázku ukazujú, akým spôsobom prvá signalizačná správa prechádza od CS k IMS užívateľovi.



Obrázok 3.24 Konfigurácia vzájomnej komunikácie IMS-CS, keď CS užívateľ zavolá IMS užívateľovi.

3.14 Konvergencia pevných a mobilných sietí

Keďže bezdrôtové aj drôtové siete môžu by integrované s použitím IMS architektúry, IMS sa stane lacným médiom pre konvergenciu pevných a mobilných sietí (Fixed to Mobile Convergence - FMC). FMC (tiež známa ako integrácia bezdrôtových/drôtových sietí) je spôsob pripojenia mobilných telefónov k infraštruktúre pevných liniek. To je v súčasnosti jedna z kľúčových strategických otázok v telekomunikačnom priemysle.

Konečným cieľom tejto konvergencie je dosiahnuť bezproblémovú užívateľskú skúsenosť s využitím viacerých umiestnení, zariadení a služieb. Vďaka konvergencia medzi pevnými a mobilnými sieťami môžu telekomunikační operátori poskytnúť užívateľom služby bez ohľadu na ich umiestnenie, prístupovú technológiu alebo typ zariadenia, ktoré používajú.

Na konvergenciu sa môžeme pozerať z troch rôznych uhlov:

- konvergencia služieb;
- konvergencia sietí;
- konvergencia zariadení.

Integrácia bezdrôtových/drôtových sietí vytvára nový vzor telekomunikačných služieb, kde je systém riadený užívateľom, na rozdiel od pôvodného vzoru systému riadeného sieťou alebo zariadením. Táto integrácia tiež prináša užívateľovi najlepšie z obidvoch svetov, pevného aj mobilného tým, že poskytuje užívateľovi služby, ktoré sa vyznačujú dostupnosťou mobilných služieb a spoľahlivosťou a kvalitou pevných služieb.

Výhody operátora

FMC ponúka obchodné príležitosti pre všetky typy operátorov. Zmeny životného štýlu, efektívne cenové modely a personalizácia služieb podnecujú užívateľov, aby zvolili operátorov s FMC riešením.

Spotrebitelia aj obchodníci dnes pokladajú mobilitu za dôležitú vlastnosť. Operátori pevných sietí môže zvýšiť príjmy zvýšením pokrytia služieb, aby zahrnuli služby ponúkané mobilnými operátormi.

Keďže v súčasnosti je mobilný trh takmer úplne nasýtený, pribúdanie nových účastníkov už nepredstavuje ten typ rastu, ktorí mobilný operátori sledujú. Operátori bezdrôtových sietí musia hľadať nové a inovatívne spôsoby zvyšovania využitia ich súčasnej užívateľskej základne. To môžu dosiahnuť ponukou nových služieb pre ich užívateľov. Operátori bezdrôtových sietí môžu poskytnúť svojim účastníkom nový spôsob zastihnutia: jedno číslo, jedno zariadenie, nepretržité pripojenie.

Osobná mobilita

Osobná mobilita poskytuje koncovým užívateľom oveľa väčší výber, pohodlie, produktivitu a úsporu nákladov, ako súčasná mobilita. Umožňuje operátorom a poskytovateľom služieb oživenie ich obchodných činností.

Mnohí užívatelia dnes majú viac telefónov (mobilný telefón, pracovný telefón a domáci telefón), pričom každý má iné číslo a používa inú prístupovú sieť.

Osobná mobilita by umožnila užívateľovi mať jeden telefón, ktorý mu umožní hovoriť cez WiFi a bez problémov prepnúť hovor na mobilnú sieť, keď sa bude nachádzať mimo pokrytia WiFi a naopak. Osobná mobilita tiež umožňuje užívateľovi zjednotiť služby ako hlasová pošta do jednej a sprístupniť ich, čím sa zvýši produktivita užívateľa. Umožňuje tiež zvýšenie efektívnosti mnohých ďalších pokročilých služieb, ako správa skupín.

Osobnú mobilitu umožňuje konvergencia; konkrétne konvergencia pevných sietí, bezdrôtových sietí a sietí IP údajov. Umožňuje užívateľovi využiť obrovský potenciál, ktorý vzniká kombináciou týchto sietí. Užívatelia majú možnosť využívať pevné aj mobilné telefóny a môžu si vybrať, ktorý použijú, v závislosti od ceny a vhodnosti. Môžu sa rozhodnúť, či uskutočnia hovor prostredníctvom pevného alebo mobilného telefónu, ak sú v práci alebo doma a majú k dispozícii obidva.

Bezproblémový automatický presun (handoff) medzi WiFi sieťami a mobilnými sieťami s minimálnou alebo žiadnou viditeľnosťou pre užívateľa, ako aj sada konvergenčných aplikácií, ktoré využívajú takýto bezproblémový automatický presun umožňujú poskytovateľovi služby dodávať osobnú mobilitu a tým aj väčšiu hodnotu pre užívateľov.

3.15 SIP kompresia

IMS podporuje multimediálne služby pomocou mechanizmu kontroly SIP volania. SIP je signalizačný klient-server protokol na báze textu používaný na vytvorenie a riadenie multimediálnych relácií s dvoma alebo viacerými účastníkmi. Správy tiež obsahujú veľké množstvo hlavičiek a parametrov hlavičiek, vrátané rozšírení a informácií súvisiacich so zabezpečením. Nastavenie SIP relácie je zdĺhavý proces, ktorý súčasťou je vyjednávanie kodekov a rozšírení, ako aj oznámenia o vzájomnej komunikácii QoS. Vo všeobecnosti poskytuje flexibilný rámec, ktorý umožňuje nastavenie relácií s rôznymi

požiadavkami. Nevýhodou však je veľký počet bytov a správ vymenených cez rádiové rozhranie. Zvýšená veľkosť správy znamená, že:

- Procedúry nastavenia volania prostredníctvom SIP budú oveľa zdĺhavejšie v porovnaní s procedúrami, ktoré využívajú signalizáciu špecifickú pre mobilný telefón, čo znamená, že koncový užívateľ pri vytváraní spojenia zaznamená oneskorenie, ktoré bude neočakávané a pravdepodobne neprijateľné.
- Signalizácia vnútorného volania určitým spôsobom negatívne ovplyvní kvalitu hlasu/výkon systému.

Podpora multimediálnych aplikácií v reálnom čase teda vyžaduje zvláštnu pozornosť, keď sa využíva SIP riadenie volania. Pre urýchlenie vytvorenia relácie 3GPP nariadila podporu SIP kompresie v UE aj v P-CSCF. Hoci je podpora kompresie povinná, 3GPP nebola nadšená z nariadenia jej podpory, pretože v budúcnosti terminály bezdrôtovej lokálnej počítačovej siete (Wireless Local Area Network - WLAN) možno nebudú používať SIP kompresiu vôbec. V čase písania bolo požadované, aby UE a P-CSCF implementovali funkčnosti kompresie tak, ako sú definované v [RFC3485], [RFC3486] a [3GPP TS 24.229]. Prvá uvedená RFC prináša celkové riešenie spôsobu kompresie SIP správ medzi dvoma entitami. Druhá RFC definuje statický slovník špecifický pre SIP/SDP, ktorý môže byť využitý v riešení signalizačnej kompresie s cieľom dosiahnuť vyššiu efektívnosť. Tretia RFC vysvetľuje akým spôsobom môže UE signalizovať, že je potrebná kompresia pre jednu alebo viac SIP správ

3.16 Vzájomná komunikácia medzi IPv4 a IPv6 v IMS

Široké nasadenie IPv6 na internete nepokročilo tak rýchlo, ako sa dúfalo alebo očakávalo, keď bol vyvinutý úvodný koncept IMS. Prispeli k tomu a ďalej prispievajú mnohé faktory, ale vo všeobecnosti akákoľvek zmena v základnej smerovacej infraštruktúre Internetu pravdepodobne zaberie oveľa viac času ako zmena prijatá len okrajoch siete.

Prekladače sieťových adries (Network Address Translator - NAT) sú ukážkou zmeny, ktorá spadá do druhej kategórie. NAT sú vo všeobecnosti pokladané za nežiadúce pre nové aj existujúce služby (napr. VoIP na báze SIP), ale z hľadiska investícií ponúkajú

dostupnú a ľahko nasaditeľnú možnosť pre rozšírenie rýchlo sa vyčerpávajúceho adresového priestoru IPv4, čím spomaľujú nasadenie dlhodobého riešenia vo forme IPv6.

V mnohých ohľadoch je to, čo sa deje všeobecne na Internete odrazom toho, čo sa deje v mobilnej doméne. Zatiaľ čo IPv6 je pokladaná za technicky nadriadenú IPv4 pre IMS, nariadenie podpory IPv6 predstavuje značnú prekážku nasadeniu akéhokoľvek systému. Použitie výlučne IPv6 tiež vyžaduje, aby roamingoví partneri a poskytovatelia služieb prešli na IPv6. To je dôvod, pre ktorý sa mnohé prvotné nasadenia rozhodli pracovať s existujúcimi GPRS prístupovými sieťami, ako aj bezpečnostnou infraštruktúrou a často existujúca sieťová infraštruktúra nepodporuje IPv6. Okrem toho 3GPP2 IP multimediálny systém, nazývaný multimediálna doména (Multimedia Domain – MMD), pracuje na IPv4 aj IPv6. To znamená, že akákoľvek vzájomná spolupráca IMS a MMD samozrejme zahŕňa aj vzájomnú spoluprácu IPv4-IPv6.

Z tohto dôvodu začalo byť zrejmé, že niektoré nasadenia IMS založené na IPv4 sú nevyhnutné, aj keď pôvodne boli špecifikované len pre podporu IPv6. Väčšinou sa tieto nasadenia IMS na báze IPv4 nazývajú "prvotné implementácie IMS“ a buď UE, alebo IMS základná sieť alebo oba používajú výlučne IPv4.

To má dva hlavné dôsledky:

- Implementácie IPv4 budú musieť vyrovnať s nutnosťou použiť súkromný adresový priestor, keďže nie všetky mobilné zariadenia môžu mať pridelenú adresu z verejného adresového priestoru.
- Po zavedení implementácií podporujúcich IPv6 popri implementáciách podporujúcich IPv4, musia byť schopné spolu pracovať bezchybným spôsobom.

Táto kapitola objasňuje otázky a riešenia vzájomnej spolupráce IPv4 a IPv6 v IMS. V Release 6 3GPP poskytuje vypracované smernice pre implementátorov prvotných IMS systémov vo forme technickej správy. To znamená, že kým nie je prvotná implementácia IMS schválená, sú poskytnuté aspoň nejaké smernice pre riešenie niektorých z najnaliehavejších záležitostí.

Preklad adresy

Základný komponent pre vyhotovenie prekladu adresy sa nazýva prekladač sieťových adries (Network Address Translator - NAT). NAT umožňuje zdieľanie jednej IP adresy

medzi viacerými hostiteľmi. Hostiteľom za NAT zariadením sú pridelené IP adresy, ktoré sú v súkromnom adresovom priestore (napr. v 192.168.0.0/16 alebo 10.0.0.0/24) a nie sú teda smerovateľné v Internete. NAT zariadenie potom vytvorí pre každé spojenie dočasné väzby medzi verejným a súkromným adresovým priestorom. Väzby sú jednoduchým namapovaním medzi verejnou IP adresou a portom na súkromnú adresu a port spojený s konkrétnym prenosom (UDP alebo TCP). Väzba trvá len po dobu trvania relácie, alebo kým časový limit pre väzba neuplynie. Väčšinou sú za účelom ušetrenia zdrojov tieto časové limity stanovené dosť agresívne.

Ďalší typ NAT je navrhnutý špeciálne pre preklad medzi verziami protokolu. Prekladač sieťových adries – Prekladač protokolu (Network Address Translator-Protocol Translator – NAT-PT) prekladá medzi IPv6 a IPv4. V skutočnosti zoberie IP datagram a nahradí hlavičku IPv6 hlavičkou IPv4 a naopak.

V IMS samotná existencia takýchto prekladacích zariadení nie je postačujúca. SIP aj SDP obsahujú jasné IP adresy, ako napríklad v poli hlavičky kontaktu SIP alebo SPD mediálnych linkách. Tieto adresy nebudú pochopiteľné ani dostupné pre peera, ktorý používa nesprávnu IP verziu. Musí teda existovať zariadenie pre bránu aplikačnej úrovne (Application Level Gateway – ALG), ktoré kontroluje SIP správy a nahrádza každý výskyt pôvodnej IP adresy preloženou adresou. NAT vo všeobecnosti nepovoľuje prevádzku smerujúcu dovnútra, kým nie je vygenerovaná prevádzka smerujúca von (t.j. je vytvorená väzba) čo znamená, že ALG musí tiež aktívne vytvárať väzby na základe mediálnych informácií obsiahnutých v SDP.

Často má ALG zariadenie rovnaké umiestnenie ako NAT zariadenie, pretože musí byť informované o prekladových väzbách a zavádzať ich. Riadiaca jednotka hranice relácie (Session Border Controller - SBC) je jedným typom takéhoto prekladača, aj keď SBC väčšinou vykonávajú aj mnohé ďalšie funkcie.

Ako možno očakávať, prekladače adries majú viaceré nedostatky:

- Sú jediným bodom zlyhania; ak je stratená prekladová väzba, celá relácia sa stane nepoužiteľná.
- ALG buď narušujú bezpečnosť alebo nefungujú správne v prítomnosti bezpečnostných mechanizmov na úrovni koncových zariadení. Zmena prenášaných správ je v podstate útokom „človek uprostred“ (Man-in-the-Middle – MITM).

- ALG nemajú transparentné vlastnosti; nová verzia SDP alebo iné pole hlavičky obsahujúcej IP adresu nebude rozpoznané alebo preložené správne.
- Problémy s rozšíriteľnosťou: Funkčnosť ALG je náročná na zdroje a NAT pre ukladanie väzieb požadujú zdroje ako aj šírku pásma.

Nie je prekvapením, že vzájomná komunikácia IPv4-IPv6 v IMS sa pokúša čo najviac zabrániť použitiu NAT a ALG. Odporúčajú sa ale pre niektoré scenáre prepojenia, ktoré sú neskôr popísané v Časti 3.17.3.

3.16.1 Porovnanie výlučnej implementácie IPv6 s duálnym zásobníkom (dual stack)

Jednou z kľúčových metód pre úspešný prechod na IPv6 je podpora prístupu dvojitej IP vrstvy na úrovni hostiteľov (a smerovačov), ktorý je tiež známy ako "činnosť duálneho zásobníka“. Duálny zásobník je technika pre poskytovanie podpory obidvom verziám IP – t.j. IPv6 aj IPv4. Hostiteľ duálneho zásobníka môže posielať a prijímať obidve verzie IP a môže teda komunikovať s obidvoma druhmi uzlov. Uzol duálneho zásobníka umožňuje tiež konfiguráciu s použitím obidvoch verzií adries, aj keď konfiguračný mechanizmus sa môže líšiť. Napríklad adresa IPv4 by mohla byť nakonfigurovaná pomocou DHCP a IPv6 adresa pomocou automatickej bezstavovej konfigurácie adresy.

Existujú aj ďalšie funkcie, ktoré musí uzol duálneho zásobníka podporovať. Napríklad musí podporovať IPv4 "A“ a IPv6 „AAAA“ DNS záznamy, bez ohľadu verziu datagramov, prostredníctvom ktorej boli tieto výsledky prijaté. Napríklad DNS dotaz zadaný pre doménu cez IPv4 môže vrátiť A aj AAAA záznamy, alebo len záznamy AAAA. Potom poradie použitia IP adries závisí od aplikácie, alebo môže byť tiež ovplyvnené poradím, v akom DNS server vracia príslušné záznamy.

Uzol môže tiež deaktivovať ktorúkoľvek z verzií protokolu zo zásobníka. V praxi však mnohé IMS uzly musia udržať IPv4 v prevádzke, keďže existujú ďalšie aplikácie – ako napríklad WWW – ktoré požadujú úplnú použiteľnosť IPv4.

UE a jadro IMS s duálnym zásobníkom ponúkajú viac možností presunu ako výlučné implementácie IPv4. Aj v keď je špecifická IP verzia deaktivovaná v zásobníku, môže byť neskôr opäť aktivovaná, keď bude verzia IPv6 viac rozšírená. Hlavným prínosom hostiteľov s duálnym zásobníkom je, že minimalizujú potrebu NAT zariadení

na sieti. Použitie hostiteľov podporujúcich len IPv6 ešte dlho nebude možné, keďže väčšina služieb bude stále založená len na IPv4.

3.16.2 Scenáre vzájomnej komunikácie

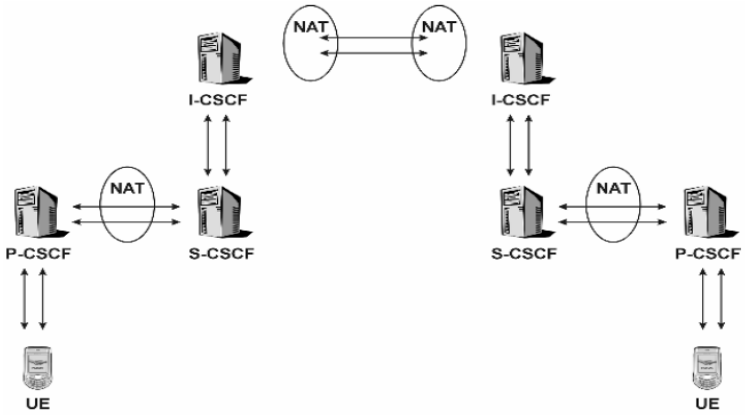
Hlavným problémom vzájomnej komunikácie IPv4-IPv6 je samozrejme rozdielna IP verzia. Existencia uzlov, ktoré rozumejú len jednej verzii vyvoláva nutnosť určitej formy prekladu. To platí pre signalizačnú prevádzku ako aj užívateľskú rovinu alebo mediálnu prevádzku. Existujú tiež mnohé spôsoby realizácie prekladu, v závislosti na tom, či jadro IMS podporuje IPv6.

Popis v tejto časti rozdelíme na scenáre v rámci domény a scenáre medzi doménami. Scenáre v rámci domény riešia vzájomnú komunikáciu UE a jadra IMS jedného IMS poskytovateľa, zatiaľ čo scenáre medzi doménami riešia vzájomné prepojenie sietí rôznych IMS poskytovateľov a uváženia na úrovni koncových zariadení medzi UE patriacimi sieťam rôznych IMS operátorov.

3.16.3 Scenáre v rámci domény

Scenáre vnútri domény sú oveľa komplikovanejšie. Ich zložitosť je dôsledkom toho, že je potrebné zohľadniť oveľa viac premenných. Okrem posielajúceho a prijímajúceho UE a jadra IMS je potrebné zohľadniť aj prenos medzi dvoma doménami, ktoré tiež môžu podporovať buď správanie založené na IPv4, duálnom zásobníku alebo IPv6. Okrem toho jadro IMS môže používať IPv4 adresy zo súkromného adresového priestoru, čo vyžaduje NAT na okraji siete pre vzájomné prepojenie s inými doménami.

Jadro IMS s duálnym zásobníkom môže vyžadovať ďalšie NAT zariadenie spojené s S-CSCF. Dôvodom je, že vzájomné prepojenie môže používať IPv4, ktorú I-CSCF a S-CSCF podporujú, ale UE nepodporuje. V takom prípade je potrebné zariadenie NAT-PT pre preklad IP verzií. Znázornené je to na Obrázku 3.25, ktorý ukazuje možné umiestnenie rôznych NAT zariadení.



Obrázok 3.25 Scenáre koncových zariadení a vzájomného prepojenia.

3.16.4 Konfigurácia a bootstrapping

Väčšinou po vytvorení L2 konektivity UE príjme IP adresu pomocou štandardnej konfigurácie, ako napríklad DHCP, alebo pomocou iného mechanizmu.

Ďalším krokom pre UE je nájsť svoj kontaktný pre IMS – a to adresu P-CSCF. V IMS sú existujúce odhaľovacie mechanizmy pre P-CSCF adresu buď špecifické pre IPv6, alebo používajú Release 5 (alebo neskorší) na báze GPRS. Pre nasadenie IMS na báze IPv4 môžu byť potrebné iné mechanizmy. Existuje niekoľko alternatívnych možností odhalenia P-CSCF adresy:

- Odhalenie pomocou GPRS by mohlo byť zmenené tak, že pri vytvorení PDP kontextu vráti aj IPv4 adresu aj IPv6 adresu.
- Pomocou DHCP možnosti pre konfiguráciu P-CSCF adresy.
- Mimopásmové zabezpečovacie mechanizmy, používajúce napríklad rámce pre správu zariadenia na báze služby posielania krátkych správ (Short Messaging Service – SMS), Over-the-Air (OTA) alebo otvorenej mobilnej aliancie (Open Mobile Alliance - OMA).
- Predbežná konfigurácia.

Použitie mimopásmového mechanizmu nevyžaduje zmeny existujúcej sieťovej infraštruktúry a preferuje ho teda pravdepodobne väčšina prvotných IMS

implementátorov. Predbežná konfigurácia adresy je tiež možnosť, ale nie je flexibilná s ohľadom na neskoršie zmeny pomenovania alebo typológie.

Okrem konfigurácie odchádzajúcej proxy adresy (napr. P-CSCF) sú v SIP hlavičke prenášané dodatočné informácie o adrese, ktorá tiež vyžaduje zváženie vzájomnej komunikácie. Napríklad akékoľvek vstupy cesty alebo adresy účtovacích entít musia byť zobrazené v IPv4 aj IPv5.

3.16.5 Prístupové siete podporujúce výlučne IPv4

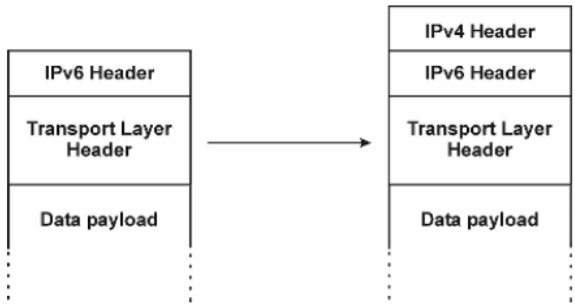
Aj keď sa nejedná výlučne o otázku IMS implementácie, z dôvodu funkčnosti v GPRS je prístupová sieť zvážená vo vzájomnej komunikácii IPv4-IPv6. Dôvodom je, že nosiče sú závislé na IP verzii: SGSN/GGSN, ktorý nepodporuje IPv6 neumožní vytvorenie IPv6 PDP kontextu. Staršie existujúce prístupové siete jednoducho nemusia podporovať IPv6. Prvé otázky súvisiace s vzájomnou komunikáciou sa teda týkajú GPRS prístupových sietí, scenárov s roamingom aj bez roamingu. Ak GPRS SGSN alebo GGSN nepodporujú IPv6, UE nie je schopné použiť natívnu IPv6, bez ohľadu na to, či ju niektorý z iných IMS elementov podporuje. Jediná dostupná možnosť pre použitie IPv6 v týchto scenároch je, že UE a jadro IMS použijú tunelovací mechanizmus, kde je každý IPv6 paket zbalený do IPv4 paketu a potom rozbalený pri výstupnom bode alebo smerovači – IP konektivita je tak vlastne pokladaná za LS prenos. Znázornené to je na Obrázku 3.26.

Zabalenie musí byť aplikované medzi hostiteľom a sieťovým uzlom s cieľom umožniť transparentnú komunikáciu s hostiteľom podporujúcim výlučne IPv6. Po rozbalení paketov ich koncový bod tunela vlastne nasmeruje na správneho hostiteľa v sieti. Tunely sú adresované a nastavené pomocou tunelovacieho mechanizmu, ako napríklad automatický intra-site protokol adresujúci tunel (Intra-Site Automatic Tunnel Addressing Protocol – ISATAP).

V ISATAP sú adresy rozhrania vytvorené s použitím statického mapovania z IPv4 adresy odkazu (t.j. posledných 32 bitov adresy rozhrania). Sú sprevádzané smerovacou tabuľkou, aby mohli byť pakety potom nasmerované na správne rozhranie. Tunelovací prístup má však niekoľko nevýhod:

- porušuje SBLP použitím Go rozhrania;

- domáca sieť musí byť nainštalovaná s tunelovacím serverom, ktorý slúži ako koncový bod tunela;
- takýto server musí tiež byť nakonfigurovaný alebo odhaliteľný UE;
- koncový bod tunela je jediným bodom zlyhania;
- použitie tunelu v scenároch s roamingom bude pravdepodobne neefektívne, keďže je celá prevádzka smerovaná cez domácu sieť – to spôsobí trojstranné smerovanie, ktoré zvýši oneskorenie;
- v každom prípade vyžaduje hostiteľa duálneho zásobníku, takže použitie natívnej IPv4 by mohlo lepším prístupom.



Obrázok 3.26 Tunelovací mechanizmus IPv6 na IPv4.

IPv6 Header – Hlavička IPv6
Transport Layer Header – Hlavička prenosovej vrstvy
Data payload – Dátový náklad
IPv4 Header – Hlavička IPv4

3.17 Kombinácia CS a IMS služieb - Kombinovanie služieb

3.17.1 Výmena schopnosti

V nasledujúcom príklade predpokladáme, že dvaja užívatelia sú spojení cez CS doménu – t.j. majú medzi CS spojenie. V tomto príklade Tobias zavolal svojej sestre na jej medzinárodné telefónne číslo. Pre umožnenie fungovania kombinačných služieb musia byť splnené viaceré požiadavky:

- v rámci CS signalizácie musí volajúca sieť poskytnúť Tobiasove telefónne číslo (MSISDN) Terezinmu UE v plnom medzinárodnom formáte – napr. +44123456789;
- Tobiasove MSISDN musí byť registrované v Tobiasovej domácej IMS sieti ako tel URL – napr. +4412345678;
- Terezine MSISDN musí byť poslané cez CS signalizáciu Tobiasovmu UE. Terezine MSISDN musí byť uvedené v medzinárodnom číselnom formáte a musí byť registrované v Terezinej domácej IMS sieti ako tel URL - napr. *tel:+36987654321*; a
- Tobias aj Tereza musia byť registrovaní s ich tel URL z tých istých UE, ktoré používajú medzi sebou pre uskutočnenie CS volaní.

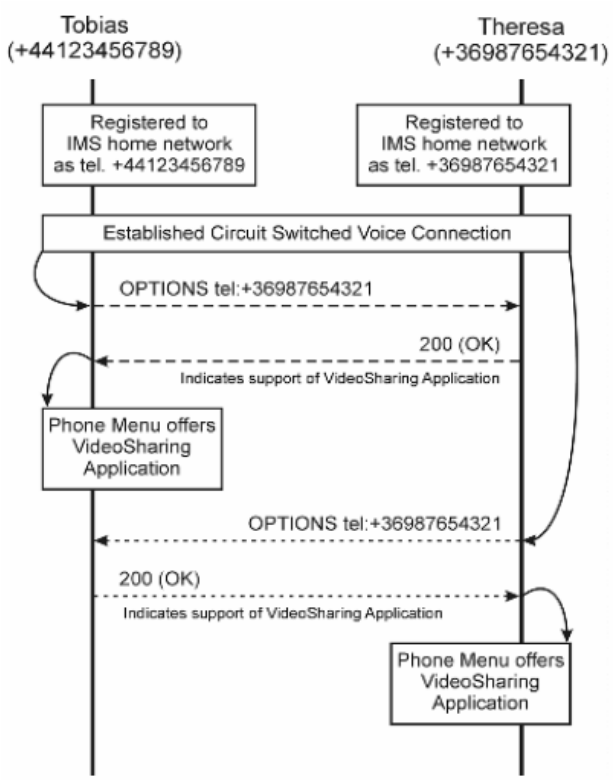
Pre zjednodušenie príkladu predpokladáme, že obidvaja užívatelia, Tobias aj Tereza, sú registrovaní len z jedného UE. Dôvodom je snaha predísť prípadom rozdvojenia. Tereza aj Tobias majú nainštalovanú aplikáciu založenú na IMS na ich UE, ktorá im okrem existujúceho CS hlasového volania umožňuje zdieľanie prúdov videa v reálnom čase. Táto peer-to-peer aplikácia bude fungovať len v prípade, že sa aplikácia nachádza na oboch UE. Za účelom poskytnutie konzistentnej užívateľskej skúsenosti bude položka menu "zdieľanie videa“ zobrazená len pre Terezu a Tobiasa, ak ich UE overili, že aplikácia je podporovaná aj na vzdialenom konci.

Pre dotázanie sa na schopnosti vzdialeného konca sa použije požiadavka SIP OPTIONS. Po nadviazaní CS volania obidve UE pošlú požiadavku OPTIONS do tel URL vzdialeného užívateľa. Tel URL bude odvodené z MSISDN vzdialeného užívateľa v CS volaní. V našom príklade Tobiasove UE pošle požiadavku OPTIONS na nasledujúcu adresu:

OPTIONS tel: +36987654321 SIP/2.0

Terezine UE pošle odpoveď 200 (OK) na túto požiadavku OPTIONS, kde budú uvedené schopnosti UE. Jedna z týchto schopností bude podpora aplikácie pre zdieľanie videa. Rovnaná výmena OPTIONS/200 (OK) bude uskutočnená v opačnom smere. Po ukončení týchto výmen bude Tereze aj Tobiasovi ponúknutá možnosť zdieľania prúdu videa s druhým užívateľom CS volania.

Ako bolo uvedené vyššie, uvedený príklad je len veľmi základný a ukazuje len akým spôsobom môžu byť v princípe vymieňané schopnosti medzi UE.



Obrázok 3.27 Výmena schopnosti počas prebiehajúceho CS volania.

Registered to IMS home network as tel. +44123456789 – Registrovaný do domácej IMS siete ako tel. +44123456789

Registered to IMS home network as tel. +36987654321 – Registrovaná do domácej IMS siete ako tel. +36987654321

Established Circuit Switched Voice Connection - Vytvorené obvodovo spínané hlasové spojenie

OPTIONS tel: +36987654321 – MOŽNOSTI tel: +36987654321

Phone Menu offers VideoSharing Application – Menu telefónu ponúka aplikáciu pre zdieľanie videa

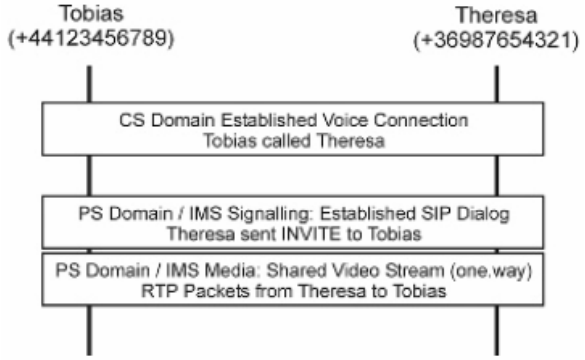
Indicates support of VideoSharing Application – Uvádza podporu aplikácie pre zdieľanie videa

3.17.2 Paralelné služby CS a IMS

Po výmene schopností môže jeden z užívateľ začať naživo zdieľať video. V našom príklad uživateľ (Theresa) chce poslať video druhemu uživateľovy (Tobias). Po

vytvorení spojenia môže prvy uživateľ poslať prúd videa cez GPRS. Obrázok 3.28 ukazuje spojenia, ktoré existujú ako paralelné.

Spojenie na základe SIP medzi dvoma užívateľmi môže byť uvoľnené buď v priebehu CS volania alebo ho aplikácia zdieľania videa uvoľní automaticky po ukončení CS volania. Je to správanie výslovne špecifické pre aplikáciu.



Obrázok 3.28 Príklad paralelných spojení pri kombinácii IMS a CS služieb.

CS Domain Established Voice Connection – CS doména nadviazala hlasové spojenie
Tobias called Theresa – Tobias zavolal Tereze
PS Domain/IMS Signalling: Established SIP Dialog - PS doména/IMS signalizácia: Nadviazaný SIP dialóg
Theresa sent INVITE to Tobias – Tereza poslala Tobiasovi INVITE
PS Domain/IMS Media: Shared Video Stream (one way) - PS doména/IMS médiá: Zdieľaný prúd videa (jedným smerom)
RTP Packets from Theresa to Tobias - RTP pakety od Terezy Tobiasovi

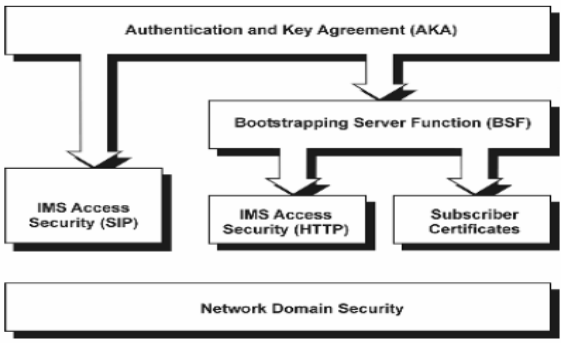
3.18 Bezpečnostné služby v IMS

Úlohou tejto časti je vysvetliť, ako funguje zabezpečenie v IMS. Zámerne sa podrobnejšie nebude venovať kryptografii, nebude preto ani do hĺbky rozoberať algoritmy a dĺžky kľúčov, taktiež nebude vykonávať žiadnu kryptoanalýzu zabezpečenia IMS. O tejto téme bolo napísaných už veľa kníh.
Táto kapitola naopak poskytne pohľad na vysokej úrovni na architektúru zabezpečenia a popíše jednotlivé komponenty tejto architektúry, vrátanie modelov a protokolov používaných na dosiahnutie požadovaných bezpečnostných vlastností. Po prečítaní tejto kapitoly by mal byť čitateľ oboznámený so základnými konceptmi architektúry

zabezpečenia IMS a rozumieť podkladovým modelom, hlavne tým ktoré sa venujú dôvere a identite a ktoré utvárajú bezpečnosť IMS ako celku.

3.18.1 Model zabezpečenia IMS

Architektúra zabezpečenia IMS sa skladá z troch stavebných blokov, ako je to znázornené na Obrázku 3.29. Prvý stavebný blok je zabezpečenie sieťovej domény (Network Domain Security - NDS) [3GPP TS 33.210], ktoré poskytuje IP zabezpečenie medzi rôznymi doménami, ako aj medzi uzlami v rámci jednej domény.



Obrázok 3.29 Architektúra zabezpečenia IMS.

Authentication and Key Agreement (AKA) - Autentifikácia a dohoda o kľúči
Bootstrapping Server Function (BSF) - Serverová bootstrapping funkcia (BSF)
IMS Access Security (SIP), IMS Access Security (HTTP) - Zabezpečenie prístupu IMS (SIP), Zabezpečenie prístupu IMS (HTTP)
Subscriber Certificates - Certifikáty účastníka
Network Domain Security – Zabezpečenie sieťovej domény

Po boku NDS je rozvrstvené zabezpečenie IMS prístupu [3GPP TS 33.203]. Zabezpečenie prístupu pre služby na báze SIP je sám o sebe nezávislý komponent, výnimku tvorí fakt, že preň určené bezpečnostné parametre sú odvodené z protokolu UMTS autentifikácie a dohody o kľúči (Authentication and Key Agreement - AKA) [3GPP TS 33.102]. AKA sa taktiež používa pre účely bootstrappingu (zavádzanie zložitejšieho systému systémom jednoduchším) - okrem iného sa menovite kľúče a certifikáty odvodzujú z AKA záznamov a následne sa používajú na zabezpečenie

aplikácií bežiacich pod hypertextovým prenosovým protokolom (Hypertext Transfer Protocol - HTTP) [RFC2616] – v takzvanej všeobecnej autentifikačnej architektúre (Generic Authentification Architecture - GAA).
Z tohto architektonického modelu sú zámerne vylúčené tie bezpečnostné vrstvy, ktoré potenciálne ležia nad zabezpečením IMS prístupu alebo bežia pod NDS. V UMTS napríklad vrstva rádiového prístupu implementuje vlastnú množinu bezpečnostných vlastností, vrátane šifrovania a integrity správ. IMS je však navrhnutý tak, že nezávisí na existencii zabezpečenia prístupu alebo zabezpečenia užívateľskej roviny.

3.18.2 Autentifikácia a dohoda o kľúči (AKA)

Zabezpečenie v IMS je založené na dlhodobom tajnom kľúči, zdieľanom medzi ISIM a autentifikačným centrom domácej siete (Authentication Centre - AUC). Najdôležitejší stavebný blok zabezpečenia IMS je modul ISIM, ktorý slúži ako úložisko pre zdieľané tajomstvo (K) a sprievodné AKA algoritmy a najčastejšie je zabudovaný v zariadení obsahujúcom čipovou kartu, ktoré sa volá univerzálna karta na báze integrovaných obvodov (Universal Integrated Curcuit Card - UICC). Prístup k zdieľanému tajomstvu je obmedzený. Modul prijme na vstupe AKA parametre a na výstupe vráti výsledné AKA parametre a výsledky. Takto nikdy neodhalí zdieľané tajomstvo vonkajšiemu svetu.

Zariadenie, na ktorom je umiestnený ISIM je odolné voči manipulácii, takže aj fyzický prístup k zariadeniu by nemal viesť k odhaleniu zdieľaného tajomstva. Pre ďalšiu ochranu ISIM pred nepovoleným prístupom podlieha užívateľ zvyčajne bezpečnostným mechanizmom v rámci domény užívateľa. Toto v podstate znamená, že aby bolo možné spustiť AKA na ISIM, je od užívateľa požadovaný PIN kód. Kombinácia vlastníctva – t.j. prístup k fyzickému zariadeniu (UICC/ISIM) - a znalosti tajného PIN kódu robí architektúru zabezpečenia IMS dôkladnou. Útočník musí vlastniť oboje - "niečo čo vlastníš" a "niečo čo vieš", čo je zložité za predpokladu, že mobilný užívateľ disponuje aspoň určitou úrovňou opatrnosti.
AKA uskutoční vzájomnú autentifikáciu ISIM a AUC a vytvorí pár šifrovacieho kľúča a kľúča integrity. Autentifikačná procedúra je spustená sieťou pomocou autentifikačnej požiadavky, ktorá obsahuje náhodnú výzvu (RAND) a sieťovú autorizačnú známku (AUTN). ISIM overí AUTN a tým overí autenticitu siete ako takej. Každý koniec taktiež spravuje sekvenciu čísel pre každé kolo autentifikačných procedúr. Ak ISIM zachytí

autentifikačnú požiadavku so sekvenciu čísel mimo rozsah, preruší autentifikáciu a ohlási sieti správu o zlyhaní synchronizácie, spolu so správnym číslom sekvencie. Toto je ďalší koncept vysokej úrovne, ktorý zabezpečuje ochranu proti opätovnému prehrávaniu.
Aby bolo možné odpovedať na autentifikačnú požiadavku siete, ISIM použije tajný kľúč na RAND na vytvorenie autentifikačnej odpovede (RES). Pre autentifikáciu ISIM je potrebné overiť RES prostredníctvom siete. V tomto momente sa už UE a sieť úspešne vzájomne autentifikovali a ako vedľajší produkt vytvorili taktiež pár relačných kľúčov: kľúč šifrovania (Cipher Key - CK) a kľúč integrity (Integrity Key - IK). Tieto kľúče môžu byť potom použité pre zabezpečenie následnej komunikácie medzi týmito dvoma entitami. Tabuľka 3.13 obsahuje zoznam niektorých centrálnych AKA parametrov spolu s popisom ich významu.

Tabuľka 3.13 Parametre autentifikácie a dohody o kľúči

AKA parameter	Veľkosť (bity)	Popis
K	128	Zdieľané tajomstvo; autentifikačný kľúč zdieľaný sieťou a mobilným terminálom
RAND	128	Náhodná autentifikačná výzva vygenerovaná sieťou
AUTN	128	(Sieťová) autentifikačná známka
SQN	48	Číslo sekvencie sledujúce sekvenciu autentifikačných procedúr
AUTS	112	Synchronizačná známka vygenerovaná ISIM pri detekcii zlyhania synchronizácie
RES	32-128[a]	Aplikačná odpoveď generovaná ISIM
CK	128	Šifrovací kľúč vygenerovaný počas autentifikácie sieťou aj ISIM
IK	128	Kľúč integrity vygenerovaný počas autentifikácie sieťou aj ISIM

3.18.3 Zabezpečenie sieťovej domény (Network Domain Security - NDS)

Jedna z hlavných identifikovaných slabostí systémov 2G je nedostatok štandardizovaných bezpečnostných riešení pre základné siete. Ak keď je rádiový prístup z mobilného terminálu k základňovej stanici zvyčajne chránený šifrovaním, uzly vo zvyšku systému posielajú prevádzku priamo. Niekedy tieto linky dokonca použijú

nechránené rádiové skoky (hops) , takže útočník, ktorý má prístup k tomuto médiu, môže veľmi jednoducho odpočúvať komunikácie.

Na základe poučenia z nedostatkov 2G sietí vzniká u 3G systémov snaha chrániť celú IP prevádzku v základnej sieti. Zabezpečenie sieťovej domény (Network Domain Security - NDS) dosahuje túto požiadavku poskytnutím diskrétnosti, integrity údajov, autentifikácie a ochrany prevádzky proti opätovnému prehrávaniu pomocou kombinácie kryptografických bezpečnostných mechanizmov a protokolových bezpečnostných mechanizmov použitých v IP zabezpečení (IPsec).

Bezpečnostné domény

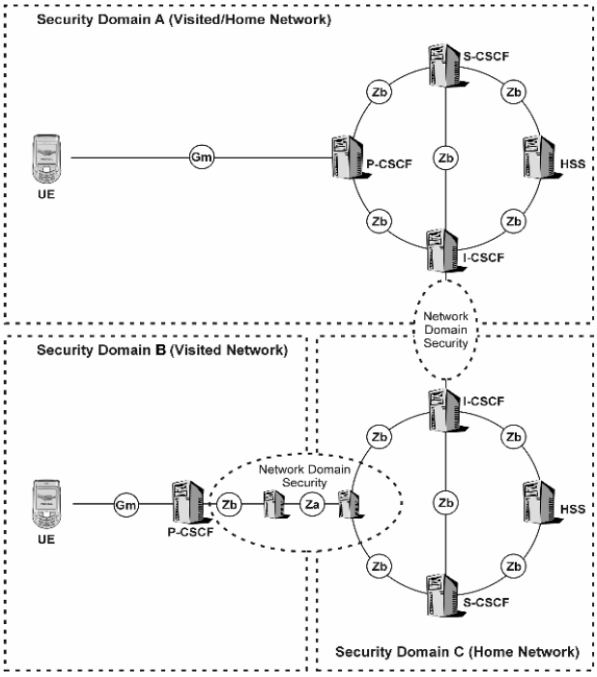
Bezpečnostné domény sú v koncepte NDS najdôležitejšie. Bezpečnostná doména je typicky sieť riadená jediným administratívnym orgánom ktorý udržuje jednotnú bezpečnostnú politiku v rámci danej domény. Dôsledkom je, že úroveň zabezpečenia a nainštalovaných bezpečnostných služieb bude vo všeobecnosti v rámci bezpečnostnej domény rovnaká.

V mnohých prípadoch zodpovedá bezpečnostná doména priamo základnej sieti operátora. Je však možné prevádzkovať viaceré bezpečnostné domény, ktoré náležia podmnožine základnej siete operátora. V NDS/IP sú rozhrania medzi rôznymi bezpečnostnými doménami označené ako Za a rozhrania medzi prvkami vnútri bezpečnostnej domény sú označené ako Zb. Kým použitie Zb rozhrania je vo všeobecnosti nepovinné a rozhoduje o ňom administrátor bezpečnostnej domény, použitie Za rozhrania je medzi rôznymi bezpečnostnými doménami vždy povinné. Autentifikácia údajov a ochrana integrity je povinná pre obidva rozhrania, pričom použitie šifrovania je pre Zb nepovinné a pre Za odporúčané.

IMS je založený na známom koncepte domácej siete a navštívenej siete. V podstate existujú dva scenáre podľa toho, či IMS terminál využíva roaming alebo nie. V prvom scenári je prvý bod kontaktu UE do IMS, nazývaný P-CSCF, umiestnený v domácej sieti, čo znamená, že UE vlastne využíva roaming takým spôsobom, že jeho prvý bod kontaktu do IMS sa nenachádza v domácej sieti. Tieto dva scenáre sú znázornené na Obrázku 3.30.

Často IMS sieť zodpovedá jedinej bezpečnostnej doméne a prevádzka medzi IMS sieťami operátora je chránená pomocou NDS/IP. To platí aj vo vyššie uvedenom druhom scenári, kde je prevádzka medzi navštívenou sieťou a domácou sieťou tiež chránená pomocou NDS/IP.

VIMS NDS/IP chráni len prevádzku medzi sieťovými prvkami v IP vrstve; sú teda požadované dodatočné bezpečnostné opatrenia. Dôležitejšie je, že v oblasti SIP prevádzky nie je prvý skok chránený pomocou NDS/IP, ale je chránený pomocou IMS prístupových bezpečnostných opatrení [3GPP TS 33.203]. Vyššie uvedený scenár, v ktorom sú IMS prvky rozdelené medzi domácu sieť a navštívenú sieť a teda medzi rôzne bezpečnostné domény vyžaduje špeciálny prístup v oblasti autentifikácie a distribúcie kľúča.



Obrázok 3.30 Bezpečnostné domény v IMS.

Security Domain A (Visited/Home Network) - Bezpečnostná doména A (Navštívená/Domáca sieť)

Security Domain B (Visited Network) - Bezpečnostná doména B (Navštívená sieť)

Network Domain Security – Zabezpečenie sieťovej domény

Security Domain C (Home Network) – Bezpečnostná doména C (Domáca sieť)

Bezpečnostné brány

Prevádzka vstupujúca a odchádzajúca z bezpečnostnej domény prechádza cez bezpečnostnú bránu (Security Gateway - SEG). SEG sa nachádza na hranici bezpečnostnej domény a tuneluje prevádzku smerom k definovanej sade iných bezpečnostných domén. Tento proces sa nazýva hub-and-spoke model; poskytuje hop-by-

hop (skok-za-skokom) zabezpečenie medzi bezpečnostnými doménami. SEG zodpovedá za presadzovanie bezpečnostnej politiky pri postupovaní prevádzky medzi bezpečnostnými doménami. Toto presadenie politiky môže zahrňovať aj filtrovanie paketov alebo funkčnosť firewallu, ale za túto funkčnosť zodpovedá administrátor domény.

V IMS je všetka prevádzka v rámci IMS základnej siete smerovaná cez SEG, obzvlášť ak ide o prevádzku medzi doménami čo znamená, že pochádza z inej bezpečnostnej domény ako z tej, kde je prijímaná. Pri ochrane IMS prevádzky medzi doménami je požadovaná dôvernosť aj integrita údajov a autentifikácia v NDS/IP.

Správa a distribúcia kľúčov

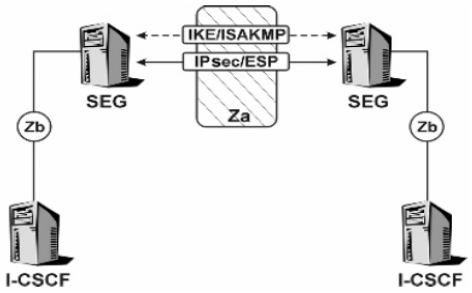
Každý SEG je zodpovedný za nastavenie a udržiavanie IPsec bezpečnostných asociácií (Security Associations - SAs) [RFC2401] so svojím peer SEGs. Tieto SAs sú vyjednané pomocou protokolu výmeny internetového kľúča (Internet Key Exchange - IKE) [RFC2409], kde je autentifikácia vykonávaná pomocou dlhodobých kľúčov uložených v SEG. SEG udržiava celkovo dve SAs pre jedno peer spojenie: jedno pre prichádzajúcu prevádzku a jedno pre odchádzajúcu prevádzku. Okrem toho SEG udržiava jednoduchú internetovú bezpečnostnú asociáciu a protokol správy kľúča (Internet Security Association and Key Management Protocol - ISAKMP) SA [RFC2408], ktoré súvisia so správou kľúča a sú použité pre vytvorenie aktuálnych IPsec SAs medzi peer hostiteľmi. Jeden z kľúčových predpokladov pre ISAKMP SA je, aby boli peer autentifikovaní. V NDS/IP je autentifikácia založená na kľúčoch vopred zdieľaného tajomstva (Preshared Secret Keys - PSKs). V 3GPP Release 6 je NDS rozšírené tak, aby mohli byť medzi SEG použité aj iné mechanizmy autentifikácie ako je PSK. Autentifikačný rámec NDS (NDS Authentication Framework - NDS/AF) [3GPP TS 33.310] definuje infraštruktúru založenú na verejnom kľúči (Public Key Infrastructure - PKI), model dôvery a mechanizmy pre autentifikáciu SEG pomocou certifikátov verejného kľúča a podpisov RSA. Model dôvery pre PKI požadovaný NDS/AF zahŕňa dva režimy krížovej certifikácie:

- Manuálna krížová certifikácia: v tomto režime sa autority rozhodujú samostatne pre dôveru inej autorite domény. Tento režim má problém s mierkou, pretože každá vzdialená bezpečnostná doména potrebuje platný, lokálne dôveryhodný (podpísaný)

certifikát. Toto obmedzenie je podobné ako obmedzenia platné pre základnú NDS/IP, s použitím PSKs.

- Krížová certifikácia používajúca premosťovaciu certifikačnú autoritu (CA – Certificate Authority): v tomto režime aplikuje entita sprostredkovateľa alebo clearinghouse 1-k-1 certifikáciu a rôzne bezpečnostné domény si navzájom dôverujú prostredníctvom tranzitnej dôvery. To obmedzuje množstvo požadovanej certifikácie, keďže jediná autorita domény potrebuje len krížovú certifikáciu s premosťovacou CA.

Krížová certifikácia je proces stanovenia dôvery medzi dvoma autoritami domény. Keď je autorita domény A krížovo certifikovaná s autoritou domény B, obe sú schopné dôverovať certifikátu tej druhej - t.j. sú schopné autentifikovať jedna druhú.



Obrázok 3.31 NDS/IP a SEG.

Bezpečnostný protokol používaný v NDS/IP pre šifrovanie, ochranu integrity údajov a autentifikáciu je Zapúzdrovací bezpečnostný náklad IPsec (Encapsulating Security Payload - ESP) [RFC2406] v tunelovacom režime. V ESP tunelovacieho režimu je celý IP datagram vrátane IP hlavičky zahrnutý do ESP paketu. Pre šifrovanie je povinný 3DES [RFC1851] algoritmus, zatiaľ čo pre integritu údajov a autentifikáciu môže byť použitý MD5 [RFC 1321] aj SHA-1 [RFC2404].

3.18.4 Zabezpečenie IMS prístupu pre služby založené na SIP

SIP je v jadre IMS, keďže sa používa na vytváranie, správu a ukončovanie rôznych typov multimediálnych relácii. Kľúčový prvok, ktorý je potrebné dosiahnuť pre zabezpečenie prístupu k IMS je chrániť SIP signalizáciu v IMS. Ako už bolo uvedené, v IMS základnej sieti je toto dosiahnuté použitím NDS/IP. Ale prvý skok (hop), čiže

rozhranie pre SIP komunikácie medzi UE a IMS P-CSCF označované ako Gm vyžaduje dodatočné opatrenia, keďže sa nachádza mimo oblasť NDS/IP.

Bezpečnostné funkcie a mechanizmy pre zabezpečený prístup do IMS sú špecifikované v [3GPP TS 33.203]. Je tam definovaný aj spôsob, akým sú UE a sieť autentifikované, ako aj spôsob ich súhlasu s použitými bezpečnostnými mechanizmami, algoritmami a kľúčmi.

Prehľad modelu dôvery

IMS zriaďuje doménu dôvery, ako je to popísané v [RFC3325], ktorá zahŕňa nasledovné IMS prvky:

- P/I/S-CSCF;
- BGCF;
- MGCF/MRFC;
- Všetky AS, ktoré nie sú pod kontrolou tretej strany.

Hlavným prvkom dôvery je identita: za účelom dôverovať prvku pristupujúcemu k IMS musí byť vytvorený vzťah s týmto prvkom (t.j. jeho identita je známa a overená). V IMS je táto identita predávaná medzi uzlami v doméne dôvery vo forme uplatňovanej identity. UE môže určiť preferenciu pre túto identitu, ak existujú viaceré identity; pridelenie uplatňovanej identity je ale úplne na hranici domény dôvery (menovite v P-CSCF). Naopak P-CSCF zohráva hlavú úlohu v autentifikácii UE.

Úroveň dôvery je vždy vzťahovaná k očakávanému správaniu entity. Napríklad Alica môže poznať Boba a dôverovať mu, že zoberie jej deti do školy. Očakáva a vie, že Bob bude jednať zodpovedne, šoférovať bezpečne a podobne. Ale nemusí dôverovať Bobovi dostatočne na to, aby mu dala prístup k jej bankovému účtu.

Iná dôležitá vlastnosť IMS modelu dôvery je, že je založený na tranzitnej dôvere. Existencia párovej dôvery medzi prvou a druhou entitou, ako aj druhou a treťou entitou automaticky zavádza dôveru medzi prvou a treťou entitou: napríklad Alica pozná a dôveruje Bobovi, ktorý zase pozná a dôveruje Celii, že zoberie jeho deti do školy. Teraz v súlade s tranzitívnou dôverou môže Alica dôverovať aj Celii, že zoberie jej deti do školy bez toho, aby niekedy osobne stretla Celiu. Stačí, že Alica dôveruje Bobovi a vie, že Celia je tiež súčasťou domény dôvery rodičovstva. Fakt, že Alica a Bob sú obaja

rodičia uisťuje Alicu, že Bob náležite starostlivo zvážil, či je Celia je vhodná pre odvedenie detí do školy. Doména dôvery rodičovstva v podstate vytvára sieť rodičov, ktorí všetci spĺňajú preddefinované správanie matky a otca.

Z hľadiska [RFC3325] musí byť očakávané správanie entity v doméne dôvery ako aj zabezpečenie zhody s očakávaným správaním špecifikované pre konkrétnu doménu dôvery T v takzvanej „Spec(T)". Súčasti, ktoré vytvárajú Spec(T) sú:

- Definícia spôsobu autentifikácie užívateľov vstupujúcich do domény dôvery a definícia použitých bezpečnostných mechanizmov, ktoré zabezpečujú komunikáciu medzi užívateľmi a doménou dôvery. V IMS má toto za následok autentifikáciu pomocou AKA protokolu a súvisiacich špecifikácii o Gm bezpečnosti v [3GPP TS 33.203].
- Definícia mechanizmov použitých pre zabezpečenie komunikácii medzi uzlami v doméne dôvery. V IMS je táto časť zdokumentovaná v NDS/IP [3GPP TS 33.210].
- Definícia postupov použitých pri určovaní súboru entít, ktoré sú súčasťou domény dôvery. V IMS tento súbor entít v podstate reprezentuje súbor peer SEGs, o ktorom je SEG v bezpečnostnej doméne informovaná.
- Uplatnenie týchto uzlov v domény dôvery je v súlade so špecifikáciami identity s uplatnenou SIP.
- Definícia riadenia súkromia. Táto definícia je založená na SIP bezpečnostných mechanizmoch a spôsobe ich použitia s uplatňovanými identitami (Časť 3.18.4 sa bude tejto problematike venovať detailnejšie).

Riešenie súkromia užívateľa

Koncept domény dôvery a uplatňovanej identity umožňuje postúpiť uplatňovanú identitu užívateľa ďalej, eventuálne prvkom, ktoré nie sú súčasťou domény dôvery. Toto vyvoláva otázky ohľadom súkromia, keďže užívateľ môže v skutočnosti požadovať, aby bola jeho identita zachovaná ako dôverná a interná pre doménu dôvery.

V IMS môže užívateľ požadovať, aby jeho identita nebola odhalená prvkom mimo doménu dôvery. To je založené na SIP súkromných rozšíreniach [RFC3323]. UE vkladá svoje preferencie ohľadom súkromia do poľa súkromia v hlavičke, ktoré je potom preverované sieťou. Možné hodnoty pre túto hlavičku sú:

- Užívateľ – stanovuje, že funkcie súkromia na užívateľskej úrovni by mali byť poskytnuté sieťou. Túto hodnotu zvyčajne nastavujú skôr prostredníci ako zástupcovia užívateľa.
- Hlavička – stanovuje, že UA požaduje, aby bola v správe použitá hlavička súkromia. Toto znamená, že všetky hlavičky citlivé na súkromie budú zatmavené a že žiadna iná citlivá hlavička nebude pridaná.
- Relácia – určuje, že UA požaduje, aby údaje citlivé na súkromie boli zatmavené pre túto reláciu (t.j. v SDP náklade správy).
- Kritické – určuje, že požadované mechanizmy súkromia sú kritické. Ak akýkoľvek z týchto mechanizmov nie je k dispozícii, požiadavka by nemala byť úspešná.
- ID – určuje, že užívateľ požaduje, aby bola jeho uplatňovaná identita udržaná vo vnútri domény dôvery. Nastavenie tejto hodnoty v praxi znamená, že pole hlavičky P uplatňovaná identita musí byť odstránené zo správy, ktorá opúšťa doménu dôvery.
- Žiadne – určuje, že UA explicitne nevyžaduje žiadne mechanizmy súkromia, ktoré by mali byť aplikované na požiadavku.

Súkromie na užívateľskej úrovni znamená funkcie súkromia, ktoré je schopné poskytnúť samotné SIP UA (napr. prostredníctvom anonymnej identity v poli From (Od) požiadavky).

Autentifikácia a dohoda o zabezpečení

Autentifikácia pre prístup IMS je založená na AKA protokole. Napriek tomu nemôže byť AKA protokol spustený priamo cez IP; namiesto toho potrebuje prostriedok prenosu na prenos protokolových správ medzi UE a domácou sieťou. Keďže konečným cieľom autentifikácie IMS prístupu je autentifikácia SIP prístupu, SIP je prirodzeným výberom pre takýto prostriedok prenosu. Spôsob, akým je v praxi AKA protokol tunelovaný vnútri SIP je bližšie popísaný v [RFC3310]. To definuje formát správ a postupy pre používanie AKA ako systém hesiel výberu autentifikácie [RFC2617] pre SIP registračný postup. Výzva na výber pochádzajúca zo siete bude obsahovať RAND a AUTN AKA parametre, kódované v príležitostnej hodnote servera. Výzva obsahuje špeciálny pokyn pre algoritmus, ktorý poučí klienta o používaní AKA protokolu pre túto konkrétnu výzvu. RES sa používa ako heslo pri počítaní súkromných údajov výberu čo

znamená, že výber systému sa používa špeciálnym spôsobom za účelom tunelovania AKA protokolu pri zabezpečení IMS prístupu.

Súčasne s autentifikáciou užívateľa musia UE a IMS vyjednať bezpečnostné mechanizmy, ktoré budú použité v zabezpečení následnej SIP prevádzky v Gm rozhraní. Protokol používaný pre túto dohodu o zabezpečení je opäť SIP, ako je to špecifikované v [RFC3329]. UE a P-CSCF si vymieňajú ich príslušné zoznamy podporovaných bezpečnostných mechanizmov a najvyšší spoločne podporovaný mechanizmus je zvolený a používaný. Zvolený bezpečnostný mechanizmus musí prinajmenšom poskytovať údaje o ochrane integrity, keďže je to požadované pre ochranu aktuálneho vyjednávania bezpečnostného mechanizmu. Po zvolení bezpečnostného mechanizmu a po začatí jeho používania je predtým vymenený zoznam znovu nahraný do siete bezpečným spôsobom. Toto sieti umožňuje overiť, že voľba bezpečnostného mechanizmu bola správna a že dohoda o zabezpečení nebola porušená. Príklad útoku, ktorý by bol možný bez tejto funkcie je "útok na spôsobenie poklesu" (bidding-down attack), kde útočník donúti peerov zvoliť si známy slabý bezpečnostný mechanizmus. Dôležitou výhodou bezpečného vyjednávania použitého bezpečnostného mechanizmu je, že nový mechanizmus môže byť neskôr pridaný a staré môžu byť odstránené. Mechanizmy môžu úspešne spoločne existovať, pretože každé UE vždy používa najsilnejší mechanizmus, ktorý má k dispozícii.

Ochrana dôvernosti a integrity

Pri zabezpečení IMS prístupu je povinná dôvernosť ako aj integrita údajov a autentifikácia. Protokol používaný pre ich poskytovanie je IPsec ESP [RFC2406].

AKA kľúče pre reláciu sú používané ako kľúče pre ESP SAs. IK sa používa ako autentifikačný kľúč a CK ako šifrovací kľúč. V závislosti na dĺžkach kľúča požadovaných šifrovacími algoritmami používanými v ESP môžu byť pre AKA relačné kľúče použité určité rozšírenia kľúčov.

Riadenie a distribúcia kľúča

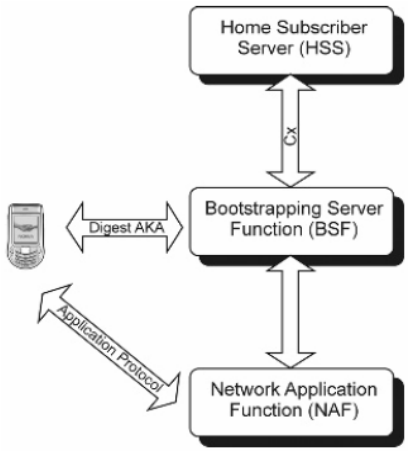
Ako je to popísané v predchádzajúcich kapitolách, P-CSCF môže sídliť tiež v navštívenej sieti. Na základe AKA protokolu je zdieľané tajomstvo prístupné len v domácej sieti čo znamená, že ak musí byť autentifikácia vykonaná v domácej sieti, musí

byť určitá delegovaná zodpovednosť pridelená P-CSCF, keďže medzi P-CSCF a UE existuje IPsec SAs. V skutočnosti zatiaľ čo autentifikácia IMS prebieha v domácej sieti, relačné kľúče vytvárané v AKA autentifikácii a používané v ESP sú dodávané do P-CSCF prenášané nad SIP registračnými správami.

Pre obnovenie SA musí sieť opätovne autentifikovať UE. Toto znamená, že UE musí tiež obnoviť registráciu, čo môže byť iniciované sieťou alebo spôsobené uplynutím registrácie. Celkový efekt je rovnaký: AKA protokol je v spustený a čerstvé kľúče sú dodávané do P-CSCF.

3.18.5 Zabezpečenie IMS prístupu pre služby založené na HTTP

Súčasne s prevádzkou SIP je potrebné, aby UE riadil údaje spojené s určitými IMS aplikáciami. Ut rozhranie hosťuje protokoly potrebné pre túto funkčnosť. Zabezpečenie Ut rozhrania zahŕňa ochranu dôvernosti a integrity údajov prevádzky založenej na HTTP [RFC2616]. Ako bolo uvedené v prechádzajúcom texte, užívateľská autentifikácia a vytvorenie kľúča pre rozhranie Ut sú tiež založené na AKA.



Obrázok 3.32 Všeobecná architektúra bootstrappingu.

Home Subscriber Server (HSS) - Domáci účastnícky server (HSS)
Digest AKA - Výber AKA
Bootstrapping Server Function – Serverová bootstrapping funkcia (BSF)
Application Protocol - Aplikačný protokol
Network Application Function (NAF) - Sieťová aplikačná funkcia (NAF)

Všeobecná architektúra bootstrappingu (Generic Bootstrapping Architecture GBA)

Ako súčasť GAA 3GPP IMS definuje Všeobecnú architektúru bootstrappingu (Generic Bootstrapping Architecture - GBA) [3GPP TS 33.220], zobrazenú na Obrázku 3.32. Serverová bootstrapping funkcia (Bootstrapping Server Function - BSF) a UE vykonávajú vzájomnú autentifikáciu založenú na AKA, ktorá umožňuje UE použiť bootstrapping nad relačnými kľúčmi z 3G infraštruktúry. Relačné kľúče sú výsledkom AKA a umožňujú ďalšie aplikácie poskytované Sieťovou aplikačnou funkciou (Network Application Function - NAF). Jeden takýto príklad je NAF, ktorá vydáva účastnícke certifikáty použitím aplikačného protokolu zabezpečeného relačnými kľúčmi vzniknutými bootstrappingom.

Autentifikácia a správa kľúčov

Autentifikácia je v rozhraní Ut vykonávaná špecializovaným prvkom nazývaným "autentifikačné proxy“. Pokiaľ ide o GBA, autentifikačné proxy je iný typ NAF. Prevádzka v Ut rozhraní prechádza cez autentifikačné proxy a je zabezpečená použitím relačného kľúča vzniknutého bootstrappingom.

Ochrana dôvernosti a integrity

Rozhranie Ut používa bezpečnosť prenosovej vrstvy (Transport Layer Security - TLS) pre ochranu dôvernosti aj integrity [3GPP TS 33.222].

4. Prednáškové cykly

V tejto kapitole sa venujem vytvoreniu prednáškových cyklov, ktoré oboznámia poslucháčov o technológii IMS. Stručnejší popis podľa kapitol jednotlivých prednášok je uvedený v tabuľke 4.1.

4.1 Úvodná prednáška

Úvodná prednáška objasní poslucháčom prečo a ako systém IMS vznikol. Treba spomenúť staršie technológie pevných a mobilných sietí, pričom treba spomenúť hovor a služby spojené s hovorom, ako je popísané v časti 1 a 1.1. Doraz je kladený na siete tretej generácie a ich vývoj od GSM až po podobu RELEASE 7, ktoré sú popísane v časti 1.2. Prednáška bude zakončená porovnaním vlastnosti IMS.

4.2 Druha prednáška

Tato prednáška poslucháča zavedie hlbšie do technológie IMS a oboznámi ho s jej architektonickými prvkami popísanými v časti 2.1. Poslucháč nadobudne obraz o službách IMS, Kvalite, o účtovaní v sieťach IMS, bezpečnosti a vrstevnom dizajne. V ďalšej časti prednášky spomenie entity a funkčné časti, ako sú riadiace funkcie relácie volania Databázy Funkcie služby, vzájomne komunikujúce funkcie Podporné funkcie, ako je popísané v časti 2.2.

4.3 Tretia prednáška

tretia prednáška vysvetí akým spôsobom sú popísané sieťové jednotky spojené medzi sebou a aký protokol je použitý. Prehľad referenčných bodov na báze SIP s časti 2.3.

4.4 Štvrtá prednáška

Predstavy koncept IMS. Popise registrácie s časti 3.1 a vytvorenia relácie IP multimediálneho subsystému s časti 3.3. Popisuje zapojené IMS entity, mechanizmus

kontroly prevádzky nosičov (časť 3.9), odhalenie vstupného bodu IMS (časť 3.7), zdieľanie jednej užívateľskej identity medzi viacerými zariadeniami(časť 3.6, Identifikácia(časť 3.4), iniciácia relácie(časť 3.3).

4.5 Piata prednáška

Nadväzuje na vedomosti získané s predchádzajúcej prednášky a rozšíri poslucháčovi znalosti o ďalšie koncepčné riešenia ako účtovanie, užívateľský profil, poskytovanie služby, konektivita medzi tradičnými CS užívateľmi a IMS užívateľmi, konvergencia pevných a mobilných sietí, SIP kompresia, vzájomná komunikácia medzi IPv4 a IPv6 v IMS, kombinácia CS a IMS služieb - Kombinovanie služieb, bezpečnostné služby v IMS.

Tabuľka 4.1

Prvá prednáška	
1	Úvod
1.1	Príklad IMS služieb
1.2	Vývoj IMS
Druha prednáška	
2.1	Architektonické požiadavky
2.2	Popis entít a funkčností súvisiacich IMS
Tretia prednáška	
2.3	Referenčné body IMS
Štvrtá prednáška	
3.1	Registrácia
3.2	Mechanizmus pre súbežnú registráciu viacerých užívateľských identít
3.3	Iniciácia relácie
3.4	Identifikácia
3.5	Moduly identity
3.6	Zdieľanie jednej užívateľskej identity medzi viacerými zariadeniami
3.7	Odhalenie vstupného bodu IMS
3.8	Priradenie S-CSCF
3.9	Mechanizmus kontroly prevádzky nosičov

Piata prednáška	
3.10	Účtovanie
3.11	Užívateľský profil
3.12	Poskytovanie služby
3.13	Konektivita medzi tradičnými CS užívateľmi a IMS užívateľmi
3.14	Konvergencia pevných a mobilných sietí
3.15	SIP kompresia
3.16	Vzájomná komunikácia medzi IPv4 a IPv6 v IMS
3.17	Kombinácia CS a IMS služieb - Kombinovanie služieb
3.18	Bezpečnostné služby v IMS

5. Záver

V mojej diplomovej práci som sa venoval podrobnejšiemu opisu technológie IMS. Je to globálna, od prístupu nezávislá a na IP štandardoch založená konektivita a architektúra kontroly služby, ktorá umožňuje rôzne typy multimediálnych služieb pre koncových užívateľov používajúcich spoločné protokoly na báze IP.

Druhá kapitola vysvetľuje základné architektonické koncepty: napríklad vysvetľujeme, prečo sú nosiče oddelené a prečo bol zvolený model domácej kontroly. Časť 2.1 ponúka široký prehľad IMS architektúry, vrátane úvodu do rôznych sieťových entít a hlavných funkčností. Časť 2.2 ide viac do hĺbky a ukazuje, ako sú entity prepojené a aké protokoly sú medzi nimi použité; popisuje tiež ich vzťahy k iným doménam: IP siete, univerzálny mobilný telekomunikačný systém (Universal Mobile Telecommunications System - UMTS) a obvodovo spínaná základná sieť (Circuit Switched Core Network - CS CN).

Tretia kapitola popisuje registrácie a vytvorenia relácie IP multimediálneho subsystému (IP Multimedia Subsystem – IMS). Popisuje zapojené IMS entity. Koncept na odhalenie proxy-riadiacej funkcie relácie volania (Proxy-Call Session Control Function - P-CSCF). Užívateľské identity z modulov identity a identity. Obslužnú riadiacu funkciu relácie volania (Serving Call Session Control Function - S-CSCF). Dalej su vysvetlene príslušné bezpečnostné spojenia, stiahnutý užívateľský profil do pridelenej S-CSCF, verejné užívateľské identity a Koncept zdieľania jednej užívateľskej identity medzi viacerými terminálmi. Vysvetľuje, ako je aplikovaná kontrola internetového protokolu (Internet Protocol – IP), keď užívateľ vytvára reláciu a ukazuje, ako môžu byť zabezpečené služby. ukazuje, ako môže operátor spoplatniť užívateľa. Stručne popísaná je vzájomná komunikácia s obvodovo spínanou (Circuit Switched –CS) sieťou. Súčasné ukazuje použitie CS a paketovo spínaných (Packet Switched – PS) komponentov. Okrem toho, je pokrytá pevná mobilná konvergencia a vzájomná komunikácia IP verzií.

Použitá literatura

The IMS: IP Multimedia Concepts and Services, SE Miikka Poikselkä, Georg Mayer, Hisham Khartabil and Aki Niemi © 2006 John Wiley & Sons, Ltd. ISBN: 0-470-01906-9

Internetové štandardy

RFC1321 Rivest, R., The MD5 Message-Digest Algorithm, April 1992.

RFC1851 Karn, P., Metzger, P. and W. Simpson, The ESP Triple DES Transform, September 1995.

RFC2401 Kent, S. and R. Atkinson, Security Architecture for the Internet Protocol, November 1998.

RFC2404 Madson, C. and R. Glenn, The Use of HMAC-SHA-1-96 within ESP and AH, November 1998.

RFC2406 Kent, S. and R. Atkinson, IP Encapsulating Security Payload (ESP), November 1998.

RFC2408 Maughan, D., Schneider, M. and M. Schertler, Internet Security Association and Key Management Protocol (ISAKMP), November 1998.

RFC2409 Harkins, D. and D. Carrel, The Internet Key Exchange (IKE), November 1998.

RFC2616 Fielding, R., Gettys, J., Mogul, J., Nielsen, H., Masinter, L., Leach, P. and T. Berners-Lee, Hypertext Transfer Protocol – HTTP/1.1, June 1999.

RFC2617 Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, HTTP Authentication: Basic and Digest Access Authentication, June 1999.

RFC3261 Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, SIP: Session Initiation Protocol, June 2002.

RFC3310 Niemi, A., Arkko, J. and V. Torvinen, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA), September 2002.

RFC3323 Peterson, J., A Privacy Mechanism for the Session Initiation Protocol (SIP), November 2002.

RFC3325 Jenning, C., Peterson, J. and M. Watson, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, November 2002.

RFC3329 Arkko, J., Torvinen, V., Camarillo, G., Niemi, A. and T. Haukka, Security Mechanism Agreement for the Session Initiation Protocol (SIP), January 2003.

RFC3485 Garcia-Martin, M., Bormann, C., Ott, J., Price, R. and A.B. Roach, The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp), February 2003.

RFC3486 Camarillo, G., Compressing the Session Initiation Protocol (SIP), February 2003.

RFC3588 Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, Diameter Base Protocol, September 2003.

Projekty sieťe tretej generácie

3GPP TS 23.002 Network architecture.

3GPP TS 23.003 Technical Specification Group Core Network; Numbering, addressing and identification.

3GPP TS 23.060 General Packet Radio Service (GPRS);Service description; Stage 2.

3GPP TS 23.107 Quality of Service (QoS) concept and architecture.

3GPP TS 23.207 End-to-end QoS concept and architecture.

3GPP TS 23.228 IP Multimedia (IM) Subsystem; Stage 2.

3GPP TS 24.008 Mobile Radio Interface Layer 3 specification; Core Network protocols; Stage 3.

3GPP TS 24.147 Conferencing using the IP Multimedia(IM) Core Network(CN) subsystem; Stage 3.

3GPP TS 24.229 IP Multimedia Call Control based on SIP and SDP; Stage 3.

3GPP TS 26.234 Transparent end-to-end packet-switched streaming service (PSS); Protocols and codecs.

3GPP TS 26.236 Packet-switched conversational multimedia applications; Transport protocols.

3GPP TS 29.207 Policy control over Go interface, June 2003.

3GPP TS 29.198 Open Service Access (OSA); Application Programming Interface (API), Multiple parts.

3GPP TS 29.208 End-to-end Quality of Service (QoS) signaling flows.

3GPP TS 29.209 Policy control over Gq interface.

3GPP TS 29.229 Cx and Dx interfaces based on the Diameter protocol; Protocol details, June 2003.

3GPP TS 31.102 Characteristics of the USIM application.

3GPP TS 31.103 Characteristics of the IP Multimedia Services Identity Module (ISIM) application.

3GPP TS 32.295 Charging management; Charging Data Record (CDR) transfer.

3GPP TS 32.295 Charging management; Charging Data Record (CDR) transfer.

3GPP TS 32.299 Diameter charging applications.

3GPP TS 33.102 3G security; Security architecture, June 2003.

3GPP TS 33.203 3G security; Access security for IP-based services, June 2003.

3GPP TS 33.210 3G security; Network Domain Security (NDS); IP network layer security, June 2003.

3GPP TS 33.220 3G security; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, 3GPP, December 2003.

3GPP TS 33.222 Generic Authentication Architecture (GAA); Access to network application functions using Secure Hypertext Transfer Protocol (HTTPS), February 2004.

3GPP TS 33.310 Network Domain Security; Authentication Framework (NDS/AF), December 2003.

ČESTNÉ VYHLÁSENIE

Vyhlasujem, že som zadanú diplomovú prácu vypracoval samostatne, pod odborným vedením vedúceho diplomovej práce prof. Ing. Karol Blunár, DrSc. a používal som len literatúru uvedenú v práci.

Súhlasím so zapožičiavaním diplomovej práce.

V Žiline dňa 16.5.2008 .....

POĎAKOVANIE

Touto cestou by som chcel poďakovať prof. Ing. Karolovy Blunárovy, DrSc. za všetky rady a pripomienky ktorými ma viedol pri vypracovávaní tejto diplomovej práce, taktiež všetkým ostatným, ktorí si našli čas a mali trpezlivosť odpovedať na moje otázky.